

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

FLÁVIO PINTO VIEIRA

**Um Algoritmo para Estimar a
Dimensão do Segundo Grupo de
Homologia de um Grupo Finitamente
Apresentado**

Goiânia
2012

FLÁVIO PINTO VIEIRA

Um Algoritmo para Estimar a Dimensão do Segundo Grupo de Homologia de um Grupo Finitamente Apresentado

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

Área de concentração: Álgebra.

Orientadora: Profa. Ticianne Proença Bueno Adorno

Coorientadora: Profa. Shirlei Serconeck

Goiânia
2012

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

V658a Vieira, Flávio Pinto.
Um algoritmo para estimar a dimensão do segundo grupo de homologia de um grupo finitamente apresentado [manuscrito] / Flávio Pinto Vieira. – 2012.
92 f.
Orientadora: Prof^ª. Dr^ª. Ticianne Proença Bueno Adorno;
Coorientadora: Prof^ª. Dr^ª. Shirlei Serconeck.
Dissertação (Mestrado) – Universidade Federal de Goiás, Instituto de Matemática e Estatística, 2012.
Bibliografia.
Apêndices.

1. Algoritmo. 2. Multiplicador de Schur. I. Título.

CDU:510.5

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem autorização da universidade, do autor e do orientador(a).

Flávio Pinto Vieira

Graduou-se em Matemática na UEG - Universidade Estadual de Goiás. Fez Especialização em Matemática pela UFG-Universidade Federal de Goiás. Foi professor da UEG-Universidade Estadual de Goiás Unidade, Universitaria de Sanclerlândia e em escolas públicas do Estado de Goiás. Atualmente é professor substituto do IFG-Instituto Federal de Educação, Ciência e Tecnologia de Goiás e da Escola Estadual Amália Hermano Teixeira.

Dedico este trabalho a toda a minha família, de uma maneira muito especial a meu pai **Alziro Camilo Vieira**, minha mãe **Jovely Pinto de de Faria** pelo exemplo de vida e pela dedicação que tiveram em me educar e mostrar a importância do conhecimento e a minha namorada **Daliane Maria de Ramos**.

Agradecimentos

Agradeço primeiramente e acima de tudo a Deus por ter me dado a vida e permitido chegar até os dias atuais com saúde e alegria de viver.

A meus pais **Alzira Camilo Vieira** e minha mãe **Jovely Pinto de Faria** por terem me ensinado a viver e sempre incentivar a continuar em busca do desconhecido. Ao meu irmão Fábio Pinto Vieira pelo exemplo de vida.

A minha orientadora Dr^a. Ticianne Proença Bueno Adorno pela confiança, paciência e dedicação em me orientar por todo o período em que desenvolvi este trabalho.

A professora Dr^a. Shirlei Serconeck pelas coorientações, confiança e incentivo que sempre teve comigo. Ao professor Mário José de Souza por ter me motivado a prosseguir os estudos durante o curso de Especialização e suas preciosas sugestões para melhoria deste trabalho. A professora Dr^a. Sheila Campos Chagas pelas correções e sugestões enriquecendo esta dissertação.

A todos os meus colegas da Especialização que foram um pilar de sustentação para que eu pudesse me ingressar no mestrado, Lucimeire, Saeny, Fernando, Sérgio, Danilo, Jeferson, Maycon.

Aos grandes colegas do mestrado que sempre foram um apoio nos momentos de dificuldade, meus sinceros agradecimentos a Fernando, Rosane, Alex, Edwin, Victor Hugo, Sérgio, Márcio, Milton Gabriel, Danilo, Caíke, Gean, José Henrique.

A todos os inesquecíveis amigos da Paróquia Nossa Senhora da Assunção, em especial dos grupos de oração Nossa Senhora da Piedade, Nossa Senhora da Assunção e do grupo de Jovens Face de Cristo que me ensinaram novamente o prazer de morrer para o mundo e viver para Deus. Ao meu grande amigo Richard que reviveu em mim a honra que é ser servo de Deus.

A todos os meus colegas de trabalho que lutam para que o Brasil seja realmente uma terra de "paz no futuro e glória no passado".

E do mais íntimo do meu coração, pelas orações e pelo carinho que sempre me tratou, Daliane Maria de Ramos te amo muito.

À CAPES e a Secretaria de Estado da Educação pelo apoio financeiro.

"O que ama a instrução ama o conhecimento, mas o que odeia a repreensão é estúpido. O homem de bem alcançará o favor do SENHOR, mas ao homem de intenções perversas ele condenará."

(Provérbios de Salomão. 12, 1-2).

Resumo

Pinto Vieira, Flávio. **Um Algoritmo para Estimar a Dimensão do Segundo Grupo de Homologia de um Grupo Finitamente Apresentado**. Goiânia, 2012. 91p. Dissertação de Mestrado. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

O trabalho tem por objetivo principal estabelecer uma cota superior para a dimensão do segundo grupo de homologia de um grupo G , com coeficientes em um corpo k de característica p , $H_2(G, k)$, usando o sistema operacional GAP. Será apresentado uma gama de exemplos, onde em alguns casos, calcularemos exatamente a dimensão e em outras somente uma cota superior.

Palavras-chave

Módulos, Categorias, Grupos Livres, Sequências Exatas, Homologia, Cohomologia, Multiplicador de Schur, Grupo Associado, GAP.

Abstract

Pinto Vieira, Flávio. **An algorithm for low dimensional group homology**. Goiânia, 2012. 91p. MSc. Dissertation. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

The main goal of this work is to establish a primary bound for the dimension of the second homology group of a group G , with coefficients in a field k of characteristic p , $H_2(G, k)$, using the operating system GAP. It will be presented with several examples, where in some cases, will be calculated the exact dimensions and in other cases only an upper bound.

Keywords

Module, Categoria, Free Group, Exact Sequence, Homology, Cohomology, Schur Multiplier, Associated Group, GAP.

Sumário

Introdução	11
1 Preliminares	15
1.1 Subgrupo de Frattini	15
1.2 Ações	16
1.3 Módulos	17
1.4 Categorias	18
1.4.1 Categorias	18
1.5 Grupos Livres	20
1.5.1 Construção de um Grupo Livre	20
1.5.2 Apresentação Finita de um Grupo	22
1.5.3 Sequências Exatas	23
1.6 Produto Tensorial	25
1.6.1 Construção de um Produto Tensorial	25
1.7 Homologia e Complexos	30
1.7.1 Homotopia	31
1.8 Funtor Derivado	31
1.8.1 Funtor Tor	33
1.9 Grupos de Homologia	33
1.9.1 Primeiro Grupo de Homologia	36
1.10 Grupos Abelianos Finitamente Gerados	38
2 O Multiplicador de Schur	44
2.1 Grupos de Cohomologia	44
2.2 O Multiplicador de Schur	48
2.2.1 Fórmula de Hopf	50
2.2.2 Exemplos de Cálculo do Multiplicador de Schur	53
2.3 Grupos de Deficiência Zero	54
3 O Segundo Grupo de Homologia de um Grupo; Relações entre Comutadores	59
3.1 Grupo Associado	59
4 Um Algoritmo para estimar o Segundo Grupo de Homologia de alguns Grupos Finitamente Apresentado	68
4.1 Primeiro Grupo de Homologia	68
4.1.1 O Primeiro Algoritmo de homologia	70
4.1.2 O Primeiro Algoritmo com Coeficiente Homológicos	71
4.2 Segundo Grupo de Homologia	71
4.2.1 O Algoritmo Tor	73

4.2.2	O Algoritmo Rank	75
4.2.3	Algoritmo Palavra Reduzida	77
4.2.4	O Algoritmo de Encontrar Base	78
4.2.5	O Algoritmo Segundo Homologia com Coeficientes	78
4.3	Exemplos	79
4.4	Considerações Finais	82
Referências Bibliográficas		86
A	Algoritmos	88

Introdução

Em 10 de Janeiro de 1875 nasce em Mogilyov, Russia, Issai Schur, um grande matemático que contribuiu em muito com o desenvolvimento das ciências exatas. Com 13 anos Schur foi para a Letônia onde fez o ginásio. Ingressou em 1894 na Universidade de Berlim no departamento de Matemática e Física. Teve como professor Frobenius que posteriormente foi seu orientador de doutorado. Se tornou professor da Universidade de Berlim em 1903 e da Universidade de Bonn de 1911 a 1916, retornando a Berlim em 1916 onde montou sua famosa escola e obteve o título de professor titular em 1919, o mantendo até ser demitido pelos nazistas em 1935. Schur é conhecido por seus trabalhos em teoria de representações de grupos, mas ele trabalhou em teoria de números e análise, [18].

Em uma série de artigos publicados por volta de 1929 ele introduziu o conceito do Multiplicador de Schur. Este é um conceito abstrato extremamente importante que surgiu a partir dos problemas concretos que Schur estava estudando. Mais tarde em 1949 Eilenberg e Mac Lane [5] definiram usando grupos de cohomologia.



Issai Schur (13 Janeiro, 1894 - 10 Janeiro, 1941)

A escola de Schur foi certamente o grupo mais influente dos matemáticos, em Berlim, e entre as mais importantes de toda Alemanha. Esta escola teve contribuições em grupos solúveis, combinatória e teoria de matrizes. Schur era extremamente popular, um de seus cursos de álgebra foi ministrado em um auditório cheio, com cerca de 400 alunos. Schur deixou a Alemanha e foi morar na Palestina, em 1939 onde morreu em 10 Janeiro

de 1941, deixando uma gama de contribuições para as mais diversas áreas da matemática em especial Álgebra. Inspirando inclusive o artigo principal deste trabalho [14].

A Topologia Algébrica passou por um desenvolvimento espetacular, durante o período da segunda guerra mundial. Em comparação com as áreas tradicionais de análise e de álgebra, a Topologia Algébrica saiu de uma posição de menor importância para exercer uma influência profunda sobre os campos mais antigos da matemática. E, em grande parte, o sucesso deste desenvolvimento pode ser atribuído à influência de Norman Steenrod. Até esta época existiam vários conceitos de homologia, mas não existia a “teoria de homologia” criada então por Steenrod.

Em 1945 foi consumado por Steenrod e Eilenberg a axiomatização da teoria de homologia. Tal teoria era complicada, mas as propriedades se caracterizaram pela beleza e simplicidade.

Também no ano de 1945 Eilenberg e MacLane publicaram o artigo “Relation between homology groups of spaces” [5], dando um avanço na teoria de homologia.

O Multiplicador de Schur de um grupo G é definido como o segundo grupo de cohomologia de G sobre os complexos não nulos, $H^2(G, \mathbb{C}^*)$, ou como o segundo grupo de homologia de G sobre os inteiros, $H_2(G, \mathbb{Z})$. Como já foi mencionado em 1949 Eilenberg e Mac Lane perceberam que a teoria de homologia implementada por eles e Steenrod, era em alguns casos a mesma criada por Schur.

Schur mostrou em 1907 que $H_2(X) \cong (R \cap F')/[F, R]$, sendo X um espaço topológico. Posteriormente em 1942 Hopf demonstra que $M(G) \cong (R \cap F')/[F, R]$, onde G é um grupo finito, tal fórmula foi batizada como “fórmula de Hopf”.

Calcular o grupo de homologia é extremamente difícil quando o grupo possui uma apresentação grande, tornando-se inviável obter o multiplicador de Schur de tais grupos. Desta forma, este trabalho procura apresentar uma teoria que possibilite contornar tal situação.

O principal objetivo deste trabalho é estudar o artigo “An Algorithm For Low dimensional Group Homology”, [14], de Joshua Roberts publicado em 2010, que usa o sistema GAP (Grupo, Algoritmos e Programas), [7], para estimar uma cota superior para a dimensão do segundo grupo de homologia de um grupo finitamente apresentado G .

Este trabalho é composto de quatro capítulos e um apêndice. bem como resultados básicos para que os leitores tenham condições de compreender o algoritmo apresentado no Capítulo 4 junto com seus exemplos.

No Capítulo 1 apresentamos definições, resultados e conceitos básicos que serão necessários para os capítulos posteriores. Iniciamos com um breve comentário sobre o *subgrupo de Frattini* de um grupo G , tal conceito é fundamental na demonstração da fórmula de Hopf (Teorema 2.26), podemos encontrar este conteúdo em [21], [23]. Definiremos *ação de grupos* que será usado no Capítulo 4 e pode ser

encontrado em, [21] e [11]. Baseado em [11], [22], [25], [12], [24], [23], definiremos *categorias, grupos livres e produto tensorial* para posteriormente trabalhar com *grupos de homologia* que é a definição central deste trabalho. Sendo (C, d) um *complexo*, o *n-ésimo módulo homológico* do complexo é definido como o quociente dos *n-ciclos* pelos *n-bordos* $H_n = H_n(C) = Z_n/B_n$. Neste capítulo construiremos o funtor derivado a esquerda do funtor $(M \otimes_R, -)$ que é o funtor $Tor_n(M, -)$, e o funtor derivado a direita do funtor $hom(-, N)$ que é o funtor $Ext_n(-, N)$. Definiremos o *n-ésimo grupo de homologia* e em especial trabalharemos com $n = 2$, ou seja, com o segundo grupo de homologia de um grupo G . Encerramos este capítulo com uma seção independente das demais apresentadas, onde trabalhamos com grupos abelianos finitamente gerados, e apresentamos um algoritmo para calcular a forma normal Smith de um grupo.

No Capítulo 2 definiremos *grupos de cohomologia* e o *multiplicador de Schur* de um grupo G que é o segundo grupo de cohomologia de G sobre os complexos não nulos, [23]. Também mostraremos que $M(G) \cong \frac{(R \cap F')}{[F, R]}$, onde F é um grupo livre finitamente gerado e R é o conjunto de relações de G , resultado popularmente conhecido como a fórmula de Hopf, [25]. Apresentamos neste capítulo uma seção de exemplos de cálculos do multiplicador de Schur de alguns grupos, segundo Karpilovsky, [15], [19], alguns destes exemplos serão posteriormente retomados no capítulo 4. Encerramos este capítulo falando dos grupos de deficiência zero que é outra maneira de apresentar o multiplicador de Schur de um grupo G , segundo Beyl e Tappe, [2].

No Capítulo 3 apresentaremos o artigo “The Second homology group of a group; relation among comutators” publicado em 1956 por Clair Miller, [17], que apresentou uma interpretação grupo-teorética do segundo grupo de homologia $H_2(G, \mathbb{Z}^*)$ de um grupo G , com coeficientes no grupo dos inteiros não nulos \mathbb{Z}^* . Neste artigo Clair Miller define um novo grupo, $H(G)$, chamado o *grupo associado* de G , que é informalmente o grupo de todas as relações que são satisfeitas por comutadores em G . Encerraremos este capítulo exibindo um homomorfismo entre $H(G)$ e $H_2(G, \mathbb{Z}^*)$, ou seja, um homomorfismo canônico entre $H(G)$ e $H_2(G, \mathbb{Z}^*)$ preservando a noção de homomorfismo induzido; se $G \rightarrow K$ é um homomorfismo temos a comutatividade do diagrama

$$\begin{array}{ccc} H(G) & \xrightarrow{h_*} & H(K) \\ \wr & & \wr \\ H_2(G, \mathbb{Z}^*) & \xrightarrow{h_*} & H_2(K, \mathbb{Z}^*). \end{array}$$

Baseado no artigo de Joshua Roberts “An algorithm for low dimensional group homology”, [14], que é o principal artigo usado neste trabalho, desenvolvemos o Capítulo 4. Roberts obteve um algoritmo para estimar a dimensão do segundo grupo de

homologia de um grupo qualquer finitamente apresentado. Mais precisamente, dado um grupo finitamente apresentado G e um corpo finito k , o segundo grupo de homologia $H_2(G, k)$ com coeficientes em k é um espaço vetorial de dimensão finita sobre k , onde G age trivialmente. Em alguns casos ele calcula exatamente esta dimensão usando alguns pacotes do GAP. Apresentaremos exemplos com grupos de ordens pequenas, alguns já comentados na seção 2.2.2 e trabalharemos com novos exemplos que foram apresentados por Anton em seu artigo *Homological symbols and the Quillen conjecture*, [1].

Encerramos este trabalho com um apêndice onde apresentamos a maneira em que os algoritmos do capítulo 4 foram inseridos no programa GAP.

Preliminares

Neste capítulo apresentaremos as definições de categorias, produto tensorial, grupos livres bem como exemplos e resultados importantes que serão usados nos capítulos posteriores.

1.1 Subgrupo de Frattini

Nesta seção trabalho definiremos o subgrupo de Frattini, bem como, apresentaremos um resultado que será usado para demonstrar a fórmula de Hopf na seção 2.2.1. As definições e resultados podem ser encontradas em [21] e [23].

Teorema 1.1 (Schur). *Seja G um grupo. Se $Z(G)$ tem índice finito em G , então G' é finito.*

Teorema 1.2 *Se G é um grupo finitamente gerado e H é um subgrupo de G de índice finito, então H é finitamente gerado.*

Definição 1.3 *Se H é subgrupo de um grupo G , H é um **subgrupo maximal** de G se, sempre que existir um subgrupo K de G , com $H \leq K \leq G$, então $H = K$ ou $K = G$.*

Exemplo 1.4 *Seja $X = \{1, 2, \dots, n\}$, denotaremos por S_n **grupo simétrico em X** . Seja A_n o grupo de todas as permutações pares de S_n . O subgrupo A_n é maximal em S_n .*

Definição 1.5 *Se G é um grupo o **subgrupo de Frattini** de G , $\Phi(G)$, é definido como a intersecção de todos os subgrupos maximais de G .*

Definição 1.6 *Um elemento $x \in G$ é chamado **não-gerador** se ele pode ser retirado do conjunto de geradores, isto é, se $G = \langle x, Y \rangle$, então $G = \langle Y \rangle$.*

Teorema 1.7 *Para cada grupo G , o subgrupo de Frattini $\Phi(G)$ é o conjunto de todos os não geradores de G .*

Demonstração. Seja x um não gerador de G , e seja M um subgrupo maximal de G . Se $x \notin M$, então $G = \langle x, M \rangle = M$, o que é uma contradição. Portanto, $x \in M$ para todo M , e assim $x \in \Phi(G)$.

Reciprocamente, se $z \in \Phi(G)$, e suponha que $G = \langle z, Y \rangle$. Se $\langle Y \rangle \neq G$, então existe um subgrupo maximal M com $\langle Y \rangle \leq M$. Mas $z \in M$ e assim $G = \langle z, Y \rangle \leq M$ o que é uma contradição. Portanto, z é um não gerador. \square

Teorema 1.8 (Gaschütz, 1953). Para cada grupo finito G , temos que $G' \cap Z(G) \leq \Phi(G)$.

Demonstração. Seja $G' \cap Z(G) = D$. Suponha que $D \not\leq \Phi(G)$, logo existe um subgrupo maximal M de G com $D \not\leq M$. Portanto, $G = MD$ assim, cada $g \in G$ tem uma fatoração $g = md$ com $m \in M$ e $d \in D$. Como $d \in Z(G)$, $gMg^{-1} = mdMd^{-1}m^{-1} = mMm^{-1} = M$, assim M é um subgrupo normal de G . Implicando que G/M tem ordem prima, daí é abeliano. Portanto, $G' \leq M$, o que é uma contradição ao fato que $D \not\leq M$. \square

1.2 Ações

Definiremos agora ação e daremos exemplos, como o da ação por conjugação que será usado em todo o trabalho em especial no capítulo 4.

Definição 1.9 Uma *ação* de um grupo G em um conjunto S é uma função

$$\begin{aligned} G \times S &\longrightarrow S \\ (g, s) &\longmapsto gs, \end{aligned}$$

tal que, para todo $s \in S$ e $g_1, g_2 \in G$, temos,

$$es = s \quad e \quad (g_1g_2)s = g_2(g_1s),$$

onde e é o elemento neutro. Quando uma tal ação é dada, dizemos que G age no conjunto S .

Exemplo 1.10 Seja G um grupo e H um subgrupo de G . Uma ação do grupo H em G , dada por $(h, x) \mapsto hx$, onde hx é produto em G . A ação de $h \in H$ em G é chamada uma *translação a esquerda*.

Exemplo 1.11 Seja H um subgrupo de um grupo G . Uma ação de H no conjunto G dada por $(h, x) \mapsto h x h^{-1}$ é chamada *conjugação* por h . O elemento $h x h^{-1}$ é chamado

conjugado de x . Se K é algum subgrupo de G e $h \in H$, então hKh^{-1} é um subgrupo de G isomorfo a K . Desta forma, H age no conjunto S de todos os subgrupos de G por conjugação: $(h, K) \mapsto hKh^{-1}$. O grupo hKh^{-1} é chamando **conjugado** por K .

1.3 Módulos

Nesta seção introduziremos o conceito de Módulos que será base para o estudo nas seções subsequentes.

Definição 1.12 *Seja K um anel comutativo com elemento identidade. Um K -módulo M (a esquerda) é um grupo abeliano munido da operação*

$$\begin{aligned} K \times A &\longrightarrow A \\ (r, a) &\longmapsto ra, \end{aligned}$$

chamada “multiplicação escalar”, tal que, para $r, s \in K$; $a, b \in A$, satisfaz as seguintes propriedades:

- (i) $r(a + b) = ra + rb$;
- (ii) $(r + s)a = ra + sa$;
- (iii) $(rs)a = r(sa)$;
- (iv) $1a = a$.

Exemplo 1.13 *Seja K um anel comutativo com elemento identidade. O anel $\mathcal{A} = \text{Mat}_n(K)$ das matrizes $n \times n$ sobre K é um K -módulo com as operações usuais de matrizes.*

Exemplo 1.14 *Seja K um anel comutativo com elemento identidade. O anel de polinômios $K[x]$ na indeterminada x é um K -módulo \mathcal{A} com as operações usuais de polinômios.*

Exemplo 1.15 *Se R é um anel, o conjunto R^n de todas as n -uplas, onde as componentes estão em R , é um R -módulo, com a adição e multiplicação por escalar definidas abaixo:*

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$$

e

$$r(a_1, \dots, a_n) = (ra_1, \dots, ra_n)$$

para $a_i, b_i, r \in R$.

1.4 Categorias

Nesta seção introduziremos alguns conceitos básicos necessários. Daremos algumas definições como de categorias e grupos livres bem como exemplos e resultados importantes.

1.4.1 Categorias

Definição 1.16 Uma *categoria* é uma classe \mathcal{C} de objetos (denotados A, B, C, \dots) juntamente com:

(i) uma classe de conjuntos disjuntos, denotados por $\text{hom}(A, B)$, um para cada par de objetos em \mathcal{C} ; (um elemento f de $\text{hom}(A, B)$ é chamado um **morfismo** de A em B e é denotado por $f : A \rightarrow B$);

(ii) para cada terna (A, B, C) de objetos de \mathcal{C} uma função

$$\text{hom}(B, C) \times \text{hom}(A, B) \rightarrow \text{hom}(A, C);$$

(para morfismos $f : A \rightarrow B$, $g : B \rightarrow C$, esta função é escrita $(g, f) \mapsto g \circ f$ e o morfismo $g \circ f : A \rightarrow C$ é chamado a *composição de f e g*); Todos sujeitos aos dois axiomas:

(I) *Associatividade*. Se $f : A \rightarrow B$, $g : B \rightarrow C$, $h : C \rightarrow D$ são morfismos de \mathcal{C} , então $h \circ (g \circ f) = (h \circ g) \circ f$.

(II) *Identidade*. Para cada objeto de \mathcal{C} existe um morfismo $1_B : B \rightarrow B$ tal que para todo $f : A \rightarrow B$, $g : B \rightarrow C$,

$$1_B \circ f = f \quad e \quad g \circ 1_B = g.$$

Notação: Denotaremos o conjunto de objetos de \mathcal{C} por $\text{obj}(\mathcal{C})$.

Exemplo 1.17 Seja \mathcal{C} uma categoria. Definimos a categoria \mathcal{D} cujos objetos são todos morfismos de \mathcal{C} . Se $f : A \rightarrow B$ e $g : C \rightarrow D$ são morfismos de \mathcal{C} , então $\text{hom}(f, g)$ consiste de todo par (α, β) , onde $\alpha : A \rightarrow C$, $\beta : B \rightarrow D$ são morfismos de \mathcal{C} , tal que o seguinte diagrama comute:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \alpha \downarrow & & \downarrow \beta \\ D & \xrightarrow{g} & C \end{array}$$

Exemplo 1.18 Seja \mathcal{G} a categoria cujos objetos são todos grupos; E $\text{hom}(A, B)$ é o conjunto de todos os homomorfismos de grupos $f : A \rightarrow B$.

