UNIVERSIDADE ESTADUAL DE CAMPINAS
Instituto de Matemática, Estatística e Computação Científica

LUCAS BARROSO ROCHA

UMA CONEXÃO ENTRE O MULTIPLICADOR DE SCHUR E A CONSTRUÇÃO $\mathscr{X}(G)$

Campinas
2024

LUCAS BARROSO ROCHA

UMA CONEXÃO ENTRE O MULTIPLICADOR DE SCHUR E A CONSTRUÇÃO $\mathscr{X}(G)$

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

Orientadora: Dessislava Hristova