Definição 1.19 Uma *categoria concreta* é uma categoria \mathcal{C} junto com uma função σ que fixa, para cada objeto A de \mathcal{C} , um conjunto $\sigma(A)$ (chamado o conjunto subjacente de A), tal que:

- (i) cada morfismo $A \rightarrow B$ de \mathcal{C} é uma função de conjuntos subjacentes $\sigma(A) \rightarrow \sigma(B)$;
- (ii) o morfismo identidade de cada objeto A de \mathcal{C} é a função identidade no conjunto subjacente $\sigma(A)$;
- (iii) a composição de morfismo em \mathcal{C} age como a composição de funções nos conjuntos subjacentes;

Exemplo 1.20 A categoria de grupos, junto com a função que fixa para cada grupo o conjunto subjacente, é uma categoria concreta.

Exemplo 1.21 Um grupo multiplicativo G pode ser considerado como uma categoria com um objetos G . Considere $\text{hom}(G, G)$ o conjunto de elementos de G ; uma operação binária em G é dada pela composição de morfismos. Se a função σ fixa para o grupo G o usual conjunto subjacente G , então esta categoria não é uma categoria concreta.

Definição 1.22 Sejam F um objeto em uma categoria concreta \mathcal{C} , X um conjunto não vazio, e $\iota : X \rightarrow F$ uma função de conjuntos. F é um **livre sobre o conjunto** X se para todo objeto A de \mathcal{C} e toda função de conjuntos $f : X \rightarrow A$, existe um único morfismo de \mathcal{C} , $\bar{f} : F \rightarrow A$, tal que $\bar{f}\iota = f$ (como uma função de conjuntos $X \rightarrow A$). A definição implica que o diagrama comuta:

$$\begin{array}{ccc} X & \xrightarrow{\iota} & F \\ & \searrow f & \nearrow \bar{f} \\ & & A \end{array}$$

Exemplo 1.23 Sejam \mathbb{Z} um objeto na categoria de grupos \mathcal{G} , $X = \{1\}$ um conjunto não vazio e $\iota : X \rightarrow \mathbb{Z}$ a função inclusão. Então \mathbb{Z} é livre sobre o conjunto X se para todo G em \mathcal{G} e toda função de conjuntos $f : X \rightarrow G$, existe um único morfismo de \mathcal{G} , $\bar{f} : \mathbb{Z} \rightarrow G$ definida por $\bar{f}(n) = g^n$. O exemplo diz que o diagrama é comutativo:

$$\begin{array}{ccc} X = \{1\} & \xrightarrow{\iota} & \mathbb{Z} \\ & \searrow f & \nearrow \bar{f} \\ & & G \end{array}$$

Definição 1.24 Um objeto I em uma categoria \mathcal{C} é dito **universal** (ou **inicial**) se para cada objeto C de \mathcal{C} existe um e somente um morfismo de I em C . Um objeto T de \mathcal{C} é dito ser **couniversal** (ou **terminal**) se para cada objeto C de \mathcal{C} existe um e somente um morfismo de C em T .

1.5 Grupos Livres

Mostraremos que existem objetos livres (grupos livres) na categoria de grupos, que serão usados para desenvolver um método de descrever grupos em termos de geradores e relações. Mostraremos também como construir coprodutos na categoria de grupos.

1.5.1 Construção de um Grupo Livre

Dado um conjunto X construiremos um grupo F que é livre no conjunto X como na definição 1.22.

Se $X = \emptyset$, F é o grupo trivial $\langle e \rangle$. Se $X \neq \emptyset$, seja X^{-1} um conjunto disjunto de X tal que $|X| = |X^{-1}|$. Escolhendo uma bijeção de X em X^{-1} denotaremos a imagem de $x \in X$ por x^{-1} . Escolhamos um conjunto unitário disjunto de $X \cup X^{-1}$, cujo elemento será denotado por 1.

Definição 1.25 Uma *palavra* em X é uma sequência (a_1, a_2, \dots) , com $a_i \in X \cup X^{-1} \cup \{1\}$ tal que para todo $n \in \mathbb{N}^*$, $a_k = 1$ para todo $k \geq n$. A sequência constante $(1, 1, 1, \dots)$ é chamada a palavra vazia e será denotada por 1.

Definição 1.26 Uma palavra (a_1, a_2, \dots) em X é uma *palavra reduzida* se:

- (i) para todo $x \in X$, x e x^{-1} não são adjacentes (isto é, $a_i = x \Rightarrow a_{i+1} \neq x^{-1}$ e $a_i = x^{-1} \Rightarrow a_{i+1} \neq x$)
- (ii) $a_k = 1$ implica $a_i = 1$ para todo $i \geq k$.

Em particular, a palavra vazia 1 é reduzida. A palavra reduzida 1 age como o elemento identidade ($w1 = 1w = w$, para todo $w \in F$).

Cada palavra reduzida não vazia é da forma $(x_1^{\lambda_1}, x_2^{\lambda_2}, \dots, x_n^{\lambda_n}, 1, 1, \dots)$, onde $n \in \mathbb{N}^*$, $x_i \in X$ e $\lambda_i = \pm 1$, (denotaremos x^1 por x , para todo $x \in X$). Cada palavra será denotada por $x_1^{\lambda_1} \dots x_n^{\lambda_n}$. Observamos também que duas palavras reduzidas $x_1^{\lambda_1} \dots x_n^{\lambda_n}$ e $y_1^{\delta_1} \dots y_m^{\delta_m}$ ($x_i, y_i \in X; \lambda_i, \delta_i = \pm 1$) são iguais se e somente se são a palavra vazia ou $m = n$ e $x_i = y_i, \lambda_i = \delta_i$, para cada $i = 1, 2, \dots, n$. Denotamos o conjunto de todas as palavras reduzidas em X por $F(X)$. A função de $X \rightarrow F(X)$ dada por $x \rightarrow x^{-1}$ é injetiva, identificaremos X com a sua imagem, considerando X como um conjunto de $F(X)$.

Definiremos agora uma operação binária em $F(X)$. Informalmente gostaríamos que o produto de palavra reduzidas não vazias fosse dado por justaposição isto é,

$$(x_1^{\lambda_1} \dots x_m^{\lambda_m})(y_1^{\delta_1} \dots y_n^{\delta_n}) = x_1^{\lambda_1} \dots x_m^{\lambda_m} y_1^{\delta_1} \dots y_n^{\delta_n}.$$

Infelizmente a palavra do lado direito da equação pode não ser reduzida, (por exemplo, se $x_m^{\lambda_m} = y_1^{-\delta_1}$). Então definiremos o produto por justaposi-

ção e se necessário, cancelaremos os termos da forma xx^{-1} ou $x^{-1}x$; por exemplo $(x_1^1 x_2^{-1} x_3^1 x_4^{-1})(x_4^1 x_3^{-1} x_5^1 x_1^1) = x_1^1 x_2^{-1} x_5^1 x_1^1$.

Assim, se as palavras $x_1^{\lambda_1} \dots x_m^{\lambda_m}$ e $y_1^{\delta_1} \dots y_n^{\delta_n}$ estão em X , com $m \leq n$, seja k o maior inteiro ($0 \leq k \leq m$), tal que $x_{m-j}^{\lambda_{m-j}} = y_{j+1}^{-\delta_{j+1}}$, para $j = 0, 1, \dots, k-1$. Definimos então

$$(x_1^{\lambda_1} \dots x_m^{\lambda_m})(y_1^{\delta_1} \dots y_n^{\delta_n}) = \begin{cases} x_1^{\lambda_1} \dots x_{m-k}^{\lambda_{m-k}} y_{k+1}^{\delta_{k+1}} \dots y_n^{\delta_n} & \text{se } k < m; \\ y_{m+1}^{\delta_{m+1}} \dots y_n^{\delta_n} & \text{se } k = m < n; \\ 1 & \text{se } k = m = n. \end{cases}$$

Pela definição, temos que o produto de palavras reduzidas é uma palavra reduzida.

Teorema 1.27 *Se X é um conjunto não vazio e $F = F(X)$ é o conjunto de todas as palavras reduzidas em X , então, F é um grupo com a operação binária definida acima.*

Demonstração. Como 1 é o elemento identidade e $x_1^{\delta_1} \dots x_n^{\delta_n}$ tem inversa $x_1^{-\delta_1} \dots x_n^{-\delta_n}$, só nos resta provar a associatividade. Para cada $x \in X$ e $\delta = \pm 1$ seja $|x^\delta|$ a função $F \rightarrow F$ dada por $1 \mapsto x^\delta$ e

$$x_1^{\delta_1} \dots x_n^{\delta_n} = \begin{cases} x^\delta x_1^{\delta_1} \dots x_n^{\delta_n} & \text{se } x^\delta \neq x_1^{\delta_1}; \\ x_2^{\delta_2} \dots x_n^{\delta_n} & \text{se } x^\delta = x_1^{-\delta_1} (= 1 \text{ se } n = 1). \end{cases}$$

Como $|x| |x^{-1}| = 1_F = |x^{-1}| |x|$, cada $|x^\delta|$ é uma permutação bijetiva de F com inversa $|x^{-\delta}|$. Seja $A(F)$ o grupo de todas permutações de F e F_0 o subgrupo gerado por $\{|x| \mid x \in X\}$. A função $\varphi : F \rightarrow F_0$ dada por $1 \mapsto 1_F$ e $x_1^{\delta_1} \dots x_n^{\delta_n} \mapsto |x_1^{\delta_1}| \dots |x_n^{\delta_n}|$ é sobrejetiva, tal que $\varphi(w_1 w_2) = \varphi(w_1) \varphi(w_2)$ para todo $w_i \in F$. Como $1 \mapsto x_1^{\delta_1} \dots x_n^{\delta_n}$ de acordo como a função $|x_1^{\delta_1}| \dots |x_n^{\delta_n}|$, e segue que φ é injetiva. O fato de F_0 ser um grupo implica a associatividade em F e que φ é um isomorfismo de grupos. \square

O grupo $F = F(X)$ é um **grupo livre em X** .

Teorema 1.28 *Seja F o grupo livre em um conjunto X e $\iota : X \rightarrow F$ a função inclusão. Se G é um grupo e $f : X \rightarrow G$ uma função de conjuntos, então existe um único homomorfismo de grupos $\tilde{f} : F \rightarrow G$ tal que $\tilde{f} \iota = f$. Em outras palavras, F é um objeto livre no conjunto X , na categoria de grupos \mathcal{G} .*

O teorema diz que o diagrama abaixo comuta.

$$\begin{array}{ccc} X & \xrightarrow{\iota} & F \\ & \searrow f & \nearrow \tilde{f} \\ & & G \end{array}$$

Demonstração. Definimos $\bar{f}(1) = e$ e se $x_1^{\delta_1} \dots x_n^{\delta_n}$ é uma palavra reduzida em X , não vazia, $\bar{f}(x_1^{\delta_1} \dots x_n^{\delta_n}) = f(x_1)^{\delta_1} \dots f(x_n)^{\delta_n}$. Como G é um grupo e $\delta_i = \pm 1$, o produto $f(x_1)^{\delta_1} \dots f(x_n)^{\delta_n}$ é um elemento bem definido de G . Verifica-se que \bar{f} é um homomorfismo de grupos tal que $\bar{f} \iota = f$. Se $g : F \rightarrow G$ é um homomorfismo tal que $g \iota = f$, então, $g(x_1^{\delta_1} \dots x_n^{\delta_n}) = g(x_1^{\delta_1}) \dots g(x_n^{\delta_n}) = g(x_1)^{\delta_1} \dots g(x_n)^{\delta_n} = g \iota(x_1)^{\delta_1} \dots g \iota(x_n)^{\delta_n} = f(x_1)^{\delta_1} \dots f(x_n)^{\delta_n} = \bar{f}(x_1^{\delta_1} \dots x_n^{\delta_n})$. Portanto \bar{f} é único. \square

Corolário 1.29 Cada grupo G é imagem homomórfica de um grupo livre.

Demonstração. Seja X um conjunto de geradores de G e seja F o grupo livre no conjunto X . Pelo teorema 1.28 a função inclusão $X \rightarrow G$ induz um homomorfismo $\bar{f} : F \rightarrow G$ tal que $x \mapsto x$ com $x \in G$. Como $G = \langle X \rangle$, a prova do teorema 1.28 mostra que \bar{f} é um epimorfismo. \square

1.5.2 Apresentação Finita de um Grupo

Definição 1.30 Seja A um subconjunto de G . O fecho normal de A em G , denotado por $\langle A^G \rangle$ é a intersecção de todos os subgrupos normais de G que contêm A .

Usaremos nesta seção a seguinte notação, X é um conjunto, $F = F(X)$ é o grupo livre em X , R é um subconjunto de F , $N = \bar{R}$ é o fecho normal de R em F , G é o grupo quociente F/N . As definições foram retiradas de [13].

Definição 1.31 Com a notação acima, escrevemos $G = \langle X | R \rangle$ e chamamos uma **apresentação livre**, ou simplesmente uma **apresentação** de G . Os elementos de X são chamados **geradores** e R são chamados **relações**. Um grupo G é chamado **finitamente apresentado** se ele tem uma apresentação com ambos X e R conjuntos finitos.

Exemplo 1.32 $\langle X | \rangle$ é uma apresentação de um grupo livre de ordem $|X|$.

Exemplo 1.33 A apresentação

$$\langle x, y | x^3, y^2, x^{-1}y^{-1}xy \rangle,$$

é uma apresentação para o grupo simétrico de ordem 6.

Exemplo 1.34 A apresentação

$$D_8 = \langle x, y | x^4, y^2, (xy)^2 \rangle,$$

é uma apresentação para o grupo diedral 8.

Exemplo 1.35 *A apresentação*

$$D_{2n} = \langle x, y \mid x^{2n}, y^2, y^{-1}xyx \rangle,$$

é uma apresentação para o grupo diedral $2n$.

1.5.3 Sequências Exatas

Definição 1.36 *Um par de homomorfismo de módulos $A \xrightarrow{f} B \xrightarrow{g} C$ é exata em B se $\text{Im} f = \text{Ker} g$. Uma sequência finita de homomorfismos de módulos, $A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \xrightarrow{f_3} \dots \xrightarrow{f_{n-1}} A_{n-1} \xrightarrow{f_n} A_n$ é exata se $\text{Im} f_i = \text{Ker} f_{i+1}$ para $i = 1, 2, \dots, n$. Uma sequência infinita de homomorfismo de módulos, $\dots \xrightarrow{f_{i-1}} A_0 \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \dots$ é exata se $\text{Im} f_i = \text{Ker} f_{i+1}$, para todo $i \in \mathbb{Z}$.*

Observação 1.37 *Quando conveniente, abusaremos da linguagem e usaremos uma sequência de módulos em vez de uma sequência de homomorfismos de módulos.*

Exemplo 1.38 *Seja R um anel. Dados R -módulos A e C temos a soma direta $B = A \oplus C$ e a sequência*

$$0 \longrightarrow A \xrightarrow{\iota} A \oplus C \xrightarrow{\pi} C \longrightarrow 0$$

onde $\iota(a) = (a, c)$ e $\pi(a, c) = c$ é uma sequência exata.

Exemplo 1.39 *Dados os \mathbb{Z} -módulos \mathbb{Z} e $\mathbb{Z}/n\mathbb{Z}$ e a sequência*

$$0 \longrightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

onde n denota a função $x \mapsto nx$, e π denota a projeção natural.

A sequência $0 \longrightarrow A \xrightarrow{f} B$ é uma sequência exata de homomorfismos de R -módulos se, e somente se, f é um monomorfismo de módulos. Similarmente, $B \xrightarrow{g} C \longrightarrow 0$ é exata se, e somente se, g é um epimorfismo. Se $A \xrightarrow{f} B \xrightarrow{g} C$ é exata, então $gf = 0$. Finalmente, se $A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ exata, então $\text{Coker} f = B/\text{Im} f = B/\text{Ker} g = \text{CoIm} g \cong C$.

Definição 1.40 *Uma sequência exata da forma $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ é chamada **sequência exata curta**; note que f é um monomorfismo e g um epimorfismo.*

Teorema 1.41 *Seja R um anel e $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ uma seqüência exata de R -módulos, então para cada R -módulo D*

$$0 \longrightarrow \text{hom}_R(D, A) \xrightarrow{\bar{\varphi}} \text{hom}_R(D, B) \xrightarrow{\bar{\psi}} \text{hom}_R(D, C)$$

é uma seqüência exata de grupos abelianos.

Demonstração. Para demonstrar o teorema devemos mostrar que:

- (i) $\text{Ker } \bar{\varphi} = 0$ (ou seja, $\bar{\varphi}$ é um monomorfismo);
- (ii) $\text{Im } \bar{\varphi} \subset \text{Ker } \bar{\psi}$;
- (iii) $\text{Ker } \bar{\psi} \subset \text{Im } \bar{\varphi}$.

De fato,

(i) Seja $f \in \text{Ker } \bar{\varphi}$, então $\varphi f = 0$, implicando que $\varphi f(x) = 0$ para todo $x \in D$. Como $0 \longrightarrow A \xrightarrow{\varphi} B$ é exata, φ é um monomorfismo, onde $f(x) = 0$ para todo $x \in D$ e $f = 0$, portanto, $\text{Ker } \bar{\varphi} = 0$.

(ii) Por hipótese $\text{Im } \varphi = \text{Ker } \psi$, implicando que $\psi \varphi = 0$ e daí $\bar{\psi} \bar{\varphi} = 0$, portanto $\text{Im } \bar{\varphi} \subset \text{Ker } \bar{\psi}$.

(iii) Se $g \in \text{Ker } \bar{\psi}$, implica que $\psi g = 0$, daí $\text{Im } g \subset \text{Ker } \psi = \text{Im } \varphi$. Como φ é um monomorfismo, $\varphi : A \rightarrow \text{Im } \varphi$ é um isomorfismo. Se h é a composição $D \xrightarrow{g} \text{Im } g \xrightarrow{\varphi^{-1}} A$, onde $\text{Im } g \subset \text{Im } \varphi$, então $h \in \text{hom}_R(D, A)$ e $g = \varphi h = \bar{\varphi}(h)$, portanto, $\text{Ker } \bar{\psi} \subset \text{Im } \bar{\varphi}$. \square

Definição 1.42 *Uma seqüência exata curta de homomorfismos de R -módulos $0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$ é uma seqüência exata **split** se existe uma plicação $j : C \rightarrow B$ tal que $pj = 1_C$.*

Teorema 1.43 *Seja R um anel. A seqüência $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$ é uma seqüência exata de R -módulos se, e somente se,*

$$0 \longrightarrow \text{hom}_R(D, A) \xrightarrow{\bar{\varphi}} \text{hom}_R(D, B) \xrightarrow{\bar{\psi}} \text{hom}_R(D, C) \longrightarrow 0 \quad (1-1)$$

é uma seqüência exata split de grupos abelianos para cada R -módulo D .

Demonstração. Pela definição de seqüência exata split, existe um homomorfismo f de B em A tal que $f\varphi = 1_A$, e temos o homomorfismo

$$\bar{f} : \text{hom}_R(D, B) \rightarrow \text{hom}_R(D, A)$$

tal que $\overline{\varphi}f = 1_{\text{hom}_R(D,A)}$, conseqüentemente $\overline{\varphi}$ é um epimorfismo, e a seqüência (1-1) é uma seqüência exata de grupos abelianos pelo teorema 1.41, logo é uma seqüência exata split.

Reciprocamente, se $D = A$ e f de B em A é tal que $1_A = \overline{\varphi}(f) = f\varphi$, então φ é um R -monomorfismo, e $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$ é uma seqüência exata split pelo teorema 1.41. \square

1.6 Produto Tensorial

O produto tensorial $A \otimes_R B$ de módulos A_R e ${}_R B$ sobre um anel R é um grupo abeliano que tem papel importante no estudo de álgebras multilineares. É freqüentemente útil olhar o produto tensorial $A \otimes_R B$ como um objeto universal em uma certa categoria. Por outro lado, é também conveniente considerar $A \otimes_R B$ como uma espécie de noção dual para o $\text{hom}_R(A, B)$.

1.6.1 Construção de um Produto Tensorial

Se A_R e ${}_R B$ são módulos sobre um anel R , e C é um grupo abeliano aditivo, então a **função bi-aditiva linear** de $A \times B$ para C é uma função $f : A \times B \rightarrow C$ tal que se $a, a_i \in A$; $b, b_i \in B$ e $r \in R$:

$$f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b) \quad (1-2)$$

$$f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2) \quad (1-3)$$

$$f(ra, b) = rf(a, b) = f(a, rb) \quad (1-4)$$

Fixados A_R e ${}_R B$ consideremos a categoria $\mathcal{M}(A, B)$ onde os objetos são funções bi-aditivas lineares em $A \times B$. Pela definição, um morfismo em $\mathcal{M}(A, B)$ da função bi-aditiva linear $f : A \times B \rightarrow C$ para a função bi-aditiva linear $g : A \times B \rightarrow D$ é um homomorfismo de grupos $h : C \rightarrow D$ tal que o diagrama comuta:

$$\begin{array}{ccc} & & C \\ & \nearrow f & \downarrow h \\ A \times B & & D \\ & \searrow g & \end{array}$$

Então, $\mathcal{M}(A, B)$ é uma categoria, que 1_C é o morfismo identidade de f em f , e que h é uma equivalência em $\mathcal{M}(A, B)$ se, e somente se, h é um isomorfismo de grupos.

Definição 1.44 *Seja A um módulo a direita e B um módulo a esquerda sobre um anel R . Seja F o grupo abeliano livre sobre o conjunto $A \times B$. Seja H o subgrupo de F gerado por todos os elementos da seguinte forma para todo $a, a' \in A; b, b' \in B; r \in R$*

$$(i) (a + a', b) - (a, b) - (a', b);$$

$$(ii) (a, b + b') - (a, b) - (a, b');$$

$$(iii) (ar, b) - (a, rb)$$

*O grupo quociente F/H é chamado o **produto tensorial** de A e B ; é denotado por $A \otimes_R B$ (ou simplesmente $A \otimes B$ se $R = \mathbb{Z}$). A classe lateral $(a, b) + X$ de elementos $(a, b) \in F$ será denotada por $a \otimes b$; a classe lateral de $(0, 0)$ é denotada por 0 .*

Como F é gerado pelo conjunto $A \times B$, o quociente $F/H = A \otimes_R B$ é gerado por todos os elementos da forma $a \otimes b$ ($a \in A, b \in B$).

Um elemento de F é uma soma $\sum_{i=1}^r n_i(a_i, b_i)$ ($n_i \in \mathbb{Z}, a_i \in A, b_i \in B$), daí a classe lateral em $A \otimes_R B = F/H$ é da forma $\sum_{i=1}^r n_i(a_i \otimes b_i)$.

A definição 1.44 implica que os geradores $a \otimes b$ de $A \otimes_R B$ satisfazem as seguintes relações (para todo $a, a_i \in A, b, b_i \in B$, e $r \in R$):

$$(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b; \quad (1-5)$$

$$a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2; \quad (1-6)$$

$$ar \otimes b = a \otimes rb. \quad (1-7)$$

Dado um anel R e módulos ${}_R A$ e ${}_R B$, a função $i : A \times B \rightarrow A \otimes_R B$ dada por $(a, b) \mapsto a \otimes b$ é uma função bi-aditiva linear. A função i é chamada **a função bi-aditiva linear canônica**.

Teorema 1.45 *Sejam ${}_R A$ e ${}_R B$ módulos sobre um anel R , e seja C um grupo abeliano. Se $g : A \times B \rightarrow C$ é uma função bi-aditiva linear, então existe um único homomorfismo $\bar{g} : A \otimes_R B \rightarrow C$ tal que $\bar{g}i = g$, onde $i : A \times B \rightarrow A \otimes_R B$ é a função bi-aditiva linear canônica. $A \otimes_R B$ é univocamente determinado a menos de isomorfismos, por esta propriedade. Em outras palavras $i : A \times B \rightarrow A \otimes_R B$ é universal na categoria $\mathcal{M}(A, B)$ de todas as funções bi-aditivas lineares em $A \times B$. O teorema diz que o seguinte diagrama comuta:*

$$\begin{array}{ccc}
 A \times B & \xrightarrow{g} & C \\
 & \searrow f & \nearrow \bar{g} \\
 & A \otimes_R B &
 \end{array}$$

Demonstração. Seja F o grupo abeliano livre no conjunto $A \times B$, e seja H o subgrupo descrito na definição 1.44. Como F é livre, a aplicação $(a, b) \mapsto g(a, b) \in C$ determina um único homomorfismo $g_1 : F \rightarrow C$. Usando o fato que g é bi-aditiva linear, mostramos que a função g_1 leva cada gerador de K em 0. Daí $K \subset \ker g_1$. Temos que g_1 induz um homomorfismo $\bar{g} : F/H \rightarrow C$ (ver **teorema 1.7**, pag.172 de [11]) tal que $\bar{g}[(a, b) + K] = g_1(a, b) = g(a, b)$. Porém $F/H = A \otimes_R B$ e $(a, b) + K = a \otimes b$. Portanto, $\bar{g} : A \otimes_R B \rightarrow C$ é um homomorfismo tal que $\bar{g}i(a, b) = \bar{g}(a \otimes b) = g(a, b)$ para todo $(a, b) \in A \times B$; que é $\bar{g}i = g$. Se $h : A \otimes_R B \rightarrow C$ é algum homomorfismo com $hi = g$, então para todo gerador $a \otimes b$ de $A \otimes_R B$,

$$h(a \otimes b) = hi(a, b) = g(a, b) = \bar{g}i(a, b) = \bar{g}(a \otimes b).$$

Como h e \bar{g} são homomorfismos que agem nos geradores de $A \otimes_R B$, temos $h = \bar{g}$, onde \bar{g} é único. Isto prova que $i : A \times B \rightarrow A \otimes_R B$ é um objeto universal na categoria $\mathcal{M}(A, B)$, e $A \otimes_R B$ é univocamente determinado a menos de isomorfismos. \square

Corolário 1.46 Se $A_R, A'_R, {}_R B$ e ${}_R B'$ são módulos sobre o anel R e $f : A \rightarrow A', g : B \rightarrow B'$ são homomorfismos de R -módulos, então existe um único homomorfismo de grupos $A \otimes_R B \rightarrow A' \otimes_R B'$ tal que $a \otimes b \mapsto f(a) \otimes g(b)$ para todo $a \in A, b \in B$.

Demonstração. A aplicação $(a, b) \mapsto f(a) \otimes g(b)$ define uma função bi-aditiva linear $h : A \times B \rightarrow C = A' \otimes_R B'$. Pelo teorema 1.45 existe um único homomorfismo $\bar{h} : A \otimes_R B \rightarrow A' \otimes_R B'$ tal que $\bar{h}(a \otimes b) = \bar{h}i(a, b) = h(a, b) = f(a) \otimes g(b)$ para todo $a \in A, b \in B$. \square

Teorema 1.47 Sejam R e S anéis e ${}_S A_R, {}_R B, {}_C R, {}_R D_S$ bi-módulos como indicados. $A \otimes_R B$ é um S -módulo tal que $s(a \otimes b) = sa \otimes b$ para todo $s \in S, a \in A, b \in B$.

Demonstração.

Para cada $s \in S$ a função $A \times B \rightarrow A \otimes_R B$ dada por $(a, b) \mapsto sa \otimes b$ é R -bi-aditiva linear, e portanto existe um único homomorfismo de grupos $\alpha_s : A \otimes_R B \rightarrow A \otimes_R B$ tal que $\alpha_s(a \otimes b) = sa \otimes b$. Para cada elemento $u = \sum_{i=1}^n a_i \otimes b_i \in A \otimes_R B$ definimos su como o

elemento $\alpha_s(u) = \sum_{i=1}^n \alpha_s(a_i \otimes b_i) = \sum_{i=1}^n sa_i \otimes b_i$. Como α_s é um homomorfismo de grupos, a ação de S é bem definida e $A \otimes_R B$ é um S -módulo a esquerda. \square

Um caso especial do teorema 1.47 ocorre quando R é um anel comutativo e cada R -módulo A é um $R - R$ bi-módulo com $ra = ar$ ($r \in R, a \in A$). Neste caso $A \otimes_R B$ é também um $R - R$ bi-módulo com

$$r(a \otimes b) = ra \otimes b = ar \otimes b = a \otimes rb = a \otimes br = (a \otimes b)r$$

para todo $r \in R, a \in A, b \in B$.

Se R é um anel comutativo, então o produto tensorial de R -módulos pode ser caracterizado por uma variação do teorema 1.45. Sejam A, B, C módulos sobre um anel comutativo R . Uma **função bilinear** de $A \times B$ em C é uma função $f : A \times B \rightarrow C$ tal que para todo $a, a_i \in A; b, b_i \in B$ e $r \in R$

$$f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b); \quad (1-8)$$

$$f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2); \quad (1-9)$$

$$f(ra, b) = rf(a, b) = f(a, rb). \quad (1-10)$$

Exemplo 1.48 Se A e B são módulos sobre um anel comutativo R , então $A \otimes_R B$ é um R -módulo e a função bi-aditiva linear canônica $i : A \times B \rightarrow A \otimes_R B$ é bilinear.

Teorema 1.49 Se A, B, C são módulos sobre um anel comutativo R e $g : A \times B \rightarrow C$ é uma função bilinear, então existe um único homomorfismo de R -módulo $\bar{g} : A \otimes_R B \rightarrow C$ tal que $\bar{g}i = g$ onde $i : A \times B \rightarrow A \otimes_R B$ é a função bilinear canônica. O módulo $A \otimes_R B$ é univocamente determinado a menos de isomorfismos por esta propriedade.

O teorema diz que o diagrama é comutativo:

$$\begin{array}{ccc} A \times B & \xrightarrow{g} & C \\ & \searrow i & \nearrow \bar{g} \\ & A \otimes_R B & \end{array}$$

Teorema 1.50 Se R é um anel com identidade e $A_R, {}_R B$ são R -módulos unitários, então existe um isomorfismo de R -módulos

$$A \otimes_R R \cong A \quad e \quad R \otimes_R B \cong B.$$

Demonstração. Como R é um R - R bi-módulo, $R \otimes_R B$ é um R -módulo a esquerda pelo teorema 1.47. A função $(r, b) \mapsto rb$ define uma função bi-aditiva linear $R \times B$ em B . Pelo teorema 1.45 existe um homomorfismo de grupos $\alpha : R \otimes_R B \rightarrow B$ tal que $\alpha(r \otimes b) = rb$. Verifica-se que α é de fato um homomorfismo de R -módulos a esquerda. Então temos que a função $\beta : B \rightarrow R \otimes_R B$ dada por $b \mapsto 1_R \otimes b$ é um homomorfismo de R -módulos tal que $\alpha\beta = 1_B$ e $\beta\alpha = 1_{R \otimes_R B}$. Daí, $\alpha : R \otimes_R B \cong B$. O isomorfismo $A \otimes_R R \cong A$ é mostrado similarmente. \square

Proposição 1.51 Se $A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ é uma seqüência exata de R -módulos à esquerda e D é um R -módulo, então

$$D \otimes_R A \xrightarrow{1_D \otimes f} D \otimes_R B \xrightarrow{1_D \otimes g} D \otimes_R C \longrightarrow 0$$

é uma seqüência exata de grupos abelianos.

Demonstração. Para demonstrar a proposição devemos mostrar que:

- (i) $Im(1_D \otimes g) = D \otimes_R C$;
- (ii) $Im(1_D \otimes f) \subset Ker(1_D \otimes g)$;
- (iii) $Ker(1_D \otimes g) \subset Im(1_D \otimes f)$.

De fato,

(i) Por hipótese g é um epimorfismo então cada gerador $d \otimes c$ de $D \otimes_R C$ é da forma $d \otimes g(b) = (1_D \otimes g)(d \otimes b)$ para algum $b \in B$. Assim $Im(1_D \otimes g)$ contém todos os geradores de $D \otimes_R C$, portanto $Im(1_D \otimes g) = D \otimes_R C$.

(ii) Como $Ker g = Im f$ temos $gf = 0$ e $(1_D \otimes g)(1_D \otimes f) = 1_D \otimes gf = 1_D \otimes 0 = 0$, portanto $Im(1_D \otimes f) \subset Ker(1_D \otimes g)$.

(iii) Seja $\pi : D \otimes_R B \rightarrow (D \otimes_R B)/Im(1_D \otimes f)$ o epimorfismo canônico. Por (ii) e pelo Primeiro Teorema do Isomorfismo existe um homomorfismo α de $(D \otimes_R B)/Im(1_D \otimes f)$ em $D \otimes_R C$ tal que $\alpha(\pi(d \otimes b)) = (1_D \otimes g)(d \otimes b) = d \otimes g(b)$. Iremos mostrar que α é um isomorfismo.

Mostraremos primeiramente que a função $\beta : D \times C \rightarrow (D \otimes_R B)/Im(1_D \otimes f)$ dada por $(d, c) \mapsto \pi(d \otimes b)$, onde $g(b) = c$, independe da escolha de b . Como g é um epimorfismo, se $g(b') = c$, então $g(b - b') = 0$ e $b - b' \in Ker g = Im f$, onde $b - b' = f(a)$ para todo $a \in A$. Como $d \otimes f(a) \in Im(1_D \otimes f)$ e $\pi(d \otimes f(a)) = 0$, temos

$$\pi(d \otimes b) = \pi(d \otimes b' + f(a)) = \pi(d \otimes b' + d \otimes f(a)) = \pi(d \otimes b' + \pi(d \otimes f(a))) = \pi(d \otimes b').$$

Portanto β é bem definida e β é bi-aditiva linear. Pelo teorema 1.45 existe $\bar{\beta} : D \otimes_R C \rightarrow (D \otimes_R B)/Im(1_D \otimes f)$ tal que $\bar{\beta}(d \otimes c) = \bar{\beta}i(d, c) = \beta(d, c) = \pi(d \otimes b)$, onde $g(b) = c$. Portanto, para algum gerador

$d \otimes c$ de $D \otimes_R C$, $\alpha\bar{\beta}(d \otimes c) = \alpha(\pi(d \otimes b)) = d \otimes g(b) = d \otimes c$, onde $\alpha\bar{\beta}$ é a função identidade. Analogamente, $\bar{\beta}\alpha$ é a identidade e α é um isomorfismo.

Este fato e o primeiro teorema do isomorfismo mostra que $\text{Ker}(1_D \otimes g) = \text{Im}(1_D \otimes f)$ e assim completamos a prova. \square

Exemplo 1.52 *Sejam os \mathbb{Z} -módulos, \mathbb{Z}_p e \mathbb{Z}_q , onde o máximo divisor comum entre p , q é 1. O $\mathbb{Z}_p \otimes \mathbb{Z}_q$ é um produto tensorial.*

1.7 Homologia e Complexos

Os conceitos básicos de álgebra homológica são os de “complexo” e de “homomorfismos de complexos” que definiremos a seguir.

Definição 1.53 *Se R é um anel, um **complexo** (C, d) para R é um conjunto de índices $C = \{C_i\}$ de R -módulos com $i \in \mathbb{Z}$, juntamente com um conjunto de índices $d = \{d_i \mid i \in \mathbb{Z}\}$ de R -homomorfismos $d_i : C_i \rightarrow C_{i-1}$ tais que $d_{i-1}d_i = 0$, para todo i . Se (C, d) e (C', d') são R -complexos, uma (cadeia) de homomorfismos de C em C' é um conjunto de indexado $\alpha = \{\alpha_i \mid i \in \mathbb{Z}\}$ de R -homomorfismos $\alpha_i : C_i \rightarrow C'_i$ tais que temos a comutatividade de*

$$\begin{array}{ccc} C_i & \xrightarrow{d_i} & C_{i-1} \\ \alpha_i \downarrow & & \downarrow \alpha_{i-1} \\ C'_i & \xrightarrow{d'_i} & C'_{i-1} \end{array}$$

para cada i . Ou seja, $\alpha d = d' \alpha$.

Exemplo 1.54 *Um R -módulo M é um complexo em que $C_i = M$, para todo $i \in \mathbb{Z}$, e $d_i : C_i \rightarrow C_{i-1}$ é identicamente nulo.*

Exemplo 1.55 *Uma sequência exata curta de R -módulos $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ define um complexo em que $C_i = 0$, $i \leq 0$, $C_1 = M''$, $C_2 = M$, $C_3 = M'$, $C_j = 0$ se $j > 3$, $d_2 = \beta$, $d_3 = \alpha$, $d_j = 0$ se $j \neq 2, 3$.*

Iremos agora definir para cada $i \in \mathbb{Z}$, um funtor, o i -ésimo funtor homomológico, da categoria de R -complexos na categoria de R -módulos. Seja (C, d) um complexo e seja $Z_i(C) = \text{Ker } d_i$, assim $Z_i(C)$ é um submódulo de C_i . Os elementos de Z_i são chamados i -ciclos. Como $d_i d_{i+1} = 0$, a imagem $d_{i+1} C_{i+1}$ que denotaremos por $B_i = B_i(C)$, é um submódulo de Z_i , e cada elemento é chamado i -bordos. O módulo $H_i = H_i(C) = Z_i/B_i$ é chamado o i -ésimo módulo homológico do complexo (C, d) .

Evidentemente, $C_{i+1} \xrightarrow{d_{i+1}} C_i \xrightarrow{d_i} C_{i-1}$ é exata se, e somente se, $H_i(C) = 0$ logo a sequência de homomorfismos infinita

$$\cdots \longleftarrow C_{i-1} \longleftarrow C_i \longleftarrow C_{i+1} \longleftarrow \cdots$$

é exata se, e somente se, $H_i(C) = 0$ para todo i .

1.7.1 Homotopia

Existe uma importante relação entre homomorfismos de complexos (\mathbf{C}, \mathbf{d}) em $(\mathbf{C}', \mathbf{d}')$ que garante que os correspondentes homomorfismos dos módulos de homologia são idênticos.

Definição 1.56 *Sejam α e β homomorfismos de um complexo (\mathbf{C}, \mathbf{d}) em um complexo $(\mathbf{C}', \mathbf{d}')$. Então α é **homotópico** a β se existe um conjunto indexado $s = \{s_i\}$ de homomorfismos de módulos $s_i : C_i \rightarrow C'_{i+1}$, $i \in \mathbb{Z}$, tal que*

$$\alpha_i - \beta_i = d'_{i+1}s_i + s_{i-1}d_i.$$

Se α e β são homotópicos, denotaremos $\alpha \sim \beta$.

1.8 Funtor Derivado

Definição 1.57 *Se \mathcal{C} e \mathcal{D} são categorias, então um **funtor covariante** $T : \mathcal{C} \rightarrow \mathcal{D}$, é uma função tal que:*

(i) *Se $A \in \text{obj}(\mathcal{C})$, então $T(A) \in \text{obj}(\mathcal{D})$;*

(ii) *Se $f : A \rightarrow A'$ em \mathcal{C} , então $T(f) : T(A) \rightarrow T(A')$ pertence a \mathcal{D} ;*

(iii) *Se $A \xrightarrow{f} A' \xrightarrow{g} A''$ em \mathcal{C} , então $T(A) \xrightarrow{T(f)} T(A') \xrightarrow{T(g)} T(A'')$ está em \mathcal{D} e*

$T(gf) = T(g)T(f)$;

(iv) *Para cada $A \in \text{obj}(\mathcal{C})$,*

$$T(1_A) = 1_{T(A)}.$$

Exemplo 1.58 *Se \mathcal{C} é uma categoria, então a **função identidade** $1_{\mathcal{C}} : \mathcal{C} \rightarrow \mathcal{C}$ definida por*

$$1_{\mathcal{C}}(A) = A \text{ para todo objeto } A,$$

e

$$1_{\mathcal{C}}(f) = f \text{ para todo morfismo } f.$$

Definir agora os funtores derivados de um funtor F da categoria $R\text{-mod}$ na categoria \mathbf{Ab} . Seja M um R -módulo e seja

$$0 \longleftarrow M \xleftarrow{\varepsilon} C_0 \xleftarrow{d_1} C_1 \xleftarrow{d_2} \dots$$

uma resolução projetiva de M . Aplicando o funtor F obtemos uma sequência de homomorfismos de grupos abelianos

$$0 \longleftarrow FM \xleftarrow{F(\varepsilon)} FC_0 \xleftarrow{F(d_1)} FC_1 \xleftarrow{F(d_2)} \dots \quad (1-11)$$

Temos que $F(0) = 0$ para o homomorfismo zero e o produto de homomorfismos sucessivos em (1-11) é 0 e assim $FC = \{FC_i\}$, $F(d) = \{F(d_i)\}$ onde a argumentação de $F\varepsilon$ é um complexo positivo sobre FM . Se F é exato, então a sequência (1-11) é exata e os grupos de homologia $H_i(FC) = 0$ para $i \geq 1$. Definimos agora

$$L_n FM = H_n(FC), \quad n \geq 0. \quad (1-12)$$

Em particular temos

$$H_0(FC) = FC_0 / F(d_1)FC_1. \quad (1-13)$$

Seja M' um segundo R -módulo e suponha que temos uma resolução projetiva $0 \longleftarrow M' \xleftarrow{\varepsilon'} C'_0 \xleftarrow{d'_1} C'_1 \dots$ de M' , e o grupo abeliano $H_n(FC')$, $n \geq 0$. Seja μ um homomorfismo de módulos de M em M' . Então temos um homomorfismo α do complexo (C, d) em (C', d') tal que $\mu\varepsilon = \varepsilon'\alpha_0$. Chamamos α o homomorfismo de cadeias sobre o dado homomorfismo μ . Como F é um funtor aditivo, temos o homomorfismo $F(\alpha)$ do complexo FC no complexo FC' tal que $F(\mu)F(\varepsilon) = F(\varepsilon')F(\alpha_0)$. Assim temos a comutatividade do diagrama,

$$\begin{array}{ccccccc} 0 & \longleftarrow & FM & \xleftarrow{F(\varepsilon)} & FC_0 & \xleftarrow{F(d_1)} & FC_1 & \longleftarrow & \dots \\ & & \downarrow F(\mu) & & \downarrow F(\alpha_0) & & \downarrow F(\alpha_1) & & \\ 0 & \longleftarrow & FM' & \xleftarrow{F(\varepsilon')} & FC'_0 & \xleftarrow{F(d'_1)} & FC'_1 & \longleftarrow & \dots \end{array}$$

e temos o homomorfismo $\widetilde{F(\alpha_n)}$ de $H_n(FC)$ em $H_n(FC')$. Este homomorfismo independe da escolha de α . Se β é um segundo homomorfismo de C em C' sobre μ , β é homotópico a α . Assim existem homomorfismos $s_n : C_n \rightarrow C'_{n+1}$, $n \geq 0$, tais que $\alpha_n - \beta_n = d'_{n+1}s_n + s_{n-1}d_n$. Como F é aditivo,

$$F(\alpha_n) - F(\beta_n) = F(d'_{n+1})F(s_n) + F(s_{n-1})F(d_n).$$

Assim $F(\alpha) \sim F(\beta)$ e $\widetilde{F(\alpha_n)} = \widetilde{F(\beta_n)}$.

Agora definimos $L_n F(\mu) = \widetilde{F(\alpha_n)}$. Assim um homomorfismo $\mu : M \rightarrow M'$ determina um homomorfismo $L_n F(\mu) : H_n(FC) \rightarrow H_n(FC')$. O funtor $L_n F$ definido por

$$(L_n F)M = H_n(FC), \quad M \in \text{ob } R\text{-mod}$$

$$(L_n F)(\mu) = \widetilde{F(\alpha_n)}, \quad \mu \in \text{hom}_R(M, M')$$

é um funtor aditivo de $R\text{-mod}$ em \mathbf{Ab} que é chamado o *n -ésimo funtor derivado à esquerda* de um dado funtor F .

Definição 1.59 O funtor derivado a esquerda do funtor $(M \otimes_R, -)$ é o funtor $Tor_n(M, -)$.

Segue a construção do funtor definido em 1.59:

1.8.1 Funtor Tor

Se $M \in R\text{-mod}$, a categoria de módulos à direita para o anel R , então $M \otimes_R$ é um funtor de $R\text{-mod}$ para \mathbf{Ab} e uma função R -módulos à esquerda N no grupo $M \otimes_R N$ e um elemento η do $\text{hom}_R(N, N')$ em $1 \otimes \eta$. $M \otimes_R$ é aditivo e exata à direita. A segunda condição significa que se $N' \rightarrow N \rightarrow N'' \rightarrow 0$ é exata, então $M \otimes N' \rightarrow M \otimes N \rightarrow M \otimes N'' \rightarrow 0$ é exata. A n -ésima derivada a esquerda do funtor de $M \otimes (= M \otimes_R)$ é denominada $Tor_n(M, -)$ ou $Tor_n^R(M, -)$. Para obter $Tor_n(M, N)$ escolhemos uma projeção resolutive de $N : 0 \leftarrow N \leftarrow^\varepsilon C_0 \leftarrow \dots$ e a forma da cadeia complexa $M \otimes C = \{M \otimes C_i\}$. Então $Tor_n(M, N)$ é a n -ésima homologia de grupos $H_n(M \otimes C)$ de $M \otimes C$. Por definição, $Tor_0(M, N) = (M \otimes C_0)/\text{im}(M \otimes C_1)$. Como $(M \otimes -)$ é exata à direita, $M \otimes C_1 \rightarrow M \otimes C_0 \rightarrow M \otimes N \rightarrow 0$ é exato e daí $M \otimes N \simeq (M \otimes C_0)/\text{im}(M \otimes C_1) = Tor_0(M, N)$.

O isomorfismo $Tor_0(M, N) \simeq M \otimes N$ e a sequência exata longa de homomorfismos implica que se $0 \rightarrow N' \rightarrow N \rightarrow N'' \rightarrow 0$ é exata, então

$$0 \leftarrow M \otimes N'' \leftarrow M \otimes N \leftarrow M \otimes N' \leftarrow Tor_1(M, N'') \leftarrow Tor_1(M, N) \leftarrow \dots$$

é exata.

1.9 Grupos de Homologia

Definiremos agora n -ésimo grupo de homologia de um grupo G . Em especial neste trabalho estamos interessados no segundo grupo de homologia de um grupo finitamente apresentado, $H_2(G, \mathbb{Z})$, que será detalhado no capítulo 4.

Apresentaremos posteriormente nas seções 1.10 e 2.2.2 exemplos de grupos de homologia. Esta seção foi fundamentada em [25].

Seja $U : \mathbf{Aneis} \rightarrow \mathbf{Grupos}$ um funtor que associa a cada anel R um grupo, de unidade $U(R)$. Seja $F : \mathbf{Grupos} \rightarrow \mathbf{Aneis}$ um funtor que associa cada grupo G seu grupo anel integral $\mathbb{Z}G$ e para cada homomorfismo de grupos $\varphi : G \rightarrow H$ o homomorfismo de anéis

$$\begin{aligned} F(\varphi) : \mathbb{Z}G &\longrightarrow \mathbb{Z}H \\ \sum_{x \in G} m_x x &\longmapsto \sum_{x \in G} m_x \varphi(x). \end{aligned}$$

Definição 1.60 *Seja G um grupo, seja A um G -módulo e seja \mathbb{Z} os inteiros visto como um G -módulo trivial. O n -ésimo grupo de homologia de G é definido por*

$$H_n(G, A) = \text{Tor}_n^{\mathbb{Z}G}(\mathbb{Z}, A).$$

Demonstraremos nesta seção o “teorema dos coeficientes universais” que será posteriormente usado na seção 4.1.1 do capítulo 4. Tal resultado pode ser encontrado em [3], que é uma demonstração mais simples e compacta que as convencionais.

A idéia central da demonstração do teorema dos coeficientes universais é expressar $\partial : C_n \rightarrow C_{n-1}$ como

$$\partial : C_n \longrightarrow \frac{C_n}{B_n} \longrightarrow \frac{C_n}{Z_n} \xrightarrow{\cong} B_{n-1} \xrightarrow{\subset} Z_{n-1} \xrightarrow{\subset} C_{n-1}. \quad (1-14)$$

Como $H_n = Z_n/B_n$, temos o a sequência exata

$$0 \longrightarrow B_n \xrightarrow{\subset} Z_n \longrightarrow H_n \longrightarrow 0, \quad (1-15)$$

para todo n . Como B_n e Z_n são subgrupos do grupo abeliano livre C_n , portanto são abelianos, e (1-15) é uma resolução livre de H_n .

Do diagrama (1-14) temos a sequência exata

$$0 \longrightarrow Z_n \xrightarrow{\subset} C_n \longrightarrow B_{n-1} \longrightarrow 0, \quad (1-16)$$

que é split por B_{n-1} ser abeliano livre. Usando (1-15) e (1-16) podemos reescrever a sequência exata canônica

$$0 \longrightarrow Z_n/B_n \xrightarrow{\subset} C_n/B_n \longrightarrow C_n/Z_n \longrightarrow 0, \quad (1-17)$$

como

$$0 \longrightarrow H_n \xrightarrow{\subset} C_n/B_n \xrightarrow{\bar{\partial}} B_{n-1} \longrightarrow 0. \quad (1-18)$$

Como B_{n-1} é abeliano livre, esta sequência exata curta é split, com homomorfismo split $s : B_{n-1} \rightarrow C_n/B_n$.

Lema 1.61 *Sejam os homomorfismos $f : K \rightarrow L$ $g : L \rightarrow M$ de grupos abelianos com homomorfismo split $s : L \rightarrow K$ tal que $f \circ s = id_L$. Então, temos a sequência exata split*

$$0 \longrightarrow Ker f \xrightarrow{\subset} Ker(g \circ f) \xrightarrow{f'} Ker g \longrightarrow 0, \tag{1-19}$$

onde $f' = f|_{Ker(g \circ f)}$, com split $s' = s|_{Ker g : Ker g \rightarrow Ker(g \circ f)}$.

Demonstração. A demonstração girará em torno do seguinte diagrama

$$\begin{array}{ccccc} & & s & & \\ & & \curvearrowright & & \\ K & \xrightarrow{f} & L & \xrightarrow{g} & M. \\ & & \curvearrowleft & & \\ & & f \circ g & & \end{array}$$

Notemos que f' e s' são definidos por $f(Ker(g \circ f)) \subset Ker g$ e $s(Ker g) \subset Ker(g \circ f)$. Isto é, se $l \in Ker g$, $(g \circ f)(sl) = gf(sl) = g(l) = 1_M$, assim, $sl \in Ker(g \circ f)$. Se $k \in Ker(g \circ f)$, $g \circ (fk) = gf(k) = 1_M$, assim $fk \in Ker g$. Então $f \circ s = id_L$, restringindo $f' \circ s' = id$. Como $Ker f \subset Ker(g \circ f)$, temos que $Ker f' = Ker f \cap Ker(g \circ f) = Ker f$. \square

Teorema 1.62 *Dado uma cadeia de complexos C em que cada C_n é abeliano livre, e um grupo G , temos para cada “n” a sequência exata curta*

$$0 \longrightarrow H_n(C) \otimes G \longrightarrow H_n(C \otimes G) \longrightarrow Tor(H_{n-1}(C), G) \longrightarrow 0, \tag{1-20}$$

que é split.

Demonstração. Fazendo o tensorial com G nas sequências acima e com (1-14), chegamos ao seguinte diagrama

$$\begin{array}{ccccccc} & & & & 0 & & (1-21) \\ & & & & \downarrow & & \\ & & & & H_n \otimes G & & \\ & & & & \downarrow & & \\ B_n \otimes G & \longrightarrow & C_n \otimes G & \longrightarrow & \frac{C_n}{B_n} \otimes G & \longrightarrow & 0 \\ & & & & \uparrow s \otimes id & \downarrow \bar{\partial} \otimes id & \\ 0 & \longrightarrow & Tor(H_{n-1}, G) & \longrightarrow & B_{n-1} \otimes G & \longrightarrow & Z_{n-1} \otimes G \\ & & & & \downarrow & \searrow & \downarrow \\ & & & & 0 & & C_{n-1} \otimes G \end{array}$$

ambas as seqüências verticais são exatas, pois (1-18) e (1-16) são split. As seqüências horizontais acima são exatas, por $(- \otimes G)$ é exato à direita. A seqüência horizontal de baixo é exata, por $Tor(H_{n-1}, G) = Ker[B_{n-1} \otimes G \rightarrow Z_{n-1} \otimes G]$ por definição.

Temos que $B_{n-1}(C \otimes G) = Im(\partial \otimes id) = Im[B_{n-1} \otimes G \rightarrow C_{n-1} \otimes G]$. Substituindo $n - 1$ por n , vemos que

$$B_n(C \otimes G) = Im[B_n \otimes G \rightarrow C_n \otimes G] = Ker[C_n \otimes G \rightarrow (C_n/B_n) \otimes G].$$

Então $(C_n \otimes G)/B_n(C \otimes G) \cong (C_n/B_n) \otimes G$. Também, $Z_n(C \otimes G) = Ker[C_n \otimes G \rightarrow Z_{n-1} \otimes G]$, e daí $(C_n \otimes G)/Z_n(C \otimes G) \cong Im[C_n \otimes G \rightarrow Z_{n-1} \otimes G] \subset Z_{n-1} \otimes G$.

Seguiremos usando a seqüência exata curta

$$0 \longrightarrow \frac{Z_n(C \otimes G)}{B_n(C \otimes G)} \xrightarrow{\subset} \frac{C_n \otimes G}{B_n(C \otimes G)} \longrightarrow \frac{C_n \otimes G}{Z_n(C \otimes G)} \longrightarrow 0,$$

para reescrever o n -ésimo grupo de homologia como

$$H_n(C \otimes G) = \frac{Z_n(C \otimes G)}{B_n(C \otimes G)} \cong Ker \left[\frac{C_n}{B_n} \otimes G \rightarrow Z_{n-1} \otimes G \right].$$

Aplicando o Lema 1.61 com $K = (C_n/B_n) \otimes G$, $L = B_{n-1} \otimes G$ e $M = Z_{n-1} \otimes G$, e usando como split $s \otimes id : L \rightarrow K$. No diagrama (1-21) identificamos $Ker[K \rightarrow L]$ com $H_n \otimes G$ e $Ker[L \rightarrow M]$ com $Tor(H_{i-1}, G)$. Esta identificação reduz a seqüência exata curta (1-19) na desejada (1-20). \square

1.9.1 Primeiro Grupo de Homologia

Mostraremos nesta seção que o primeiro grupo de homologia de um grupo G é isomorfo ao abelianizado de G . Tal resultado posteriormente será usado na seção 4.1 do capítulo 4. As definições e resultados apresentadas aqui podem ser encontradas em [25].

Definição 1.63 *A aplicação*

$$\begin{aligned} \varepsilon : \mathbb{Z}G &\longrightarrow \mathbb{Z} \\ \sum_{x \in G} m_x x &\longmapsto \sum_{x \in G} m_x, \end{aligned}$$

é chamada **aumento**, e $\mathcal{G} = Ker \varepsilon$ é chamado **ideal de aumento**.

Existe uma seqüência exata

$$0 \longrightarrow \mathcal{G} \longrightarrow \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0,$$

onde $\varepsilon : \mathbb{Z}G \longrightarrow \mathbb{Z}$ é definido por $\sum_{x \in G} m_x x \longmapsto \sum_{x \in G} m_x$. A aplicação ε é uma aplicação entre anéis e o $\text{Ker } \varepsilon = \mathcal{G}$ é um ideal bilateral em $\mathbb{Z}G$.

Lema 1.64 *Para qualquer grupo G , existe um isomorfismo*

$$H_1(G, \mathbb{Z}) \cong \mathcal{G}/\mathcal{G}^2.$$

Teorema 1.65 *Para qualquer grupo G , existe um isomorfismo*

$$H_1(G, \mathbb{Z}) \cong G/G'.$$

Demonstração. Como $H_1(G, \mathbb{Z}) \cong \mathcal{G}/\mathcal{G}^2$, pelo Lema 1.64 é suficiente provar que $\mathcal{G}/\mathcal{G}^2 \cong G/G'$.

Defina

$$\begin{aligned} \lambda : G &\longrightarrow \mathcal{G}/\mathcal{G}^2 \\ x &\longmapsto \lambda(x) = (x-1) + \mathcal{G}^2. \end{aligned}$$

Para ver que λ é um homomorfismo, note que

$$\begin{aligned} (x-1)(y-1) &= xy - y - x + 1 \\ &= xy - 1 - x + 1 - y + 1 \\ &= xy - 1 - (x-1) - (y-1), \end{aligned}$$

logo, $xy - 1 - (x-1) - (y-1) = (x-1)(y-1) \in \mathcal{G}^2$. Assim,

$$\begin{aligned} \lambda(xy) &= xy - 1 + \mathcal{G}^2 \\ &= (x-1) + (y-1) + (x-1)(y-1) + \mathcal{G}^2 \\ &= (x-1) + (y-1) + \mathcal{G}^2 \\ &= x - 1 + \mathcal{G}^2 + y - 1 + \mathcal{G}^2 \\ &= \lambda(x) + \lambda(y). \end{aligned}$$

Como $\mathcal{G}/\mathcal{G}^2$ é abeliano, $G' \leq \text{Ker } \lambda$. Temos que λ induz um homomorfismo

$$\begin{aligned} \lambda' : G/G' &\longrightarrow \mathcal{G}/\mathcal{G}^2 \\ xG' &\longmapsto \lambda(x) = (x-1) + \mathcal{G}^2. \end{aligned}$$

□

1.10 Grupos Abelianos Finitamente Gerados

Nesta seção apresentaremos um algoritmo para calcular a “forma normal Smith” de um grupo finitamente apresentado. Tal algoritmo também pode ser encontrado em [13] e é usado na seção 4.1 no capítulo 4.

Dado algum grupo G , recordemos que o grupo derivado (ou grupo comutador) é o grupo G' gerado por todos os comutadores $\{g^{-1}h^{-1}gh \mid g, h \in G\}$ de elementos de G . É claro que $G' \triangleleft G$ e que $G_{ab} := G/G'$ é abeliano. Além disso, G' é o menor subgrupo de G com esta propriedade (assim G_{ab} é o maior grupo quociente abeliano de G).
Notação: $X = \{x_1, x_2, \dots, x_r\}$, $C = \{[x_i, x_j] \mid 1 \leq i < j \leq r\}$, $r \in \mathbb{N}$.

Proposição 1.66 *Se $G = \langle X \mid R \rangle$, então $G_{ab} = \langle X \mid R, C \rangle$.*

Demonstração. Ver [13]. □

Exemplo 1.67 *Seja G um grupo dado pela apresentação*

$$\langle x, y, z, t \mid (xyz)^6 = e, t^2 = (xz)^2, (xy^3zt^2)^2 = e, (yt^2)^2 = x^2z^3, (xyz)^4(yt)^2 = e \rangle.$$

Então G_{ab} tem a apresentação

$$\langle x, y, z, t \mid (xyz)^6 = e, t^2 = (xz)^2, (xy^3zt^2)^2 = e, (yt^2)^2 = x^2z^3, (xyz)^4(yt)^2 = e,$$

$$[x, y] = [x, z] = [x, t] = [y, z] = [y, t] = [z, t] = e \rangle.$$

Em forma de comutadores, podemos operar as potências dos elementos das cinco primeiras relações e converter essas em relações para obter as seguintes formas mais convenientes:

$$\langle x, y, z, t \mid x^6y^6z^6, x^2z^2t^{-2}, x^2y^6z^2t^4, x^{-2}y^2z^{-3}t^4, x^4y^6z^4t^2,$$

$$[x, y], [x, z], [x, t], [y, z], [y, t], [z, t] \rangle.$$

A potência de cada gerador das cinco primeiras relações são definidas como as somas dos expoentes.

Definição 1.68 *O rank de um grupo G , denotado por $\text{rank}(G)$ é a cardinalidade do menor conjunto gerador de G , ou seja*

$$\text{rank}(G) = \min\{|X|; X \subset G, \langle X \rangle = G\}.$$

O grupo G_{ab} dado acima exemplo 1.67 é o grupo quociente A/B , onde $A = A(x, y, z, t)$ é um grupo livre de *rank* 4 e $B = \langle 6x + 6y + 6z, 2x + 2z - 2t, 2x + 6y + 2z + 4t, -2x + 2y - 3z + 4t, 4x + 6y + 4z + 2t \rangle$, com notação aditiva.

Neste caso, a matriz dos coeficientes é a seguinte

$$M = \begin{bmatrix} 6 & 6 & 6 & 0 \\ 2 & 0 & 2 & -2 \\ 2 & 6 & 2 & 4 \\ -2 & 2 & -3 & 4 \\ 4 & 6 & 4 & 2 \end{bmatrix}. \quad (1-22)$$

Descreveremos agora um técnica que usa $\langle F, R \rangle$ para calcular G_{ab} .

Definição 1.69 Uma matriz M $m \times n$, está na **Forma Normal Smith** se ela satisfaz as seguintes condições:

- i. $M_{ij} \neq 0$ quando $i \neq j$.
- ii. $M_{ii} \geq 0$ para $1 \leq i \leq \min(m, n)$.
- iii. Para $1 \leq i \leq \min(m, n)$ $M_{ii} | M_{i+1i+1}$.

Exemplo 1.70 A seguinte matriz está na forma normal Smith

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 24 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Apresentaremos um algoritmo para reduzir uma matriz M $r \times s$ sobre \mathbb{Z} , dos coeficientes de uma apresentação de um grupo à “forma normal Smit” e posteriormente ilustraremos com um exemplo. Observe a analogia existente com a eliminação Gaussiana.

Notação: P : Permutar linhas,

M : multiplicar uma linha por uma unidade (± 1),

A : adicionar a uma linha um múltiplo escalar de outra linha.

E o similar para colunas.

1. Escolha uma entrada d de M de módulo menor possível (se não existe um tal d , então M é a matriz nula, o mova para a posição $(1, 1)$ usando P).
2. Use a operação M para tornar $d > 0$.

3. Divida a entrada $(2, 1)$ por d e use uma operação A para substituí-lo por um b $0 \leq b < d$. Se $s = 1$ vá para a etapa 7.
4. Se $b = 0$ vá para a etapa 6, se não transponha as linha 1 e 2 e retorne a etapa 3, com b no lugar de d .
5. Repita as etapas 3 e 4 até que a entrada $(2, 1)$ seja 0 (no qual o novo valor de d na posição $(1, 1)$ será o maior fator comum das entradas $(1, 1)$ e $(2, 1)$ no início da etapa 3).
6. Desempenhe as etapas de 3 – 5 nas linhas remanescentes utilizando somente as entradas não nulas da primeira coluna e o d da entrada $(1, 1)$.
7. desempenhe as etapas de 3 – 6 nas colunas até que cada entrada da primeira linha seja zero exceto para d na entrada $(1, 1)$.
8. Se d divide cada entrada da matriz, vá para a etapa 11. Se não, use a operação P e uma operação A para obter b na entrada $(2, 1)$ com $d \nmid b$.
9. Repita as etapas de 3 – 5 utilizando somente as entradas não nulas da primeira coluna e o d na entrada $(1, 1)$ então retorne a etapa 7 com o novo d .
10. Repita as etapas 8 e 9 utilizando a entrada $(1, 1)$ $d = d_1$ dividindo as outras entradas da matriz.
11. Aplique as etapas de 1 – 10 na matriz obtida pela remoção da primeira linha e primeira coluna para obter um d_2 na entrada $(1, 1)$ que divide todas as outras entradas (e é divisível por d_1).
12. Repita a etapa 11 até que ou as linhas, colunas ou as entradas não nulas se esgotem.

Teorema 1.71 *Seja A um matriz $m \times n$ com entradas em \mathbb{Z} . Existe uma matriz inversível S $m \times m$ com entradas em \mathbb{Z} e uma matriz inversível T $n \times n$, tal que o produto SAT é uma matriz $m \times n$*

$$\begin{pmatrix} a_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & a_2 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & a_r & 0 & 0 \\ 0 & 0 & \cdots & 0 & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}.$$

Definição 1.72 *Os M_{ii} 's da definição da matriz na Forma Normal Smith são chamados fatores invariantes de M .*

Exemplo 1.73 Aplicaremos o algoritmo a matriz M apresentada em (1-22).

$$M = \begin{bmatrix} 6 & 6 & 6 & 0 \\ 2 & 0 & 2 & -2 \\ 2 & 6 & 2 & 4 \\ -2 & 2 & -3 & 4 \\ 4 & 6 & 4 & 2 \end{bmatrix}$$

Como o elemento de menor módulo positivo é 2, escolheremos o da entrada (2,1). A etapa 1 consiste da transposição das duas primeiras linhas, obtendo:

$$M = \begin{bmatrix} 2 & 0 & 2 & -2 \\ 6 & 6 & 6 & 0 \\ 2 & 6 & 2 & 4 \\ -2 & 2 & -3 & 4 \\ 4 & 6 & 4 & 2 \end{bmatrix}.$$

Desempenharemos as etapas de 2 – 6 para zerar os elementos da primeira coluna exceto o elemento da entrada (1,1) (quatro operações linhas do tipo A):

$$M = \begin{bmatrix} 2 & 0 & 2 & -2 \\ 0 & 6 & 6 & 0 \\ 0 & 6 & 0 & 6 \\ 0 & 2 & -1 & 2 \\ 0 & 6 & 0 & 6 \end{bmatrix}.$$

Aplice a etapa 7 para zerar os elementos da primeira linha exceto o elemento da entrada (1,1):

$$M = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 6 & 0 & 6 \\ 0 & 6 & 0 & 6 \\ 0 & 2 & -1 & 2 \\ 0 & 6 & 0 & 6 \end{bmatrix}.$$

Para a etapa 8, transponha as linhas 2 e 4; e então adicione a coluna 3 a coluna 1:

$$M = \begin{bmatrix} 2 & 0 & 0 & 0 \\ -1 & 2 & -1 & 2 \\ 0 & 6 & 0 & 6 \\ 0 & 6 & 0 & 6 \\ 0 & 6 & 0 & 6 \end{bmatrix}.$$

Para a etapa 9 adicione as linhas 1 a linha 2, então transponha as duas primeiras linhas, então subtraia as duas vezes a linha 1 da linha 2, e finalmente concluímos a primeira linha (etapa 7);

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -4 & 2 & -4 \\ 0 & 6 & 0 & 6 \\ 0 & 6 & 0 & 6 \\ 0 & 6 & 0 & 6 \end{bmatrix}.$$

Para o passo 11 aplique para a submatrix 4×3

$$M = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 6 & 6 \\ 0 & 6 & 6 \\ 0 & 6 & 6 \end{bmatrix}.$$

finalmente, aplique a etapa 12 à matrix 3×2

$$M = \begin{bmatrix} 6 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

M é assim reduzida a forma normal Smith

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Exemplo 1.74 Suponha que G tenha a apresentação

$$\langle F | R \rangle = \langle x, y, z | (xy)^2, (xz)^{-1}x^3, (xy^2z^{-1})^2 \rangle.$$

Então em notação aditiva temos

$$\langle x, y, z \mid 2x + 2y, 2x - z, 2x + 4x - 2z \rangle.$$

Portanto $G/[G, G]$ é o quociente de $F(x, y, z)$ pelo subgrupo gerado por

$$\{(2, 2, 0), (2, 0, -1), (2, 4, -2)\}.$$

Em forma matricial temos

$$M = \begin{bmatrix} 2 & 2 & 0 \\ 2 & 0 & -1 \\ 2 & 4 & -2 \end{bmatrix},$$

cuja Forma Normal Smith é dada por

$$M = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{bmatrix}.$$

E concluímos que $G/[G, G] \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$.

O Multiplicador de Schur

Neste capítulo trabalharemos com o Multiplicador de Schur, que é exatamente o segundo grupo de cohomologia de um grupo sobre C^* . Concluiremos este, com uma seção de exemplos que serão retomados no capítulo 4, usando um algoritmo computacional. Todas as definições e exemplos poderão ser encontrados em [15], [19], [23].

2.1 Grupos de Cohomologia

Nesta seção definiremos o segundo grupo de cohomologia de um grupo que será base para as seções posteriores.

Definição 2.1 *Se K e Q são grupos então uma **extensão de K por Q** é um grupo G tendo um subgrupo normal $K_1 \simeq K$ com $G/K_1 \simeq Q$.*

Em outras palavras se K e Q são grupos, uma extensão de K por Q é uma sequência exata curta

$$1 \longrightarrow K \longrightarrow G \longrightarrow Q \longrightarrow 1,$$

onde G é uma extensão de K por Q .

Exemplo 2.2 *O grupo S_3 é uma extensão de \mathbb{Z}_2 por \mathbb{Z}_3 .*

Definição 2.3 *Uma **extensão central** de K por Q é uma extensão G de K por Q com $K \leq Z(G)$.*

Exemplo 2.4 *O grupo Diedral 8 (\mathbb{D}_8) é uma extensão do grupo cíclico 2 (\mathbb{C}_2), pelo grupo de Klein (\mathbb{V}_4). E como $\mathbb{C}_2 \leq Z(\mathbb{V}_4)$, a extensão é central.*

Definição 2.5 *Se $K \leq G$, então um **transversal (direita)** de K em G (ou um conjunto completo de representantes de classes laterais a direita) é um subconjunto T de G contendo um elemento de cada classe lateral a direita de K em G .*

Definição 2.6 Se $\pi : G \rightarrow Q$ é sobrejetivo, então um **levantamento** de $x \in Q$ é um elemento $l(x) \in G$ com $\pi(l(x)) = x$.

Se escolhermos um levantamento $l(x)$ para cada $x \in Q$, então o conjunto de todos estes levantamentos é uma transversal do $\text{Ker } \pi$, pois, se $x \in Q$ e $l(x)$ é um levantamento para x temos

$$\pi(l(x)) = x \Leftrightarrow \pi(l) = 1_Q \Leftrightarrow l \in \text{Ker } \pi.$$

Neste caso a função $l : Q \rightarrow G$ é também chamado um transversal à direita (assim ambos l e $l(Q)$ são chamadas transversal a direita).

Teorema 2.7 [23]. Se G é uma extensão de K por Q e $l : Q \rightarrow G$ um transversal. Se K é abeliano, então existe um homomorfismo $\theta : Q \rightarrow \text{Aut}(K)$ com

$$\theta_x(a) = l(x) + a - l(x),$$

para cada $a \in K$. Mais ainda, se $l_1 : Q \rightarrow G$ é outra transversal, então $l(x) + a - l(x) = l_1(x) + a - l_1(x)$, para todo $a \in K$ e $x \in Q$.

Definição 2.8 Chamaremos a terna ordenada (Q, K, θ) de **data** se, K é um grupo abeliano, Q é um grupo e $\theta : Q \rightarrow \text{Aut}(K)$ é um homomorfismo. Dizemos que um grupo G satisfaz esta data se G é uma extensão de K por Q e, para cada transversal $l : Q \rightarrow G$, temos que

$$xa = \theta_x(a) = l(x) + a - l(x),$$

para todo $x \in Q$ e $a \in K$.

Sejam G e Q grupos e $\pi : G \rightarrow Q$ um homomorfismo sobrejetor com $\text{ker}(\pi) = K$ e escolha um transversal $l : Q \rightarrow G$ com $l(1) = 0$. Uma vez que a transversal foi escolhida, cada elemento $g \in G$ tem uma única expressão da forma

$$g = a + l(x), \quad a \in K, \quad x \in Q,$$

assim $l(x)$ é um representante da classe lateral de K em G , e G é a união disjunta dessas classes laterais. Existe uma fórmula, para todo $x, y \in Q$,

$$l(x) + l(y) = f(x, y) + l(xy), \quad \text{para algum } f(x, y) \in K, \quad (2-1)$$

por que ambos $l(x) + l(y)$ e $l(xy)$ representam a mesma classe lateral de K .

Definição 2.9 Se $\pi : G \rightarrow Q$ é um homomorfismo sobrejetor com kernel K e se $l : Q \rightarrow G$ é uma transversal com $l(1) = 0$, então a função $f : Q \times Q \rightarrow K$ definida por

$$l(x) + l(y) = f(x, y) + l(xy), \quad \text{para algum } f(x, y) \in K,$$

é chamado um **conjunto fator** (ou **cociclo**).

Observação 2.10 O conjunto fator f depende do transversal l .

Teorema 2.11 Seja $\pi : G \rightarrow Q$ um homomorfismo sobrejetor com kernel K , seja $l : Q \rightarrow G$ uma transversal com $l(1) = 0$, e seja $f : Q \times Q \rightarrow K$ o correspondente conjunto fator :

(i) para todo $x, y \in Q$

$$f(1, y) = 0 = f(x, 1);$$

(ii) O **cociclo identidade** se define para cada $x, y, z \in Q$ por :

$$f(x, y) + f(xy, z) = xf(y, z) + f(x, yz).$$

Demonstração.

(i) A definição de f nos diz que $l(x) + l(y) = f(x, y) + l(xy)$. Em particular, se $x = 1$

$$l(1) + l(y) = f(1, y) + l(y),$$

como $l(1) = 0$ temos, $l(y) = f(1, y) + l(y)$. Implicando que $f(1, y) = 0$. Da mesma forma se verifica que $f(x, 1) = 0$.

(ii) O cociclo identidade segue da associatividade

$$\begin{aligned} [l(x) + l(y)] + l(z) &= f(x, y) + l(xy) + l(z) \\ &= f(x, y) + f(xy, z) + l(xyz). \end{aligned}$$

por outro lado,

$$\begin{aligned} l(x) + [l(y) + l(z)] &= xf(y, z) + l(xy) + l(z) \\ &= xf(y, z) + f(xy, z) + l(xyz). \end{aligned}$$

Portanto, $f(x, y) + f(xy, z) = xf(y, z) + f(xy, z)$.

□

Teorema 2.12 Considere a data (Q, K, θ) . A função $f : Q \times Q \rightarrow K$ é um cociclo se, e somente se, ela satisfaz o cociclo identidade

$$xf(y, z) - f(xy, z) + f(x, yz) - f(x, y) = 0$$

bem como $f(1,y) = 0 = f(x,1)$ para todo $x, y, z \in Q$. Mais precisamente, existe uma extensão de G satisfazendo a data e uma transversal $l : Q \rightarrow G$ tal que f é o cociclo correspondente.

Demonstração. A implicação segue do teorema anterior.

Para mostrar a recíproca, seja G o conjunto de todos os pares ordenados $(a,x) \in K \times Q$ com a operação

$$(a,x) + (b,y) = (a + xb + f(x,y), xy).$$

A prova que G é um grupo pode ser encontrada no (teorema 7.22 página 270 de [23]). O cociclo identidade necessita ser associativo; a identidade é $(0,1)$; a inversa é dada por

$$-(a,x) = (-x^{-1}a - x^{-1}f(x,x^{-1},x^{-1})).$$

Defina

$$\begin{aligned} \pi : G &\longrightarrow Q \\ (a,x) &\longmapsto x. \end{aligned}$$

π é um homomorfismo sobrejetor com kernel $\{(a,1) : a \in K\}$. Identificamos K com $\ker \pi$ via $a \mapsto (a,1)$, então $K \triangleleft G$ e G é uma extensão de K por Q .

Verificaremos se G realiza esta data. Podemos mostrar para cada transversal $l : Q \rightarrow G$ que $xa = l(x) + a - l(x)$ para todo $x \in Q$ e $a \in K$. Podemos ter $l(x) = l(b,x)$ para algum $b \in K$. Portanto

$$\begin{aligned} l(x) + a - l(x) &= (b,x) + (a,1) - (b,x) \\ &= (b + xa, x) + (-x^{-1}b - x^{-1}f(x,x^{-1},x^{-1}), x^{-1}) \\ &= (b + xa + x[-x^{-1}b - x^{-1}f(x,x^{-1},x^{-1})] + f(x,x^{-1},1), 1) \end{aligned}$$

Como K é abeliano, o último termo se resume a $(xa,1)$. Como algum elemento de K , identificamos xa com $(xa,1)$, e assim G satisfaz a data.

Finalmente, definimos uma transversal $l : Q \rightarrow K$ por $l(x) = (0,x)$ para todo $x \in Q$. O conjunto fator F corresponde a esta transversal satisfaz $F(x,y) = l(x) + l(y) - l(xy)$. Por um cálculo simples mostramos que $F(x,y) = (f(x,y),1)$ e f é o conjunto fator como queríamos. \square

Notação: Denotaremos a extensão G construída na prova do teorema 2.12 por G_f ; ele satisfaz (Q, K, θ) e tem f como cociclo.

Definição 2.13 $Z^2(Q, K, \theta)$ é o conjunto de todos os cociclos $f : Q \times Q \rightarrow K$.

O teorema 2.12 mostra que $Z^2(Q, K, \theta)$ é um grupo abeliano em relação a adição $f + g : (x, y) \mapsto f(x, y) + g(x, y)$.

Definição 2.14 Dado a Data (Q, K, θ) , um **cobordo** é uma função $g : Q \times Q \rightarrow K$ tal que exista $h : Q \rightarrow K$ com $h(1) = 0$ tal que

$$g(x, y) = xh(x) - h(xy) + h(x).$$

O conjunto de todos os cobordos é denotado por $B^2(Q, K, \theta)$.

Temos que $B^2(Q, K, \theta)$ é um subgrupo de $Z^2(Q, K, \theta)$, isto é, cada cobordo g satisfaz o cociclo identidade e $g(x, 1) = 0 = g(1, x)$ para todo $x \in Q$.

Definição 2.15 Dada a data (Q, K, θ) , então

$$H^2(Q, K, \theta) = Z^2(Q, K, \theta) / B^2(Q, K, \theta)$$

é chamado o **segundo grupo de cohomologia da data**.

Definição 2.16 Duas extensões G e G' satisfazendo a data (Q, K, θ) são **equivalentes** se existe um conjunto fator f de G e f' de G' com $f' - f \in B^2(Q, K, \theta)$; isto é, o conjunto fator determina o mesmo elemento de $H^2(Q, K, \theta)$.

2.2 O Multiplicador de Schur

Quando θ é trivial, isto é, $\theta(x) = 1_K$ para todo $x \in Q$, então simplificaremos a notação e escreveremos $H^2(Q, K)$.

Definição 2.17 Se Q é um grupo, então seu **Multiplicador de Schur** é o grupo abeliano

$$M(Q) = H^2(Q, C^*),$$

onde C^* denota o grupo multiplicativo dos números complexos não nulos.

Como usamos notação multiplicativa para C^* também usamos notação multiplicativa para $M(Q)$. Assim, como θ é trivial, uma função $f : Q \times Q \rightarrow C^*$ é um cociclo se, e somente se, para todo $x, y \in Q$:

$$f(1, y) = 1 = f(x, 1);$$

$$f(x, y)f(xy, z)^{-1}f(x, yz)f(x, y)^{-1} = 1;$$

uma função $g : Q \times Q \rightarrow C^*$ é um cobordo se, e somente se, existe um função $h : Q \rightarrow C^*$ com $h(1) = 1$ tal que

$$g(x, y) = h(x)h(xy)^{-1}h(y).$$

Dois cociclos f e g são equivalentes se, e somente se, fg^{-1} é um cobordo.

Definição 2.18 Se G é um grupo finito, seu **expoente minimal**, denotado por $\exp(G)$, é o menor inteiro positivo e , tal que, $x^e = 1$, para todo $x \in G$.

Teorema 2.19 Se Q é um grupo finito, então $M(Q)$ é um grupo abeliano finito e $\exp(M(Q))$ divide $|Q|$.

Demonstração. Se $f : Q \times Q \rightarrow C^*$ é um cociclo, defina

$$\begin{aligned} \sigma : Q &\longrightarrow C^* \\ x &\longmapsto \sigma(x) = \prod_{z \in Q} f(x, z). \end{aligned}$$

Note que $\sigma(1) = 1$. Multiplicando o cociclo identidade

$$f(y, z)f(xy, z)^{-1}f(x, yz)f(x, y)^{-1} = 1$$

para todo $z \in Q$ obtemos

$$\sigma(y)\sigma(xy)^{-1}\sigma(x) = f(x, y)^n,$$

onde $n = |Q|$ (como z percorre todo Q , o mesmo ocorre com yz). Mas esta equação nos diz que $(fB^2(Q, C^*))^n = 1$, isto é, $M(Q)^n = 1$. Assim, o expoente mínimo de $M(Q)$ divide n quando Q é finito. Para o acaso $x \in Q$, defina $h : Q \rightarrow C^*$, escolhendo $h(1) = 1$ e $h(x)$ sendo alguma n -ésima raiz de $\sigma(x)^{-1} : h(x)^n = \sigma(x)^{-1}$. Defina $g : Q \times Q \rightarrow C^*$ por $g(x, y) = f(x, y)h(y)h(xy)^{-1}h(x)$. f e g são equivalentes pois diferem por um cobordo. Por outro lado,

$$\begin{aligned} g(x, y)^n &= f(x, y)^n h(y)^n h(xy)^{-n} h(x)^n \\ &= \sigma(y)\sigma(xy)^{-1}\sigma(x)\sigma(y)^{-1}\sigma(xy)\sigma(x)^{-1} = 1. \end{aligned}$$

Portanto, cada elemento $[f] \in M(Q)$ determina uma função $g : Q \times Q \rightarrow Z_n$, onde Z_n denota o subconjunto de C^* contendo todas as n -ésimas raízes da unidade. O resultado segue, por existir somente um número finito de tais funções. \square

Teorema 2.20 (Alperin-Kuo, 1967). Se Q é um grupo finito, $e = \exp(M(Q))$, e $e' = \exp(Q)$, então ee' divide $|Q|$.

Demonstração. Ver Teorema 7.68, página 210 de [23]. \square

2.2.1 Fórmula de Hopf

Hopf mostrou em 1942 que $H_2(X) \cong (R \cap F')/[F, R]$, onde X é um espaço topológico. Schur em 1907 provou que $M(G) \cong (R \cap F')/[F, R]$, onde G é finito. No capítulo 4 apresentaremos um algoritmo que dá uma estimativa do segundo grupo de homologia de um grupo finitamente apresentado G . Tal algoritmo usa a fórmula de Hopf que mostraremos nesta seção.

Lema 2.21 *Se G é grupo finito e*

$$1 \longrightarrow K \longrightarrow E \longrightarrow G \longrightarrow 1,$$

é uma extensão central, então $K \cap E'$ é finito.

Demonstração. Como a extensão é central, $K \leq Z(E)$, assim temos $[E : Z(E)] \leq [E : K] = |G| < \infty$. Daí $Z(E)$ tem índice finito em E e pelo teorema de Schur (teorema 1.1) temos que E' é finito. Portanto, $K \cap E' \leq E'$ que é finito. \square

Lema 2.22 *Se $G = F/R$ é um grupo finito, onde F é livre, então existe uma extensão central*

$$1 \longrightarrow R/[F, R] \longrightarrow F/[F, R] \longrightarrow G \longrightarrow 1.$$

Além disso, se F é finitamente gerado, então $R/[F, R]$ é também finitamente gerado.

Demonstração. Como $R \triangleleft F$, temos $[F, R] \leq R$, além disso, $[F, R] \triangleleft F$. Existe assim a sequência exata

$$1 \longrightarrow R/[F, R] \longrightarrow F/[F, R] \xrightarrow{\nu} F/R \longrightarrow 1,$$

que é uma extensão central. F ser finitamente gerado implica que $F/[F, R]$ é finitamente gerado. Como, G é finito, $R/[F, R] \leq F/[F, R]$ é um subgrupo de índice finito e assim o Teorema 1.2 mostra que $R/[F, R]$ é finitamente gerado. \square

Definição 2.23 *Se G é um grupo, seu subgrupo de torsão é definido por*

$$tG = \{x \in G : nx = 0, \text{ para algum inteiro no nulo } n\}.$$

Lema 2.24 *Seja $G = F/R$ um grupo finito, onde F é um grupo livre finitamente gerado. O subgrupo de torsão de $R/[F, R]$ é $(R \cap F')/[F, R]$, e existe um subgrupo S com $[F, R] \leq S \leq R$, com $S \triangleleft F$, e com*

$$R/[F, R] = (R \cap F')/[F, R] \oplus S/[F, R].$$

Demonstração. Ver lema 11.15, página 362, [23]. □

Lema 2.25 *Seja G um grupo finito com $G = F/R$, onde F é um grupo livre finitamente gerado. Então:*

(i) *Existe uma extensão central*

$$1 \longrightarrow K \longrightarrow E \longrightarrow G \longrightarrow 1,$$

com $K \leq E'$ e com $K \cong (R \cap F')/[F, R]$.

(ii) $|(R \cap F')/[F, R]| \leq |M(G)|$.

Demonstração.

(i) Escolha S como no lema 2.24, com $S \triangleleft F$, $[F, R] \leq S \leq R$ e $R/[F, R] = (R \cap F')/[F, R] \oplus S/[F, R]$. Considere a sequência exata

$$1 \longrightarrow R/S \longrightarrow F/S \longrightarrow G \longrightarrow 1.$$

Como $R/[F, R]$ é central em $F/[F, R]$, segue que $R/S \cong (R/[F, R])/(S/[F, R])$ é central em $F/S \cong (F/[F, R])/(S/[F, R])$; além disso, a definição de S nos dá $(R/[F, R])/(S/[F, R]) \cong (R \cap F')/[F, R]$. Finalmente, $R/S = (R \cap F')S/S \leq F'S/S = (F/S)'$.

□

O resultado seguinte é conhecido com a Fórmula de “Hopf”.

Teorema 2.26 (Schur, 1907). *Se G é um grupo com $G = F/R$, onde F é um grupo livre finitamente gerado, então*

$$M(G) \cong \frac{(R \cap F')}{[F, R]}.$$

Demonstração. Sejam

$$1 \longrightarrow L \longrightarrow U \xrightarrow{\pi} G \longrightarrow 1.$$

uma extensão central com $L \leq U'$, $\{y_1, \dots, y_n\}$ uma base de F , e $v : F \rightarrow G$ um homomorfismo sobrejetivo. Para todo i , escolha $u_i \in U$ com $\pi(u_i) = v(y_i)$. Como F é livre com base $\{y_1, \dots, y_n\}$, existe um homomorfismo $\sigma : F \rightarrow U$ com $\pi\sigma = v$. Temos que $L = L \cap U' \leq Z(U) \cap U' \leq \Phi(U)$, pelo teorema 1.8. Portanto,

$$U = \langle u_1, \dots, u_n, L \rangle \leq \langle u_1, \dots, u_n, \Phi(U) \rangle = \langle u_1, \dots, u_n \rangle,$$

pelo teorema 1.7, assim σ é sobrejetiva.

Se $a \in L$, então $a = \sigma(w)$ para algum $w \in F$ (por σ ser sobrejetiva), e assim $1 = \pi(a) = \pi\sigma(w) = v(w)$. Dai, $w \in \ker(v) = R$, assim $a = \sigma(w) \in \sigma(R)$; isto é, $L \leq \sigma(R)$. Para a inclusão reversa, se $r \in R$, então $\pi\sigma(r) = v(r) = 1$, assim $\sigma(r) \in \ker(\pi) = L$. Logo $L = \sigma(R)$. Note que $\sigma([F, R]) = [\sigma(F), \sigma(R)] = [U, L] = 1$, pois L é central, assim σ induz um homomorfismo $\bar{\sigma} : F/[F, R] \rightarrow U$. Mas $\bar{\sigma}((R \cap F')/[F, R]) = \sigma(R) \cap \sigma(F') = L \cap U' = L$, assim $|(R \cap F')/[F, R]| \geq |L|$.

Pelo teorema 7.66 página 208 de [23], existe uma extensão central

$$1 \longrightarrow L \longrightarrow U \longrightarrow G \longrightarrow 1$$

com $L \cong M(G)$ e $L \leq U'$. Portanto, o Lema 2.25 (ii) nos dá

$$|M(G)| = |L| \leq |(R \cap F')/[F, R]| \leq |M(G)|.$$

Retornando ao lema 2.25 com $K \cong (R \cap F')/[F, R]$, a injeção $\delta : K^* \rightarrow M(G)$ será sobrejetiva, e assim $M(G) \cong (R \cap F')/[F, R]$. \square

Definição 2.27 *Se A é um grupo abeliano finitamente gerado, seja $d(A)$ o número de elementos do menor conjunto que gera A ; isto é, A pode ser gerado por algum conjunto com $d(A)$ elementos, mas não pode ser gerado por um conjunto com $d(A) - 1$ elementos.*

Teorema 2.28 *Se Q é um grupo finito tendo uma apresentação com n geradores e r relações, então*

$$d(M(Q)) \leq r - n.$$

Demonstração. Ver corolário 11.21 página 365 de [23]. \square

Podemos relacionar o segundo grupo de homologia com o segundo grupo de cohomologia de um grupo G dado pela apresentação F/R .

Teorema 2.29 [15]. *Seja G um grupo finito arbitrário dado pela apresentação $G \cong F/R$, então*

$$M(G) = H^2(G, \mathbb{C}^*) \cong H_2(G, \mathbb{Z}).$$

Demonstração. Ver teorema 2.7.3 página 78 de [15]. \square

2.2.2 Exemplos de Cálculo do Multiplicador de Schur

Apresentaremos agora uma seção de exemplos do Multiplicador de Schur de um grupo finitamente apresentado. Tais exemplos serão posteriormente retomados no capítulo 4, e verificados com o algoritmo lá apresentado.

Exemplo 2.30 [23]. Se \mathbb{V} é o 4-grupo (grupo de Klein), então, $M(\mathbb{V}) \cong \mathbb{Z}_2$.

Demonstração. O teorema 2.20 mostra que $\exp(M(\mathbb{V})) = 2$. Como \mathbb{V} tem a apresentação $\mathbb{V} = \langle a, b | a^2 = 1, b^2 = 1, (ab)^2 = 1 \rangle$, pelo teorema 2.28 $d(M(\mathbb{V})) = 3 - 2 = 1$. Assim, $M(\mathbb{V})$ é cíclico e de ordem 2. Portanto, $M(\mathbb{V}) \cong \mathbb{Z}_2$. \square

Exemplo 2.31 [19]. Se G é um grupo cíclico, então $M(G) = \{1\}$.

Demonstração. Uma apresentação para o grupo cíclico G de ordem n é dada por $\langle a | a^n = e \rangle$. Como G tem um gerador e uma relação, então $d(M(G)) = 0$. Portanto, $M(G) = \{1\}$. \square

Exemplo 2.32 [23]. Se G é o grupo Q_{2n} dos quatérnios generalizados, então $M(G) = \{1\}$.

Demonstração. Uma apresentação para o grupo dos quatérnios generalizados é dada por $Q_{2n} = \langle a, b | a^{2n} = 1, b^2 = a^n, b^{-1}ab = a^{-1} \rangle$. Da relação $b^{-1}ab = a^{-1}$ obtemos

$$\begin{aligned} b^{-1}ab &= a^{-1} \\ (b^{-1}ab)^n &= (a^{-1})^n \\ \underbrace{b^{-1}abb^{-1}ab \cdots b^{-1}ab}_{n\text{-vezes}} &= a^{-n} \\ b^{-1}a^n b &= a^{-n} \end{aligned} \tag{2-2}$$

Substituindo em (2-2) a relação $b^2 = a^n$ obtemos $a^{-n} = b^{-1}b^2b = b^2 = a^n$. Implicando que $a^{-n} = a^n$, ou seja, $a^{2n} = 1$ que é exatamente a primeira das relações da apresentação de Q_{2n} . Desta forma Q_{2n} terá somente duas relações, implicando que $d(Q_{2n}) = 0$. Portanto $M(G) = \{1\}$. \square

Exemplo 2.33 [19]. Seja G o grupo diedral $2n$ do exemplo 1.35. Então

$$M(D_{2n}) = \begin{cases} \{1\}, & \text{se } n \text{ é ímpar} \\ \mathbb{Z}_2, & \text{se } n \text{ é par.} \end{cases}$$

Demonstração. Ver [19] página 69. □

Definição 2.34 Seja k um corpo. Definimos o **grupo linear especial** sobre k , $SL(n, k)$, como o conjunto de todas as matrizes $n \times n$ com determinante 1, sobre k , onde k é um corpo. Se $k = \mathbb{Z}_q$ denotamos G por $SL(n, q)$.

Exemplo 2.35 [19]. Seja $G = SL(2, q)$, com $q = p^f$ para algum primo p . Então $M(G) = \{1\}$, exceto para $q = 2^2$ e $q = 3^2$.

Demonstração. Ver [19] página 90. □

Definição 2.36 Seja k um corpo. O centro de $SL(n, k)$, que denotaremos por $Z(SL(n, k))$ é o grupo das matrizes escalares aI , com I a matriz identidade; onde $a^n = 1$. Definiremos como o **grupo especial linear projetivo** o grupo

$$PSL(n; k) = \frac{SL(n; k)}{Z(SL(n; k))}$$

Se k for um corpo de característica q , mudaremos a notação para $PSL(n, q)$.

Exemplo 2.37 [19]. Seja $G = PSL(2, q)$, onde $q = p^f$, $f \geq 1$, para algum primo p . temos que

$$M(G) = \begin{cases} \{1\}, & \text{para } p = 2 \text{ e } p^f \neq 2^2, \\ \mathbb{Z}_2, & \text{para } p > 2 \text{ e } p^f \neq 3^2, \\ \mathbb{Z}_2, & \text{para } p^f = 2^2, \\ \mathbb{Z}_6, & \text{para } p^f = 3^2. \end{cases}$$

Demonstração. Ver [19] página 94. □

2.3 Grupos de Deficiência Zero

Nesta seção daremos um tratamento diferente para o Multiplicador de Schur de um grupo finitamente apresentado. Trataremos aqui dos grupo de deficiência zero e trabalharemos com alguns exemplos. Esta seção pode ser encontrada em [2].

Se um grupo G tem n geradores e m relações, escreveremos

$$P = \langle x_1, \dots, x_n; r_1, \dots, r_m \rangle \quad (2-3)$$

ou

$$P = \langle x_1, \dots, x_n; r_1 = \dots = r_m \rangle \quad (2-4)$$

Nestas fórmulas F é definido implicitamente como o grupo livre em x_1, \dots, x_n e R o fecho normal das relações r_j e $G = F/R$.

Definição 2.38 A *deficiência* de uma apresentação finita P como em (2-3) é definida como $def(P) = m - n$. Se G é um grupo finitamente apresentado, então sua deficiência é definida como

$$def(G) = \inf\{def(P)\}$$

onde P varia sobre todas as apresentações finitas de G .

Lema 2.39 Quando G é um grupo abeliano finitamente gerado, sendo $d(G)$ o número mínimo de geradores. Então as seguintes condições valem para grupos abelianos finitamente gerados A e B

- (i) $d(A \times B) \leq d(A) + d(B)$;
- (ii) $d(A \times B) = d(A) + d(B)$ se B abeliano livre.

Proposição 2.40 (Inequação de P. Hall) Se G é um grupo finitamente apresentado, então G_{ab} e $M(G)$ são abelianos finitamente gerados e

$$def(G) \geq d(M(G)) - rank(G_{ab}). \quad (2-5)$$

Demonstração. Dado alguma apresentação finita P de G como em (2-3) sendo F e R definidos como acima. Pela fórmula de Hopf temos a sequência exata

$$0 \longrightarrow M(G) \longrightarrow \frac{R}{[R,F]} \longrightarrow F_{ab} \longrightarrow G_{ab} \longrightarrow 0.$$

$K := Ker(F_{ab} \rightarrow G_{ab})$, sendo um subgrupo de F_{ab} , é novamente abeliano livre. Como F é gerado pelos elementos da forma $f r_i f^{-1} = [f, r_1] r_i$ com $1 \leq i \leq m$ e $f \in F$, o grupo abeliano $R/[R, F]$ é gerado pelas classes laterais $r_1[R, F], \dots, r_m[R, F]$, assim $d(R/[R, F]) \leq m$ e $M(G)$ é finitamente gerado. Pela aditividade da função *rank* na sequência exata curta e pelo lema 2.39 (ii)

temos

$$\begin{aligned} \text{def}(P) &= m - n \geq d(R/[R, F]) - n = d(M(G)) + d(K) - n \\ &= d(M(G)) + \text{rank}(K) - \text{rank}(F_{ab}) \\ &= d(M(G)) - \text{rank}(G_{ab}). \end{aligned}$$

□

Observação 2.41 *Se um grupo G possui deficiência 0, (2-5) na Inequação de P. Hall será*

$$\text{rank}(G_{ab}) \geq d(M(G)).$$

Teorema 2.42 *Quando G_{ab} é subgrupo de torção para um grupo finito G , a inequação de P. Hall se reduz a*

$$\text{def}(G) \geq d(M(G)).$$

Com tal ferramenta em mão podemos estimar uma cota para o *rank* do multiplicador de Schur de alguns grupos.

Exemplo 2.43 *O grupo cíclico 2 com apresentação $G = \langle a \mid a^2 \rangle$, tem deficiência zero logo $d(M(G)) \leq 0$. A mesma idéia poderá ser usada para qualquer n . Baseado em [2] uma lista completa de grupos de deficiência zero é dada por $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, 0 , $\mathbb{C}^n \times \mathbb{Z}$, \mathbb{C}^n para $n \geq 2$.*

Exemplo 2.44 *Segundo [2] página 183 uma apresentação para $SL(2, \mathbb{Z})$ é dada por*

$$\langle x, y \mid x^4, x^2, y^3 \rangle,$$

Usando o sistema operacional GAP, temos que $G_{ab} = \mathbb{C}_{12}$, ou seja,

```
gap> f:=FreeGroup(2);
<free group on the generators [ f1, f2 ]>
gap> r:=[f.1^4, f.1^2*f.2^-3];
[ f1^4, f1^2*f2^-3 ]
gap> g:=f/r;
<fp group on the generators [ f1, f2 ]>
gap> d:=DerivedSubgroup(g);
Group(<fp, no generators known>)
gap> h:=g/d;
Group([ f1*f3^2, f2*f3^2 ])
```

```
gap> StructureDescription(h);
  ``C12'' .
```

Como \mathbb{C}_{12} é de torção e $\text{def}(SL(2, \mathbb{Z})) = 0$. Portanto, pela Inequação de P. Hall, temos que $d(M(SL(2, \mathbb{Z}))) \leq 0$ implicando que $M(SL(2, \mathbb{Z})) = 0$.

Exemplo 2.45 Segundo [2] página 183 uma apresentação para $PSL(2, \mathbb{Z})$ é dada por

$$\langle x, y \mid x^2, y^3 \rangle,$$

Usando o sistema operacional GAP, temos que $G_{ab} = \mathbb{C}_6$, ou seja,

```
gap> f:=FreeGroup(2);
<free group on the generators [ f1, f2 ]>
gap> r:=[f.1^2, f.2^3];
[ f1^2, f2^3 ]
gap> g:=f/r;
<fp group on the generators [ f1, f2 ]>
gap> d:=DerivedSubgroup(g);
Group(<fp, no generators known>)
gap> h:=g/d;
Group([ f1*f2, f2^2 ])
gap> StructureDescription(h);
  ``C6'' .
```

Como \mathbb{C}_6 é de torção e $\text{def}(SL(2, \mathbb{Z})) = 0$. Pela desigualdade de Inequação de P. Hall, temos que $d(M(PSL(2, \mathbb{Z}))) \leq 0$ implicando que $M(PSL(2, \mathbb{Z})) = 0$.

Exemplo 2.46 Segundo [2] página 184 uma apresentação para D_∞ é dada por

$$\langle x, y \mid y^2 = yxy^{-1}x = e \rangle,$$

Usando o sistema operacional GAP, temos que $G_{ab} = \mathbb{C}_2 \times \mathbb{C}_2$, ou seja,

```
gap> f:=FreeGroup(2);
<free group on the generators [ f1, f2 ]>
gap> r:=[f.2^2, f.2*f.1*f.2^-1*f.1];
[ f2^2, f2*f1*f2^-1*f1 ]
gap> g:=f/r;
<fp group on the generators [ f1, f2 ]>
gap> d:=DerivedSubgroup(g);
Group(<fp, no generators known>)
```

```
gap> h:=g/d;
Group([ f1, f2 ])
gap> StructureDescription(h);
``C2 x C2''.
```

Como $\mathbb{C}_2 \times \mathbb{C}_2$ é de torção e $\text{def}(D_\infty) = 0$. Pela desigualdade de Inequação de P. Hall, temos que $d(D_\infty) \leq 0$ implicando que $M(D_\infty) = 0$.

O Segundo Grupo de Homologia de um Grupo; Relações entre Comutadores

Neste capítulo comentaremos o artigo de Clair Miller publicado em 1952 [17]. Tal trabalho foi inovador e ousado para sua época.

Clair Miller se preocupou em dar uma interpretação grupo-teórica para o segundo grupo de homologia de um grupo G . Para isso define o grupo, $H(G)$, chamado o associado de um grupo G , que é informalmente o grupo satisfazendo todas as relações de comutadores em G , módulo o fecho normal de $\langle G, G \rangle$.

3.1 Grupo Associado

Dado um grupo G , seja $\langle G, G \rangle$ o grupo livre de todos os pares $\langle x, y \rangle$, com $x, y \in G$. Considere o homomorfismo

$$\begin{aligned} \varphi: \langle G, G \rangle &\longrightarrow [G, G] \\ \langle x, y \rangle &\longmapsto [x, y]. \end{aligned}$$

Se $w \in \langle G, G \rangle$ sua imagem em $[G, G]$ é denotada por $[w]$.

Definição 3.1 Definimos $Z(G)$, como o Kernel de φ , ou seja,

$$Z(G) = \{w \in \langle G, G \rangle \mid [w] = 1\}.$$

Seja $B(G)$ o subgrupo normal de $\langle G, G \rangle$ gerado pelas relações

$$\langle x, x \rangle \sim 1; \tag{3-1}$$

$$\langle x, y \rangle \sim \langle y, x \rangle^{-1}; \tag{3-2}$$

$$\langle xy, z \rangle \sim \langle y, z \rangle^x \langle x, z \rangle; \tag{3-3}$$

$$\langle x, z \rangle^x \sim \langle x, [y, z] \rangle \langle y, z \rangle; \quad (3-4)$$

onde x, y e $z \in G$. E por definição

$$\langle y, z \rangle^x = \langle y^x, z^x \rangle = \langle xzx^{-1}, x^{-1}zx \rangle. \quad (3-5)$$

Em outras palavras $B(G)$ é o subgrupo normal gerado por todos $\langle x, x \rangle$, todos $\langle x, y \rangle \langle y, x \rangle$, etc. O símbolo \sim significa congruência em $\langle G, G \rangle \text{ mod } B(G)$. Temos que $B(G) \subset Z(G)$, pois a imagem por φ dos geradores de $B(G)$ tem comutadores triviais.

Definição 3.2 Definimos o **grupo associado** de G como

$$H(G) = Z(G)/B(G).$$

Definição 3.3 Se $h : G \rightarrow K$ é um homomorfismo, definimos

$$\begin{aligned} h_{\#} : \langle G, G \rangle &\longrightarrow \langle K, K \rangle \\ \langle x, y \rangle &\longmapsto h_{\#} \langle x, y \rangle = \langle h(x), h(y) \rangle. \end{aligned}$$

Então $h_{\#}$ leva $Z(G)$ em $Z(K)$, pois se $\langle x, y \rangle \in Z(G)$ implica $h_{\#}(\langle x, y \rangle) = \langle h(x), h(y) \rangle = h \langle x, y \rangle \in Z(K)$ e $B(G)$ em $B(K)$ induzindo um homomorfismo

$$h_* : H(G) \longrightarrow H(K),$$

que satisfaz

$$(hg)_* = h_* g_*, \quad 0_* = 0, \quad 1_* = 1,$$

onde 0 é o homomorfismo nulo, $0(x) = 1$ e 1 é um homomorfismo identidade $1(x) = x$.

Pela inversão em ambos os lados de (3) e quocientando por (2) temos

$$\begin{aligned} &\stackrel{(3-3)}{\implies} \langle xy, z \rangle \sim \langle y, z \rangle^x \langle x, z \rangle \\ &\implies \langle xy, z \rangle^{-1} \sim (\langle y, z \rangle^x \langle x, z \rangle)^{-1} \\ &\implies \langle xy, z \rangle^{-1} \sim \langle x, z \rangle^{-1} (\langle y, z \rangle^x)^{-1} \\ &\stackrel{(3-2)}{\implies} \langle z, xy \rangle \sim \langle z, x \rangle (\langle y, z \rangle^{-1})^x \\ &\stackrel{(3-2)}{\implies} \langle z, xy \rangle \sim \langle z, x \rangle \langle z, y \rangle^x, \end{aligned}$$

identificando $z \sim x$, $x \sim y$ e $y \sim z$ temos

$$\langle x, yz \rangle \sim \langle x, y \rangle \langle x, z \rangle^y. \quad (3-6)$$

Das muitas consequências da definição de $B(G)$, destacamos as seguintes propriedades:

Propriedade 3.4

$$\langle x, y \rangle^{(a,b)} \sim \langle x, y \rangle^{[a,b]}$$

onde $\langle x, y \rangle^{(a,b)}$ é por definição $\langle a, b \rangle \langle x, y \rangle \langle a, b \rangle^{-1}$.

Demonstração. A prova será feita desenvolvendo $\langle ax, by \rangle$ de duas maneiras, usando (3-3) e (3-6)

$$\langle ax, by \rangle \stackrel{(3-6)}{\sim} \langle ax, b \rangle \langle ax, y \rangle^b \stackrel{(3-3)}{\sim} \langle x, b \rangle^a \langle a, b \rangle \langle x, y \rangle^{ba} \langle a, y \rangle^b.$$

Por outro lado

$$\langle ax, by \rangle \stackrel{(3-3)}{\sim} \langle x, by \rangle^a \langle a, by \rangle \stackrel{(3-6)}{\sim} \langle x, b \rangle^a \langle x, y \rangle^{ab} \langle a, b \rangle \langle a, y \rangle^b.$$

Comparando o que obtivemos,

$$\begin{aligned} \langle a, b \rangle \langle x, y \rangle^{ab} &\sim \langle x, y \rangle^{ab} \langle a, b \rangle \\ \langle a, b \rangle \langle x, y \rangle^{ba} \langle a, b \rangle^{-1} &\sim \langle x, y \rangle^{ab}, \end{aligned}$$

substituindo x e y por $x^{ba^{-1}}$ e $y^{ba^{-1}}$ respectivamente, temos

$$\begin{aligned} \langle a, b \rangle \langle x^{ab^{-1}}, y^{ba^{-1}} \rangle^{ba} \langle a, b \rangle^{-1} &\sim \langle x^{ba^{-1}}, y^{ba^{-1}} \rangle^{ba} \\ \langle a, b \rangle \langle x, y \rangle \langle a, b \rangle^{-1} &\sim \langle x, y \rangle^{ab(ba)^{-1}} = \langle x, y \rangle^{aba^{-1}b^{-1}} = \langle x, y \rangle^{[a,b]}. \end{aligned}$$

Portanto, $\langle x, y \rangle^{(a,b)} \sim \langle x, y \rangle^{[a,b]}$. □

Propriedade 3.5

$$[\langle x, y \rangle, \langle a, b \rangle] \sim \langle [x, y], [a, b] \rangle.$$

Demonstração.

$$\begin{aligned} [\langle x, y \rangle, \langle a, b \rangle] &= \langle a, b \rangle \langle x, y \rangle \langle a, b \rangle^{-1} \langle x, y \rangle^{-1} \\ &= \langle x, y \rangle^{(a,b)} \langle x, y \rangle^{-1} \\ &\stackrel{(3,4)}{\sim} \langle x, y \rangle^{[a,b]} \langle x, y \rangle^{-1} \\ &\stackrel{(3,4)}{\sim} \langle [a, b], [x, y] \rangle \langle x, y \rangle \langle x, y \rangle^{-1} \\ &\sim \langle [a, b], [x, y] \rangle. \end{aligned}$$

□

Propriedade 3.6

$$\langle b, b' \rangle \langle a_0, b_0 \rangle \sim \langle [b, b'], a_0 \rangle \langle a_0, [b, b'] b_0 \rangle \langle b, b' \rangle.$$

Demonstração.

$$\langle a_0, [b, b'] b_0 \rangle \stackrel{(3-6)}{\sim} \langle a_0, [b, b'] \rangle \langle a_0, b_0 \rangle \stackrel{(3,4)}{\sim} \langle a_0, [b, b'] \rangle \langle a_0, b_0 \rangle \langle b, b' \rangle.$$

Substituindo em (3.6), temos

$$\begin{aligned} \langle [b, b'], a_0 \rangle \langle a_0, [b, b'] b_0 \rangle \langle b, b' \rangle &\sim \langle [b, b'], a_0 \rangle \langle a_0, [b, b'] \rangle \langle a_0, b_0 \rangle \langle b, b' \rangle \\ &\sim \langle [b, b'], a_0 \rangle \langle [b, b'], a_0 \rangle^{-1} \langle b, b' \rangle \langle a_0, b_0 \rangle \langle b, b' \rangle^{-1} \langle b, b' \rangle \\ &\sim \langle b, b' \rangle \langle a_0, b_0 \rangle. \end{aligned}$$

□

Propriedade 3.7

$$\langle b, b' \rangle \langle b_0, a_0 \rangle \sim \langle [b, b'] b_0, a_0 \rangle \langle a_0, [b, b'] \rangle \langle b, b' \rangle.$$

Demonstração.

$$\langle [b, b'] b_0, a_0 \rangle \stackrel{(3-3)}{\sim} \langle b_0, a_0 \rangle \langle [b, b'], a_0 \rangle \stackrel{(3,4)}{\sim} \langle b_0, a_0 \rangle \langle [b, b'], a_0 \rangle.$$

Substituindo em (3.7) temos

$$\begin{aligned} \langle [b, b'] b_0, a_0 \rangle \langle a_0, [b, b'] \rangle \langle b, b' \rangle &\sim \langle b_0, a_0 \rangle \langle [b, b'], a_0 \rangle \langle a_0, [b, b'] \rangle \langle b, b' \rangle \\ &\sim \langle b, b' \rangle \langle b_0, a_0 \rangle \langle b, b' \rangle^{-1} \langle [b, b'], a_0 \rangle \langle [b, b'], a_0 \rangle^{-1} \langle b, b' \rangle \\ &\sim \langle b, b' \rangle \langle b_0, a_0 \rangle. \end{aligned}$$

□

Propriedade 3.8

$$\langle b, b' \rangle \langle a, a' \rangle \sim \langle [b, b'], [a, a'] \rangle \langle a, a' \rangle \langle b, b' \rangle.$$

Demonstração.

$$\begin{aligned}
 \langle [b, b'], [a, a'] \rangle \langle a, a' \rangle \langle b, b' \rangle &\stackrel{(3.5)}{\sim} \langle [b, b'], \langle a, a' \rangle \rangle \langle a, a' \rangle \langle b, b' \rangle \\
 &\sim \langle b, b' \rangle \langle a, a' \rangle \langle b, b' \rangle^{-1} \langle a, a' \rangle^{-1} \langle a, a' \rangle \langle b, b' \rangle \\
 &\sim \langle b, b' \rangle \langle b_0, a_0 \rangle
 \end{aligned}$$

□

Propriedade 3.9

$$\langle x^n, y^s \rangle \sim 1, \quad n = \pm 1, \pm 2, \dots; s = \pm 1, \pm 2, \dots$$

Demonstração. Usaremos indução sobre a soma $n + s$, para n e s não negativos.

Se $n + s = 1$. De (3-3), temos

$$\langle xy, z \rangle \sim \langle y, z \rangle^x \langle x, z \rangle,$$

tomando $x = z$ e $y = 1$

$$\begin{aligned}
 \langle x, x \rangle &\sim \langle 1, x \rangle^x \langle x, x \rangle \\
 1 &\sim \langle 1, x \rangle^x 1 = \langle 1, x \rangle^x = \langle 1^x, x^x \rangle = \langle 1, xx^{-1} \rangle = \langle 1, x \rangle,
 \end{aligned}$$

ou seja,

$$\langle x^0, x^s \rangle \sim 1.$$

Suponha por indução que $\langle x^n, x^s \rangle \sim 1$, assim

$$\begin{aligned}
 \langle x^n, x^{s+1} \rangle &= \langle x^n, x^s x \rangle \stackrel{(3-6)}{\sim} \langle x^n, x^s \rangle \langle x^n, x \rangle^{x^s} \sim 1 \langle x^n, x \rangle^{x^s} \stackrel{(3-4)}{\sim} \langle x^s, [x^n, x] \rangle \langle x^n, x \rangle \\
 &= \langle x^s, x^n x x^{-n} x \rangle \langle x^n, x \rangle = \langle x^s, 1 \rangle \langle x^n, x \rangle \sim \langle x^n, x \rangle.
 \end{aligned}$$

Resta mostrarmos que $\langle x^n, x \rangle \sim 1$, para isso vamos usar indução sobre n . Para $n = 1$ temos que $\langle x^1, x \rangle \sim 1$. Suponha por indução que $\langle x^n, x \rangle \sim 1$,

$$\langle x^{n+1}, x \rangle = \langle x^n x^1, x \rangle \sim \langle x, x \rangle^{x^n} \langle x^1, x \rangle \sim 1.$$

□

Teorema 3.10 *O grupo associado de um grupo livre é um grupo unitário.*

Demonstração. Se F possuir apenas um gerador e como por (3-1), $\langle x^n, x^s \rangle \sim 1$, então $H(F) = 1$.

Se F é um grupo livre com finitos geradores o resultado segue por indução do lema 3.11.

Se F é livre com infinitos geradores, seja K um subgrupo de F finitamente gerado e $i : K \rightarrow F$ o homomorfismo inclusão. Se $u \in H(F)$, então pela definição de i_* , $u \in i_*H(K)$. \square

Lema 3.11 *Se $G = A * B$ é o produto livre de A e B , então $H(G) \simeq H(A) \times H(B)$.*

Demonstração. Seja $i : A \rightarrow G$ e $j : B \rightarrow G$ as inclusões naturais e $p : G \rightarrow A$ e $q : G \rightarrow B$ as projeções naturais. Assim temos os homomorfismos mostrados no diagrama,

$$\begin{array}{ccc}
 H(A) & & H(B) \\
 & \searrow^{i_*} & \swarrow_{j_*} \\
 & H(G) & \\
 & \swarrow_{p_*} & \searrow_{q_*} \\
 H(A) & & H(B)
 \end{array}$$

i_* e j_* são homomorfismos injetores e $i_*H(A)$ e $j_*H(B)$ disjuntos, pois A e B são disjuntos pela definição de produto livre. Se $H(G)$ é o produto dos grupos $i_*H(A)$ e $j_*H(B)$, $H(G) = i_*H(A)j_*H(B)$, o diagrama também mostra $H(G)$ é o produto direto $H(G) = i_*H(A) \times j_*H(B)$. O problema é então demonstrar que $H(G) = i_*H(A)j_*H(B)$.

A fim de demonstrar que $H(G) = i_*H(A)j_*H(B)$, vamos nos preocupar com três subgrupos de $\langle G, G \rangle$; $\mathcal{A} = i_{\#}\langle A, A \rangle$, $\mathcal{B} = j_{\#}\langle B, B \rangle$ e M o subgrupo de $\langle G, G \rangle$ gerado pelos elementos da forma $\langle a, b \rangle$, com $1 \neq a \in A$ e $1 \neq b \in B$. Seja $\langle x, y \rangle$ um gerador de $\langle G, G \rangle$ com $x = a_1b_1 \dots a_sb_s$, $y = \bar{a}_1\bar{b}_1 \dots \bar{a}_r\bar{b}_r$, com $a_i, \bar{a}_j \in A$, $b_i, \bar{b}_j \in B$. Aplicando repetidas vezes (3-3) e (3-6) vemos que $\langle x, y \rangle$ é congruente $mod B(G)$ a um produto da forma $\langle a, a' \rangle^z, \langle b, b' \rangle^z, \langle a, b \rangle^z$ e $\langle b, a \rangle^z$, com $a, a' \in A$, $b, b' \in B$ e $z \in G$. Por exemplo, se $x = a_1b_1$ e $y = \bar{a}_1\bar{b}_1$ temos

$$\begin{aligned}
 \langle x, y \rangle &= \langle a_1b_1, \bar{a}_1\bar{b}_1 \rangle \stackrel{(3-3)}{\sim} \langle b_1, \bar{a}_1\bar{b}_1 \rangle^{a_1} \langle a_1, \bar{a}_1\bar{b}_1 \rangle \stackrel{(3-6)}{\sim} (\langle b_1, \bar{a}_1 \rangle \langle b_1, \bar{b}_1 \rangle^{\bar{a}_1})^{a_1} \langle a_1, \bar{a}_1 \rangle \langle a_1, \bar{b}_1 \rangle^{\bar{a}_1} \\
 &\sim (\langle b_1, \bar{a}_1 \rangle^{a_1} \langle b_1, \bar{b}_1 \rangle^{\bar{a}_1 a_1}) \langle a_1, \bar{a}_1 \rangle \langle a_1, \bar{b}_1 \rangle^{\bar{a}_1}.
 \end{aligned}$$

Cada elemento dessa forma pode ser decomposto em um produto de termos do mesmo tipo, sem o expoente z , usando repetidas vezes as regras

$$\langle a, a' \rangle^{a_0} = \langle a^{a_0}, a'_{a_0} \rangle \quad (3-7)$$

$$\langle a, a' \rangle^{b_0} \sim \langle b_0, [a, a'] \rangle \langle a, a' \rangle \quad (3-8)$$

$$\langle a, b \rangle^{a_0} \sim \langle a_0 a, b \rangle \langle b, a_0 \rangle \quad (3-9)$$

$$\langle a, b \rangle^{b_0} \sim \langle b_0, a \rangle \langle a, b_0 b \rangle, \quad (3-10)$$

mais quatro regras similares são obtidas dessas trocando a com b , a_0 com b_0 e a' com b' . (3-7) e (3-8) são consequências de (3-5) e (3-4). (3-9) é dada por

$$\langle a_0 a, b \rangle \langle b, a_0 \rangle \stackrel{(3-3)}{\sim} \langle a, b \rangle^{a_0} \langle a_0, b \rangle \langle b, a_0 \rangle \sim \langle a, b \rangle^{a_0} \langle a_0, b \rangle \langle a_0, b \rangle^{-1} \sim \langle a, b \rangle^{a_0}.$$

E (3-10) segue por

$$\langle b_0, a \rangle \langle a, b_0 b \rangle \stackrel{(3-6)}{\sim} \langle b_0, a \rangle \langle a, b_0 \rangle \langle a, b \rangle^{b_0} \sim \langle a, b \rangle^{b_0}.$$

Assim vemos que $\langle x, y \rangle$ e elementos $w \in \langle G, G \rangle$, são congruentes a um produto π de termos $\langle a, a' \rangle$, $\langle b, b' \rangle$, $\langle a, b \rangle$ e $\langle b, a \rangle$.

Agora tome cada termo $\langle b, b' \rangle$ em π e o comute para a direita (começando com o mais a direita e procedendo um de cada vez) usando (3.6), (3.7) e (3.8). Assim para um elemento arbitrário $w \in \langle G, G \rangle$, $w \sim \pi \sim \pi' \beta$, com β um produto de termos $\langle b, b' \rangle$ e π' um produto de termos da forma $\langle a, a' \rangle$, $\langle a, b \rangle$ e $\langle b, a \rangle$. Agora tome cada termo da forma $\langle a, a' \rangle$ em π' e comute para a esquerda usando os equivalentes da propriedades (3.6), (3.7) trocando a por b ; assim temos $w \sim \pi' \beta \sim \alpha \pi'' \beta$, com π'' envolvendo somente termos $\langle a, b \rangle$ e $\langle b, a \rangle$ e α um produto de termos $\langle a, a' \rangle$. Trocando cada $\langle b, a \rangle$ em π'' por $\langle a, b \rangle^{-1}$, trocando π'' por $\mu \in M$ temos

$$w \sim \alpha \mu \beta,$$

com $\alpha \in \mathcal{A}$, $\beta \in \mathcal{B}$ e $\mu \in M$.

Agora seja $w \in Z(G)$, isto é, $[w] = 1$. Então $[\alpha][\mu][\beta] = [w] = 1$, e projetando em A vemos que $[\alpha] = 1$. Da mesma forma, $[\beta] = 1$, assim $[\mu] = 1$. Contudo $\mu = 1$ implica que $\mu = 1 \in M \subset \langle G, G \rangle$. Para concluirmos isso, seja μ escrito como uma palavra reduzida no grupo livre M , $\mu = \langle a_1, b_1 \rangle^{\epsilon_1} \dots \langle a_p, b_p \rangle^{\epsilon_p}$, com $\epsilon_i = \pm 1$, $a_i \neq 1 \neq b_i$. Então por indução em p , vemos que $[\mu]$ pode ser escrito como uma palavra reduzida no produto livre $G = A * B$ em que as duas últimas entradas são $b_p^{-1} a_p^{-1}$ se $\epsilon_p = -1$ ou $a_p^{-1} b_p^{-1}$ se $\epsilon_p = +1$. Em particular $[\mu] \neq 1$ e μ não é uma palavra vazia.

Assim, $\mu = 1$ implica $w \sim \alpha \mu \beta = \alpha \beta$, onde $[\alpha] = 1$ e $[\beta] = 1$, que mostra que $H(G) = i_* H(A) j_* H(B)$. \square

Teorema 3.12 *Existe um homomorfismo canônico entre $H(G)$ e $H_2(G, \mathbb{Z})$ preservando a noção de homomorfismo induzido; se $G \rightarrow K$ é um homomorfismo temos a comutatividade do diagrama*

$$\begin{array}{ccc} H(G) & \xrightarrow{h_*} & H(K) \\ | \wr & & | \wr \\ H_2(G, J) & \xrightarrow{h_*} & H_2(K, \mathbb{Z}). \end{array}$$

Demonstração. Suponha que G seja dado como um grupo quociente de um grupo E por um subgrupo central N de E . O homomorfismo $\eta : E \rightarrow G$ aplica E em G , com kernel N .

Definimos um homomorfismo

$$\begin{aligned} \psi : \langle G, G \rangle &\longrightarrow E \\ \langle x, y \rangle &\longmapsto [\bar{x}, \bar{y}], \end{aligned}$$

onde $\eta(\bar{x}) = x$ e $\eta(\bar{y}) = y$. O homomorfismo ψ independe da escolha de \bar{x} e \bar{y} . Pois, suponha que exista x' e \bar{x} representantes da mesma classe, assim como y' e \bar{y} , ou seja,

$$\begin{aligned} x'N = \bar{x}N &\Leftrightarrow x'\bar{x}^{-1} \in N \leq Z(E) \\ y'N = \bar{y}N &\Leftrightarrow y'\bar{y}^{-1} \in N \leq Z(E). \end{aligned}$$

Como $x'\bar{x}$ e $y'\bar{y}$ estão em $Z(E)$ temos

$$\begin{aligned} (x'\bar{x}^{-1})\bar{y}^{-1} &= \bar{y}^{-1}(x'\bar{x}^{-1}) \\ &= (y'^{-1}y')\bar{y}^{-1}(x'\bar{x}^{-1}) \\ &= y'^{-1} \underbrace{(y'\bar{y}^{-1})}_{\in Z(E)}(x'\bar{x}^{-1}) \\ &= y'^{-1}x'(y'\bar{y}^{-1})\bar{x}^{-1} \\ &= y'^{-1}x'y'(\bar{y}^{-1}\bar{x}^{-1}) \\ x'\bar{x}^{-1}\bar{y}^{-1}\bar{x}\bar{y} &= y'^{-1}x'y' \\ \bar{x}^{-1}\bar{y}^{-1}\bar{x}\bar{y} &= x'^{-1}y'^{-1}x'y' \\ [\bar{x}, \bar{y}] &= [x', y']. \end{aligned}$$

O homomorfismo ψ leva $Z(G)$ em $N \cap [E, E]$ e leva $B(G)$ em 1, e assim induz um homomorfismo $\phi : H(G) \rightarrow N \cap [E, E]$. Temos que a sequência

$$H(E) \xrightarrow{\eta_*} H(G) \xrightarrow{\phi} N \cap [E, E]$$

é exata em $H(G)$, isto é, $\ker \phi = \text{Im } \eta_*$. Pois, se $x = zB(E) \in H(E)$, temos $\phi(\eta_*(zB(E))) = [z] = e$, pelo fato que $z \in Z(E)$, assim vemos que $\text{Im } \eta_* \subset \text{Ker } \phi$. Por

outro lado, se $gB(G) \in \text{Ker } \phi$, onde $g = \langle g_i, g_j \rangle$, temos, $\phi(gB(G)) = [g] = e_N$, tal que $\eta(\bar{g}_i) = g_i$ e $\eta(\bar{g}_j) = g_j$, vemos que $\langle \bar{g}_i, \bar{g}_j \rangle \in Z(E)$ e portanto, $\langle g_i, g_j \rangle B(G) \in \text{Im } \eta_*$.

Se G é um grupo qualquer, vamos representar G como o quociente de um grupo livre F por um subgrupo R , $G = F/R$. Sendo $F^0 = F/[F, R]$ e $R^0 = R/[F, R]$ temos,

$$\begin{array}{ccc} F & \xrightarrow{\lambda} & F^0 \xrightarrow{\eta} G \\ \cup & & \cup \\ R & \xrightarrow{h_*} & R^0 \\ \cup & & \\ & & [F, R] \end{array}$$

onde λ e η são o homomorfismos. R^0 está no centro de F^0 , assim ϕ aplica $H(G)$ em $R^0 \cap [F^0, F^0]$. Examinando a sequência $H(F^0) \longrightarrow H(G) \longrightarrow R^0 \cap [F^0, F^0]$, ϕ é injetivo desde que $\eta_* = 0$. Para mostrarmos que $\eta_* = 0$, seja $w = \langle x_1, y_1 \rangle \cdots \langle x_p, y_p \rangle \in Z(F^0)$. Então $[w] = [x_1, y_1] \cdots [x_p, y_p] = 1 \in F^0$, e, escolha $\bar{x}_i, \bar{y}_i \in F$ tal que $\lambda(\bar{x}_i) = x_i$ e $\lambda(\bar{y}_i) = y_i$, e temos $\bar{w} = \langle \bar{x}_1, \bar{y}_1 \rangle \cdots \langle \bar{x}_p, \bar{y}_p \rangle$, com $\lambda_{\#} \bar{w} = w$, $\lambda[\bar{w}] = [w] = 1$, e daí $[\bar{w}] \in [F, R]$. Portanto $[\bar{w}] = [f_1, r_1] \cdots [f_q, r_q]$, para $f_i \in F$ e $r_i \in R$. Entretanto F é livre, $H(F) = 1$ e $B(F) = Z(F)$. Daí $\bar{w} \sim \langle f_1, r_1 \rangle \cdots \langle f_q, r_q \rangle \text{ mod } B(F)$. Então

$$\eta_{\#} w = \eta_{\#} \lambda_{\#} \bar{w} \sim \eta_{\#} \lambda_{\#} (\langle f_1, r_1 \rangle \cdots \langle f_q, r_q \rangle) \sim \langle \eta \lambda f_1, 1 \rangle \cdots \langle \eta \lambda f_q, 1 \rangle \sim 1$$

e $\eta_* = 0$.

Assim $\phi : H(G) \simeq R^0 \cap [F^0, F^0]$. Entretanto $R^0 \cap [F^0, F^0] = R \cap [F, F]/[F, R]$ é a fórmula de Hopf (teorema 2.26), de modo que temos construído o isomorfismo desejado. \square

Um Algoritmo para estimar o Segundo Grupo de Homologia de alguns Grupos Finitamente Apresentado

Dado um grupo finitamente apresentado G , a fórmula de Hopf (Teorema 2.26) expressa o segundo grupo de homologia de G em termos dos geradores e relações. Apresentaremos um algoritmo que usa a fórmula de Hopf para estimar o segundo grupo de homologia $H_2(G, k)$, com coeficientes em um corpo finito k , e retomaremos alguns exemplos apresentados na subseção 2.2.2 e complementaremos com exemplos usando $G = SL_2$ sobre um anel específico dos inteiros. Este último foi retirado da Conjectura de Quillen [1].

Observação 4.1 *Sejam R um subanel com identidade dos números complexos \mathbb{C} e SL_n e GL_n o grupo discreto das matrizes $n \times n$ sobre R com determinante não nulo e 1 respectivamente. Se $H(GL_n) := H^*(GL_n; \mathbb{Z}_l)$ denota o grupo de cohomologia de GL_n , módulo l . Então a inclusão natural $\mathbb{R} \subset \mathbb{C}$ induz uma estrutura do módulo $H(GL_n)$ sobre o anel de cohomologia módulo l das classes de Chern $P_n := H^*(BGL_n(\mathbb{C}); \mathbb{Z}_l)$, onde $BGL_n(\mathbb{C})$ denota o espaço dos grupos de Lie $GL_n(\mathbb{C})$ das matrizes $n \times n$ inversíveis sobre \mathbb{C} . Em [20] Quillen conjecturou que para certos primos l e anéis K o módulo $H(GL_n)$ é livre sobre P_n . Chamamos esta afirmação de **Conjectura de Quillen** de rank n para o primo l .*

Os algoritmos aqui apresentados estão reescritos no Apêndice A da forma como foram implementados no programa.

4.1 Primeiro Grupo de Homologia

Consideremos um grupo $G = F/R$, onde F é um grupo livre finitamente gerado e R um subgrupo normal de F . Assim, temos a sequência exata

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1 ,$$

onde F é um grupo livre finitamente gerado e R um subgrupo normal de F , tal que F age em R por conjugação.

Definição 4.2 Se F e R são dois grupos não necessariamente comutativos, então uma estrutura de F -módulos em R é uma aplicação

$$\begin{aligned} F \times R &\longrightarrow R \\ (f, r) &\longmapsto r^f, \end{aligned}$$

com, $r \in R$ e $f \in F$, tal que

- (i) $r^1 = r$;
- (ii) $(r_1 r_2)^f = r_1^f r_2^f$;
- (iii) $r^{f_1 f_2} = (r^{f_1})^{f_2}$.

Se F age em R por conjugação então, R é um F -módulo finitamente gerado, ou seja, temos a aplicação

$$\begin{aligned} F \times R &\longrightarrow R \\ (f, r) &\longmapsto r^f = f^{-1} r f, \end{aligned}$$

que satisfaz,

- (i) $r^1 = 1r1 = r$;
- (ii) $(r_1 r_2)^f = f^{-1} r_1 r_2 f = f^{-1} r_1 (f f^{-1}) r_2 f = (f^{-1} r_1 f) (f^{-1} r_2 f) = r_1^f r_2^f$;
- (iii) $r^{f_1 f_2} = (f_1 f_2)^{-1} r f_1 f_2 = f_2^{-1} f_1^{-1} r f_1 f_2 = f_2^{-1} r^{f_1} f_2 = (r^{f_1})^{f_2}$.

Observação 4.3 A menos que seja mencionado, daqui para frente todos os grupos serão dados com notação multiplicativa.

Como já vimos o primeiro grupo de homologia de um grupo G é isomorfo ao abelianizado de G , ou seja, $H_1(G, \mathbb{Z}) \cong G/[G, G] = G/G' = G_{ab}$, Teorema 1.65. Assim, o primeiro grupo de homologia, $H_1(G, \mathbb{Z})$, é um grupo abeliano tal que

$$H_1(G, \mathbb{Z}) \cong \frac{G}{G'} = \frac{G}{[G, G]} = \frac{F/R}{[F/R, F/R]} \cong \frac{F/R}{[F, F]/R} \cong \frac{F/R}{[F, F]R/R} \cong \frac{F}{[F, F]R}, \quad (4-1)$$

além disso, pelo terceiro teorema do isomorfismo $\frac{F/R}{[F, F]R} \cong F/[F, F]$ (Teorema 2.27, página 37, [23]). De (4-1) temos a sequência exata curta

$$1 \longrightarrow R/[F, F] \longrightarrow F \longrightarrow H_1(G, \mathbb{Z}) \longrightarrow 1,$$

onde $[F, F]$ denota o subgrupo comutador de F .

Se F age em $R[F, F]$ por conjugação, vemos que $R[F, F]$ é um F -módulo finitamente gerado, pois, $R[F, F]$ é subgrupo de F que é finitamente gerado, e

$$\begin{aligned} F \times R[F, F] &\longrightarrow R[F, F] \\ (f, x) &\longmapsto x^f = f^{-1}xf, \quad \text{onde } x = r[f_1, f_2], \end{aligned}$$

que satisfaz,

- (i) $(r[f_1, f_2])^1 = 1r[f_1, f_2]1 = r[f_1, f_2]$;
- (ii) $(r_1[f_1, f_2]r_2[f'_1, f'_2])^f = f^{-1}r_1[f_1, f_2]r_2[f'_1, f'_2]f = f^{-1}r_1[f_1, f_2](ff^{-1})r_2[f'_1, f'_2]f = (f^{-1}r_1[f_1, f_2]f)(f^{-1}r_2[f'_1, f'_2]f) = (r_1[f_1, f_2])^f(r_2[f'_1, f'_2])^f$;
- (iii) $(r[f_1, f_2])^{f_1f_2} = (f_1f_2)^{-1}r[f_1, f_2]f_1f_2 = f_2^{-1}f_1^{-1}r[f_1, f_2]f_1f_2 = f_2^{-1}(r[f_1, f_2]^{f_1})f_2 = (r[f_1, f_2]^{f_1})^{f_2}$.

A fórmula de comutadores

$$[xy, z] = (xy)^{-1}z^{-1}xyz = y^{-1}x^{-1}z^{-1}xzyy^{-1}z^{-1}yz = [x, z]^y[y, z]$$

prova que como F é um grupo finitamente gerado, e $[F, F]$ é um subgrupo de F , então $[F, F]$ é finitamente gerado. Este argumento nos leva a um algoritmo que dá a estrutura de $H_1(G, \mathbb{Z})$. A entrada é uma lista finita de geradores de F , que denotaremos por S , e uma lista finita de geradores para o F -módulo R , que denotaremos por T . A saída é uma lista de inteiros descrevendo a estrutura do grupo abeliano finitamente gerado $H_1(G, \mathbb{Z})$.

4.1.1 O Primeiro Algoritmo de homologia

Algoritmo 4.1: PrimeiraHomologia(F,R)

Entrada: Grupo Livre F , Relações R

Saída: Lista de invariantes abelianas do grupo finitamente apresentado F/R

- 1 $M :=$ Matriz das Relações de F/R
 - 2 $N :=$ Forma Normal Smith de M
 - 3 **retorna** Entradas Diagonais de N .
-

O comando **AbelianInvariants**() do *GAP* carrega o algoritmo acima. O algoritmo para reduzir a matriz para a *forma Normal Smith* foi dado na seção 1.10. Recordemos que dada uma apresentação finita para F/R que consiste de n geradores S e m relações T , existe uma matriz associada $n \times m$, M , cuja (i, j) entrada é a soma dos

expoentes de todas as ocorrências dos j -ésimos geradores das i -ésimos relações. A lista resultante das entradas diagonais de N é um conjunto de entradas de posição (i, i) para $i = 1, \dots, \min(n, m)$ e consiste de inteiros positivos e zeros. Cada inteiro positivo n corresponde a uma cópia de \mathbb{Z}_n onde $H_1(G, \mathbb{Z})$ é soma direta dos \mathbb{Z}_n , ver exemplo 1.74.

Este resultado será estendido para o caso em que o primeiro grupo de homologia de G é tomado com coeficientes em um corpo finito k . Neste caso, o primeiro grupo de homologia de G que denotamos por $H_1(G; k)$ é um k -espaço vetorial de dimensão finita. Sua dimensão será determinada pelo Teorema dos Coeficientes Universais, (Teorema 1.62), que nos dá a sequência exata curta

$$1 \longrightarrow k \otimes H_1(G, \mathbb{Z}) \longrightarrow H_1(G, k) \longrightarrow \text{Tor}(H_0(G), k) \longrightarrow 1,$$

onde $\text{Tor}(-, k)$ é um funtor derivado do funtor $(k \otimes -)$. O algoritmo toma como entrada a lista finita S e T do algoritmo 4.1 junto com a característica p do corpo finito k . A saída é um inteiro representando a dimensão do espaço vetorial $H_1(G, k)$.

4.1.2 O Primeiro Algoritmo com Coeficiente Homológico

Algoritmo 4.2: *PrimeiroCoeficienteHomolgico*(F, R, p)

Entrada: Grupo Livre F , Relações R , Primo p =Característica(k)

Saída: Dimensão do espaço vetorial $k \otimes H_1(G; k)$ sobre k

```

1  $T := \text{PrimeiraHomologia}(F, R)$ 
2  $X := []$ 
3 para  $x \in T$  faça
4   | se  $x \equiv 0 \pmod{p}$  então
5   |   | adicione  $x$  a  $X$ 
6   | fim
7 fim
8 retorna  $\text{tamanho}(X)$  {número de elementos da lista de  $X$ }
```

4.2 Segundo Grupo de Homologia

Estenderemos nosso estudo para o segundo grupo de homologia de um grupo G que é um grupo abeliano que denotaremos por $H_2(G, \mathbb{Z})$. Pela celebre fórmula devido a Hopf Teorema 2.26 (“fórmula de Hopf”, $H_2(G, \mathbb{Z}) \cong (R \cap F') / ([F, R])$) temos a seguinte sequência exata

$$1 \longrightarrow [F, R] \longrightarrow R \cap [F, F] \longrightarrow H_2(G, \mathbb{Z}) \longrightarrow 1,$$

onde $[F, R]$ é o subgrupo de F gerado pelos comutadores $[f, r]$ com $f \in F$ e $r \in R$.

Temos que

$$\begin{aligned} F \times [F, R] &\longrightarrow [F, R] \\ (f, [f_1, x_1]) &\longmapsto [f_1, x_1]^f = f^{-1}[f_1, x_1]f, \end{aligned}$$

que satisfaz,

$$(i) [f_1, x_1]^1 = [f_1, x_1];$$

$$(ii) ([f_1, x_1][f_2, x_2])^f = f^{-1}[f_1, x_1][f_2, x_2]f = f^{-1}[f_1, x_1](ff^{-1})[f_2, x_2]f = (f^{-1}[f_1, x_1]f)(f^{-1}[f_2, x_2]f) = [f_1, x_1]^f [f_2, x_2]^f;$$

$$(iii) [f_1, x_1]^{f_1 f_2} = (f_1 f_2)^{-1}[f_1, x_1]f_1 f_2 = f_2^{-1}f_1^{-1}[f_1, x_1]f_1 f_2 = f_2^{-1}[f_1, x_1]^{f_1} f_2 = ([f_1, x_1]^{f_1})^{f_2}.$$

Junto com, a fórmula

$$[x, y^z] = x^{-1}(y^{-1})^z x y^z = x^{-1}z^{-1}y^{-1}zx(yy^{-1})z^{-1}yz = [zx, y][y, z],$$

prova que $[F, R]$ é um F -módulo finitamente gerado sobre a conjugação. Contudo, a intersecção $R \cap [F, F]$ não é determinada por um algoritmo, e iremos somente estimar o grupo $H_2(G, \mathbb{Z})$ como um subgrupo do grupo $R/[F, R]$. Este grupo quociente é abeliano pois $[F, R]$ contém $[R, R]$ e se F age por conjugação, então esta ação é trivial, isto é

$$\begin{aligned} F \times R/[F, R] &\longrightarrow R/[F, R] \\ (f, x) &\longmapsto x^f = f^{-1}xf = x, \end{aligned}$$

com $x \in R/[F, R]$. Em particular, como R é um F -módulo finitamente gerado segue que o grupo quociente $R/[F, R]$ é um grupo abeliano finitamente gerado. Consequentemente, $H_2(G, \mathbb{Z})$ é um grupo abeliano finitamente gerado cuja estrutura gostaríamos definir.

Começaremos com a seguinte sequência exata

$$1 \longrightarrow H_2(G, \mathbb{Z}) \longrightarrow R/[F, R] \longrightarrow F/[F, F] \longrightarrow F/R[F, F] \longrightarrow 1, \quad (4-2)$$

em que os dois últimos termos são determinados como comentamos acima (4-1). Além disso, começando com uma lista finita de geradores T para o F -módulo R , iremos designar um algoritmo para encontrar um conjunto de geradores para $H_2(G, \mathbb{Z})$.

Para simplificar a discussão, seja k um corpo finito de característica p . Pelo teorema dos coeficientes universais (Teorema 1.62) temos a seguinte sequência exata curta

$$1 \longrightarrow k \otimes H_2(G, \mathbb{Z}) \longrightarrow H_2(G; k) \longrightarrow \text{Tor}(H_1(G, \mathbb{Z}), k) \longrightarrow 1 \quad (4-3)$$

Onde o último termo será ser determinado como segue. Como entrada iniciaremos com as invariantes abelianas de $H_1(G, \mathbb{Z})$ encontradas pelo primeiro algoritmo junto com a característica p do corpo k . A saída é um inteiro representando a dimensão do espaço vetorial $\text{Tor}(H_1(G), k)$ sobre k .

4.2.1 O Algoritmo Tor

Algoritmo 4.3: : $\text{Tor}(F, R, p)$

Entrada: Grupo Livre F , Relatores R , Primo $p = \text{Característica}(k)$

Saída: Dimensão de $\text{Tor}(H_1(G, \mathbb{Z}), k)$ sobre k

```

1  $T := \text{PrimeiraHomologia}(F, R)$ 
2  $X := []$ 
3 para  $x \in T$  faça
4   | se  $x \neq 0$  e  $x \equiv 0 \pmod{p}$  então
5   |   | adicione  $x$  a  $X$ 
6   | fim
7 fim
8 retorna  $\text{tamanho}(X)$ 

```

O primeiro termo $k \otimes H_2(G, \mathbb{Z})$ da sequência exata (4-3) é um espaço vetorial de dimensão finita sobre k , onde a dimensão somente será estimada por um algoritmo que descreveremos a seguir.

Da sequência exata (4-2) extraímos a sequência exata

$$1 \longrightarrow H_2(G, \mathbb{Z}) \longrightarrow \frac{R}{[F, R]} \longrightarrow \frac{R[F, F]}{[F, F]} \longrightarrow 1, \quad (4-4)$$

onde o último termo é um subgrupo do grupo abeliano livre $F/[F, F]$, ou seja, $R[F, F]/[F, F]$ é um grupo e está contido em $F/[F, F]$ pois, se $x \in R[F, F]/[F, F]$, então

$$x = r[f_1, f_2][F, F] = r f_1^{-1} f_2^{-1} f_1 f_2 [F, F].$$

Ou seja,

$$\underbrace{r f_1^{-1} f_2^{-1} f_1 f_2 [F, F]}_{\in F}.$$

Portanto, $x \in F/[F, F]$.

Temos que um subgrupo de um grupo abeliano livre finitamente gerado é abeliano livre, isto é, como $F/[F, F]$ é um grupo abeliano livre e $R[F, F]/[F, F]$ é subgrupo de $F/[F, F]$, temos que $R[F, F]/[F, F]$ é abeliano livre e consequentemente a sequência exata acima é split pelo (Teorema 3.1 da referência [11] página 5). Em particular, pelo tensorial com k na sequência (4-4), obtemos uma sequência exata curta de k -espaços vetoriais

$$1 \longrightarrow k \otimes H_2(G, \mathbb{Z}) \longrightarrow k \otimes \frac{R}{[F, R]} \longrightarrow k \otimes \frac{R[F, F]}{[F, F]} \longrightarrow 1. \quad (4-5)$$

Usando a propriedade universal (Teorema 1.49), com a função bi-aditiva linear

$$\begin{aligned} g : R/[F, F] \times k &\longrightarrow R/R^p[F, F] \\ (r[F, F], n) &\longmapsto r^n[F, F], \end{aligned}$$

temos uma única aplicação entre $R[F, F]/R^p[F, F]$ e $R[F, F]/[F, F]$ que é o último termo da sequência (4-5), tal que o seguinte diagrama comute

$$\begin{array}{ccc} R/[F, F] \times k & \xrightarrow{g} & R/R^p[F, F] \\ & \searrow i & \nearrow \bar{g} \\ & R/[F, F] \otimes k & \end{array}$$

Onde R^p denota o subgrupo de F gerado pelas p -ésimas potências dos elementos de R .

Em particular, pelo terceiro teorema do isomorfismo (Teorema 2.27, página 37, [23])

$$\frac{F/R^p[F, F]}{R[F, F]/R^p[F, F]} \cong F/R[F, F],$$

assim, existe uma sequência exata curta de grupos abelianos finitamente gerados

$$1 \longrightarrow k \otimes \frac{R[F, F]}{[F, F]} \longrightarrow \frac{F}{R^p[F, F]} \longrightarrow \frac{F}{R[F, F]} \longrightarrow 1, \quad (4-6)$$

cujos dois últimos termos são calculados pelo nosso primeiro algoritmo.

Definição 4.4 Para um grupo abeliano A , definimos o **p -subgrupo primário de A** como sendo

$$p^\infty(A) = \{a \in A \mid a^{p^i} = 1 \text{ para algum } i > 0\}.$$

A ordem deste subgrupo é da forma p^e . Chamaremos “ e ” o **p^∞ -rank de A** .

O p^∞ -rank de um grupo abeliano finitamente gerado A será calculado tomando como entrada as invariantes abelianas de A e o primo p .

Aplicando o p -subgrupo primário a sequência (4-6) obtemos outra sequência exata curta

$$1 \longrightarrow k \otimes \frac{R[F,F]}{[F,F]} \longrightarrow p^\infty\left(\frac{F}{R^p[F,F]}\right) \longrightarrow p^\infty\left(\frac{F}{R[F,F]}\right) \longrightarrow 1, \quad (4-7)$$

pois o primeiro termo é uma p -torção. Observe que enquanto $F/R[F,F]$ é dado em termos de S e T o grupo quociente $F/R^p[F,F]$ pode ser dado da mesma forma, mas substituindo T por T^p , a lista finita de p -potências de elementos em T .

4.2.2 O Algoritmo Rank

Faremos agora um breve comentário sobre números p -ádicos.

Definição 4.5 Chamaremos de **dígito p -ádico** um número natural entre 0 e $p - 1$ (incluindo). Um inteiro p -ádico é por definição uma sequência $(a_i)_{i \in \mathbb{N}}$ de dígitos p -ádicos.

Convencionamos escrever esta sequência como

$$\cdots a_i \cdots a_2 a_1 a_0,$$

(isto é, os a_i são escritos da esquerda para a direita).

Se n é um número natural, sua representação p -ádica é dada por

$$\overline{a_{k-1} a_{k-2} \cdots a_1 a_0}$$

(em outras palavras $n = \sum_{i=0}^{k-1} a_i p^i$) com cada a_i um dígito p -ádico, então identificamos n com o inteiro p -ádico (a_i) com $a_i = 0$ se $i \geq k$.

Definição 4.6 Se n é um número inteiro, sua **valuação p -ádica** é o expoente da maior potência de p que divide n . Que denotaremos por $v_p(n)$.

Por convenção, $v_p(0) = \infty$. Se $r = a/b$ é um racional, sua valuação p -ádica é por definição $v_p(r) = v_p(a) - v_p(b)$.

Por exemplo, a valuação 7-ádica de 7 é 1. E de 14 também é 1, assim bem como de 21, 28, 35 e 56. A valuação 7-ádica de 49 é por outro lado 2, assim como é de 98. E a valuação 7-ádica de 343 é 3. A valuação 7-ádica de $1/7$ é -1 , assim bem como de $3/7$, $1/14$, $5/56$. A valuação 7-ádica de $1/2$ ou $8/3$ é 0. E a valuação 7-ádica de $48/49$ é -2 .

Algoritmo 4.4: RankPrimárioPrincipal(F, R, p)**Entrada:** Grupo Livre F , Relatores R , Primo p **Saída:** p^∞ – rank de F/R

```

1  $T := PrimeiraHomologia(F, R)$ 
2  $Y := []$ 
3 para  $x \in T$  faça
4   se  $x \neq 0$  e  $x \equiv 0 \pmod p$  então
5      $y := p$ -ádica valuação de  $x$ 
6     adicione  $y$  a  $Y$ 
7   fim
8 fim
9  $s :=$  Soma de  $(Y)$  { $s$  é a soma dos elementos de  $Y$ }
10 retorna  $s$ 

```

Observação 4.7 O comando do GAP **PadicValuation** (n, p) do algoritmo 4.4, da a valuação p -ádica do inteiro n .

Até agora estávamos construindo as ferramentas para chegarmos ao nosso objetivo que é dar uma cota superior para a dimensão do segundo grupo de homologia de um grupo finitamente apresentado com coeficientes em um corpo k de característica p . Para simplificar a notação, sejam

$$\begin{aligned}
 a &= \text{dimensão de } Tor(H_1(G), k), & (\text{algoritmo 4.3}) \\
 b &= p^\infty - \text{rank de } \frac{F}{R[F, F]}, & (\text{algoritmo 4.4}) \\
 c &= p^\infty - \text{rank de } \frac{F}{R^p[F, F]}, & (\text{algoritmo 4.4}) \\
 d &= \text{dimensão de } H_2(G, k), & (\text{nosso objetivo}) \\
 e &= \text{dimensão de } k \otimes \frac{R}{[F, R]}, & (\text{ainda vamos definir})
 \end{aligned}$$

onde a é determinado pelo algoritmo *Tor*, b e c pelo algoritmo *Rank*, e e ainda será estudado. Pela propriedade aditiva da dimensão p^∞ -rank, deduzimos das sequências exatas acima que.

Da sequência exata (4-7) temos,

$$b = c - \dim\left(k \otimes \frac{R[F, F]}{[F, F]}\right). \quad (4-8)$$

Da sequência exata (4-5) temos,

$$\dim\left(k \otimes \frac{R[F, F]}{[F, F]}\right) = e - \dim(k \otimes H_2(G, \mathbb{Z})) \quad (4-9)$$

E da sequência exata (4-3) temos,

$$a = d - \dim(k \otimes H_2(G, \mathbb{Z})). \quad (4-10)$$

Substituindo em (4-10), (4-9) e depois (4-8) temos

$$\begin{aligned} a &= d - \dim(k \otimes H_2(G, \mathbb{Z})) \\ a &= d - e + \dim\left(k \otimes \frac{R[F, F]}{[F, F]}\right) \\ a &= d - e + c - b \\ d &= a + e - c + b \end{aligned}$$

Onde o ponto central de nossa dificuldade é encontrar o “ e ”.

Primeiro descreveremos um algoritmo que reduz um elemento do grupo via um sistema de reescrita.

4.2.3 Algoritmo Palavra Reduzida

O algoritmo que segue já havia sido apresentado por Anton no artigo “Homological symbols and the Quillen conjecture”, [1].

Algoritmo 4.5: : *PalavraReduzida*(F, R, Z, R', p)

Entrada: Grupo Livre F , Relatores R , Teste da Palavra z , Sublista R' de R ,
Primo p

Saída: Palavra Reduzida x em $F/[F, R]R^pR'$

- 1 $G := F/[F, R]R^pR'$
 - 2 $RG :=$ Sistema reescrito para G
 - 3 $x :=$ Palavra reduzida de (z) no sistema reescrito RG
 - 4 **retorna** x
-

Usaremos o sistema de reescrita dado pelo algoritmo Knuth-Bendix [16], implementado no GAP via o pacote *KBMA* [9].

4.2.4 O Algoritmo de Encontrar Base

Algoritmo 4.6: *EncontrarBase*(F, R, p, R')

Entrada: Grupo Livre F , Relatores R , Primo p , Sublista R' de R

Saída: Tamanho do conjunto gerador para $[F, R]R^p R' / [F, R]R^p$

```

1  $X := R'$ 
2 para  $x \in X$  faça
3    $x' :=$  PalavraReduzida( $F, R, x, \text{Diferença}(X, [x]), p$ ) {Diferença(A,B) é o
   complemento de  $B$  em  $A$ }
4   se  $x' = \text{identidade}$  então
5      $X := \text{Diferença}(X, [x])$ 
6   fim
7 fim
8 retorna tamanho( $X$ )

```

O algoritmo checka a independência linear de cada elemento x de R' com respeito a $R' - \{x\}$ em $[F, R]R^p R' / [F, R]R^p$. Quando x identificado pelo sistema de reescrita é linearmente dependente em $R' - \{x\}$, ele é removido de R' . O resultado final será uma lista de geradores linearmente independente.

Concluiremos esta discussão com o grande algoritmo que toma como entrada uma lista finita de geradores S e uma lista finita de relatores T para o grupo G junto com um primo p e dará como saída um inteiro d representando um limite superior para a dimensão de $H_2(G, k)$, onde k é um corpo de característica p .

4.2.5 O Algoritmo Segundo Homologia com Coeficientes

Algoritmo 4.7: *SegundoCoeficienteHomolgico*(F, R, R', p)

Entrada: Grupo Livre F , Relatores R , Primo p , Sublista R' de R gerando

$R / [F, R]R^p$,

Saída: Um inteiro d tal que $\dim(H_2(G, k)) \leq d$

```

1  $a := \text{Tor}(F, R, p)$ 
2  $b := \text{RankPrimárioPrincipal}(F, R[F, F], p)$ 
3  $c := \text{RankPrimárioPrincipal}(F, R^p[F, F], p)$ 
4  $e := \text{EncontrarBase}(F, R, p, R')$ 
5  $d := a + b - c + e$ 
6 retorna  $d$ 

```

É importante notar que a redução do teste da palavra do algoritmo **PalavraReduzida** é o problema da palavra [4]. Tal problema geralmente não tem

solução, quando a palavra não é a identidade. Contudo, se G é finito, ou mais geral, se a reescrita é confluenta (quando o programa consegue fazer os cálculos sem grandes problemas), então a redução do sistema reescrito é determinado e uma base é alcançada (a confluncia para um grupo finito é garantida na teoria acima; na prática ele pode tomar um longo tempo ou requerer mais memória do que está disponível). De qualquer maneira, isto não é o caso comum do problema da palavra que em geral é indeterminado; assim o resultado do **EncontrarBase** é em geral, a cardinalidade de um conjunto de geradores que não é necessariamente uma base. Portanto, neste caso não encontraremos a dimensão de $H_2(G, k)$, apenas um limite superior.

4.3 Exemplos

Nesta seção, aplicaremos o algoritmo discutido acima para alguns grupos. Os primeiros exemplos serão alguns dos que já foram apresentados na subseção 2.2.2, com o objetivo de ilustrar o efeito que o algoritmo tem em grupos com apresentações pequenas. Os demais exemplos são grupos mais interessantes. Na próxima seção deste capítulo discutiremos tais cálculos.

Exemplo 4.8 *O grupo \mathbb{V} é o 4-grupo (grupo de Klein):*

$$\begin{aligned} G &= \mathbb{V}, \\ S &= [a, b], \\ T &= [a^2 = 1, b^2 = 1, (ab)^2 = 1], \\ p &= 2, \\ d &= 3. \end{aligned}$$

Aqui o algoritmo dá uma cota superior para a dimensão do $H_2(\mathbb{V}_4, \mathbb{Z})$, pois, como podemos observar no exemplo 2.30 da subseção 2.2.2 o segundo $H_2(\mathbb{V}_4, \mathbb{Z}) = \mathbb{Z}_2$, com dimensão 2.

Exemplo 4.9 O grupo cíclico \mathbb{C}_3 :

$$\begin{aligned} G &= \mathbb{C}_3, \\ S &= [a], \\ T &= [a^n = e], \\ p &= 2, \\ d &= 0. \end{aligned}$$

Neste caso o algoritmo da exatamente a dimensão do $H_2(\mathbb{C}_3, \mathbb{Z})$, como podemos observar no exemplo 2.31 da subseção 2.2.2 o segundo $H_2(\mathbb{C}_3, \mathbb{Z}) = \{1\}$.

Exemplo 4.10 O grupo \mathbb{Q}_8 dos quatérnios:

$$\begin{aligned} G &= \mathbb{Q}_8, \\ S &= [a, b], \\ T &= [a^4 = 1, b^2 a^{-2} = 1, b^{-1} a b a = 1], \\ p &= 2, \\ d &= 2. \end{aligned}$$

Exemplo 4.11 O grupo diedral \mathbb{D}_8 :

$$\begin{aligned} G &= \mathbb{D}_8, \\ S &= [a, b], \\ T &= [a^4 = 1, b^2 = 1, b^{-1} a b a = 1], \\ p &= 2, \\ d &= 3. \end{aligned}$$

Neste caso o algoritmo da exatamente a dimensão do $H_2(\mathbb{D}_8, \mathbb{Z})$, como podemos observar no exemplo 2.33 da subseção 2.2.2, $H_2(\mathbb{D}_8, \mathbb{Z}) = \mathbb{Z}_2$, com dimensão 2.

Exemplo 4.12 *O grupo simétrico 5:*

$$\begin{aligned}
 G &= S_5, \\
 S &= [a, b], \\
 T &= [a^5, b^2, (a^{-1}b)^4, (a^2ba^{-2}b)^2], \\
 p &= 2, \\
 d &= 2.
 \end{aligned}$$

Seguiremos considerando três grupos lineares sobre $\mathbb{Z}[1/p, \zeta_p]$, onde ζ_p são as p -ésimas raízes da unidade. As apresentações para estes grupos podem ser encontrado em [1].

Exemplo 4.13 *O grupo Linear:*

$$\begin{aligned}
 G &= SL_2(\mathbb{Z}[1/3, \zeta_3]), \\
 S &= [z, u_1, a, b, b_0, b_1, b_2, w], \\
 T &= [b_0^{-1}ba, b_1^{-1}zbza, b_2^{-1}z^2bz^2a, w^{-1}zu_1, z^3, zu_1z^{-1}u_1^{-1}, a^4, a^2za^{-2}z^{-1}, a^2u_1a^{-2}u_1^{-1}, \\
 &\quad zaza^{-1}, u_1au_1a^{-1}, b_0b_1b_0^{-1}b_1^{-1}, b_0b_2b_0^{-1}b_2^{-1}, b_1b_2b_1^{-1}b_2^{-1}, b^3a^{-2}, b_0b_1b_2a^{-2}, \\
 &\quad b_0^{-3}w^{-1}b_0^{-1}w, b_1^{-3}w^{-1}b_1^{-1}w, b_2^{-3}w^{-1}b_2^{-1}w, (b_0b_1^{-1}a^{-1}u_1)^3, a^2b^{-1}u_1bz^2b^{-1}b_0^{-1}zbz^2u_1], \\
 p &= 3, \\
 d &= 0.
 \end{aligned}$$

Exemplo 4.14 *O grupo Linear:*

$$G = SL_2(\mathbb{Z}[1/5, \zeta_5]),$$

$$S = [z, u_1, u_2, a, b, b_0, b_1, b_2, b_3, b_4, w],$$

$$T = [b_0^{-1}ba, b_1^{-1}z^2bz^2a, b_2^{-1}z^4bz^4a, b_3^{-1}zbza, b_4^{-1}z^3bz^3a, w^{-1}zu_1u_2, z^5, zu_1z^{-1}u_1^{-1}, zu_2z^{-1}u_2^{-1}, u_1u_2u_1^{-1}u_2^{-1}, a^4, a^2za^{-2}z^{-1}, a^2u_1a^{-2}u_1^{-1}, a^2u_2a^{-2}u_2^{-1}, zaza^{-1}, u_1au_1a^{-1}, u_2au_2a^{-1}, b_0b_1b_0^{-1}b_1^{-1}, b_0b_2b_0^{-1}b_2^{-1}, b_0b_3b_0^{-1}b_3^{-1}, b_0b_4b_0^{-1}b_4^{-1}, b_1b_2b_1^{-1}b_2^{-1}, b_1b_3b_1^{-1}b_3^{-1}, b_1b_4b_1^{-1}b_4^{-1}, b_2b_3b_2^{-1}b_3^{-1}, b_2b_4b_2^{-1}b_4^{-1}, b_3b_4b_3^{-1}b_4^{-1}, b^3a^{-2}, b_0b_1b_2b_3b_4a^{-2}, b_0^{-5}w^{-1}b_0w, b_1^{-5}w^{-1}b_1w, b_2^{-5}w^{-1}b_2w, b_3^{-5}w^{-1}b_3w, b_4^{-5}w^{-1}b_4w, (b_0b_1^{-1}a^{-1}u_1)^3, (b_0b_2^{-1}a^{-1}u_2)^3, (b_0b_1^{-1}b_2^{-1}b_3a^{-1}u_1u_2)^3, a^2b^{-1}u_1bz^3b^{-1}b_0^{-1}z^2bz^4u_1, a^2b^{-1}u_2bzb^{-1}b_0^{-1}z^4bz^3u_2],$$

$$p = 5,$$

$$d = 3.$$

4.4 Considerações Finais

Concluimos este trabalho fazendo um comentário sobre os exemplos apresentados acima. Alguns destes exemplos já foram citados na subseção 2.2.2, onde foi calculado explicitamente o Multiplicador de Schur dos respectivos grupos. Na seção anterior usamos o celebre algoritmo apresentado neste trabalho para calcular um limite superior para a dimensão do segundo grupo de homologia de tais grupos, confirmando os resultados já encontrados na subseção 2.2.2.

Detalhes dos exemplos apresentados acima:

- *Exemplo 4.8.* O sistema é confluyente para o grupo de Klein. Apresentando o seguinte resultado:

```
SHC(f,r,2,r);
```

```
[3]
```

```
gap> time;
```

```
12
```

```
StringTime(12);
```

```
“ 0:00:00.012”
```

Ou seja, o sistema operacional *GAP* gasta um total de 12 milésimos de segundo para apresentar o resultado.

- *Exemplo 4.9.* O sistema é confluyente para o grupo cíclico 3. Apresentando o seguinte resultado:

```
SHC(f,r,2,r);
```

```
[0]
```

```
gap> time;
```

```
12
```

```
StringTime(12);
```

```
“ 0:00:00.012”
```

Ou seja, o sistema operacional *GAP* gasta um total de 12 milésimos de segundo para apresentar o resultado.

- *Exemplo 4.10.* O sistema é confluyente para o grupo dos Quatérnios Q_4 . Apresentando o seguinte resultado:

```
gap> SHC(f,r,2,r);
```

```
[2]
```

```
gap> time;
```

```
12
```

```
StringTime(8);
```

```
“ 0:00:00.008”
```

Ou seja, o sistema operacional *GAP* gasta um total de 8 milésimos de segundo para apresentar o resultado.

- *Exemplo 4.11.* O sistema é confluyente para o grupo dos Diederl \mathbb{D}_4 . Apresentando o seguinte resultado:

```
gap> SHC(f,r,2,r);
```

```
[3]
```

```
gap> time;
```

```
8
```

```
StringTime(8);
```

```
“ 0:00:00.008”
```

Ou seja, o sistema operacional *GAP* gasta um total de 8 milésimos para apresentar o resultado.

- *Exemplo 4.12.* O sistema é confluyente para o grupo Simétrico 5, \mathbb{S}_5 . Apresentando o seguinte resultado:

```
gap> SHC(f,r,2,r);
```

```
[2]
```

```
gap> time;
```

```
4
```

```
gap> StringTime(4);
```

```
“ 0:00:00.004”
```

Ou seja, o sistema operacional *GAP* gasta um total de 4 milésimos de segundo para

apresentar o resultado.

- *Exemplo 4.13.* O sistema não é confluyente para o grupo $SL_2(\mathbb{Z}[1/3, \zeta_3])$.

Apresentando o seguinte resultado:

```
gap> SHC(f,r,3,r);
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
‡ WARNING: system is not confluyente, so reductions may not be to normal form.
```

```
[0]
```

```
gap> time;
```

```
21600000
```

```
gap> StringTime(216000);
```

```
“ 6:00:00.000”
```

Ou seja, o sistema operacional *GAP* gasta aproximadamente de 6 horas para apresentar o resultado.

- *Exemplo 4.14.* O sistema não é confluyente para o grupo $SL_2(\mathbb{Z}[1/3, \zeta_3])$.

Apresentando o seguinte resultado:

```
gap> SecondHomologyCoefficients(f,r,5,r);
```

```
[3]
```

```
gap> time;
```

```
1441506
```

```
gap> StringTime(144150600);  
"40:02:30.600"
```

Ou seja, o sistema operacional *GAP* gasta aproximadamente de 40 horas para apresentar o resultado.

Referências Bibliográficas

- [1] ANTON, M. F. **Homological Symbols and the Quillen Conjecture**. Journal of Pure and Applied Algebra, 213:440–453, 2009.
- [2] BEYL, F; TAPPE, J. **Group Extensions, Representations, and the Schur Multiplier**. Springer-Verlag, New York, 1982.
- [3] BOARDMAN, J. M. **Universal Coefficient Theorem for Homology**. Technical report, Department of Mathematics, <http://www.math.jhu.edu/~jmb/note/ucthgy.pdf>, Baltimore, Maryland, U.S., 2008.
- [4] BRITTON, J. L. **The Word Problem For Groups**. Proc. London Math, 3(1958):493–506, 1945.
- [5] EILENBERG, S; MACLANE, S. **Relation Between Homology Groups of Spaces**. Ann. of Math, 46(1945):480–509, 1945.
- [6] EILENBERG, S; MACLANE, S. **Cohomology Theory in Abstract Groups I**. Ann. of Math, 48(2010):27–37, 1947.
- [7] GROUP, T. G. **GAP-Group, Algorithms, and Programming**. Technical report, Version 4.4.10, <http://www.gap-system.org>, 2007.
- [8] HOFFMAN, K; KUNZE, R. **Linear Algebra**. Prentice Hall Inc, New Jersey, second edition, 1971.
- [9] HOLT, D. F; EICK, B; O'BRIEN, E. **GAP Package Cohomolo**. Technical report, <http://www.warwick.ac.uk/staff/D.F.Holt/cohomolo/>, 2008.
- [10] HOPF, H. **Fundamental Groupe und Aweite Bettische Gruppe**. Comment. Math. Helv., 14(1942):257–309, 1945.
- [11] HUNGERFORD, T. **Algebra**. Springer, New York, 1974.
- [12] JACOBSON, N. **Basic Algebra**. Consulting Editora, New York, 1965.
- [13] JOHNSON, D. **Representation of Groups**. London, second edition, 1990.

- [14] JOSHUA, R. **An Algorithm For Low Dimensional Group Homology**. Homology, Homotopy and applications, 12(1):27–37, 2010.
- [15] KARPILOVSKY, G. **The Schur Multiplier**. New York, 1987.
- [16] KNUTH, D. E; BENDIX, P. B. **Simple Word Problems in Universal Algebras, in Computational Problems in Abstract Algebra**. Pergamon Press, Oxford, (1942):263–297, 1970.
- [17] MILLER, C. **The Second Homology Group of a Group; Relations Among Commutators**. American Mathematical Society, 3(4):588–595, 1952.
- [18] Technical report, <http://www.aprender-math.info/portugal/historyDetail.htm?id=Schur>.
- [19] PEREIRA, E. R. **O Multiplicador de Schur e Grupos de Recobrimento Total**. Technical report, Universidade de Brasília, Brasília, Df, 1999.
- [20] QUILLEN, D. **The Spectrum of an Equivariant Cohomology Ring**. Ann. of Math., 2:573–602, 1971.
- [21] ROBINSON, D. **A Course in the Theory of Groups**. Springer, New York, second edition, 1996.
- [22] ROTMAN, J. **Notes on Homological Algebra**. University of Illinois, Urbana, Urbana, 1970.
- [23] ROTMAN, J. **An Introduction to the Theory of Groups**. Springer-Verlag, New York, fourth edition, 1995.
- [24] ROTMAN, J. **Advanced Modern Algebra**. Prentice Hall, Upper Saddle River, NJ, 2002.
- [25] ROTMAN, J. **An Introduction to Homological Algebra**. Springer, Urbana, fourth edition, 2009.
- [26] VIEIRA, F. P. **O Teorema Syzygy de Hilbert**. Technical report, Universidade Federal de Goiás, Goiania, Go, 2009.

Algoritmos

No corpo do trabalho apresentamos de forma elegante os algoritmos que utilizamos no *GAP*. Neste apêndice, são apresentados esses mesmos algoritmos na forma que foram inseridos no programa.

Algoritmo A.1: *PRIMEIRAHOMOLOGIA(F,R,p)*

```
A:=AbelianInvariants(g);
```

Algoritmo A.2: *PRIMEIROCOEFICIENTEHOMOLOGICO(F,R,p)*

```
FHC:=function(f,r,p)
local A, X, x;

A:=AbelianInvariants(f/r);
X:=[];

for x in A do
  if x mod p = 0 then Add(X,x);
  fi;
od;

return Size(X);

end;
```

Algoritmo A.3: *Tor(F,R,p)*

```
TOR := function(f, r, p)
local A, X, x;

A:=AbelianInvariants(f/r);
X:=[];

for x in A do
  if x <> 0 and x mod p =0 then Add(X, x);
  fi;
od;

return Size(X);

end;
```

Algoritmo A.4: *PrimeiroPrimarioRank(F,R,p)*

```
PPR := function(f, r, p)
local A, X, y, x;

A:=AbelianInvariants(f/r);
X:=[];

for x in A do
  if x <> 0 and x mod p =0 then
    y:=PadicValuation(x, p);
    Add(X, y);
  fi;
od;

return Sum(X);

end;;
```

Algoritmo A.5: *PalavraReduzida*(F, R, p)

```

RequirePackage('`kbmag`');

RWA:=function(f,r,TestWord,R,p)
local S, GG, C, G, RG, OR;
S:=List(r,x->x^p);
GG:=GeneratorsOfGroup(f);
C:=ListX(GG,r,Comm);

G:=f/Concatenation(C,S,R);
RG:=KBMAGRewritingSystem(G);
OR:=OptionsRecordOfKBMAGRewritingSystem(RG);
MakeConfluent(RG);

return ReducedWord(RG,TestWord);
end;;

```

Algoritmo A.6: *EncontrarBase*(F, R, p)

```

FB:=function(f,r,p,R)
local H,TestWord,x,X;
X=[];
H:=R;
for x in H do
  TestWord:=RWA(f,r,x,
  Difference(H,[x]),p);
  Add(X,TestWord);
if IsOne(TestWord)=true then H:=Difference(H,[x]);
fi;
od;
return Size(H);
end;;

```

Algoritmo A.7: *EncontrarBase*(F, R, p)

```
SHC:=function(f, r, p, R)

local a,b,c,d,e,h,j,i;

h:=GeneratorsOfGroup(f);
j:=ListX(h,h,Comm);
i:=List(r,x->x^p);

a:=TOR(f,r,p);
b:=PPR(f,Concatenation(r,j),p);
c:=PPR(f,Concatenation(i,j),p);
e:=FB(f,r,p,R);
d:=a+b-c+e;
return [d];
end;;
```
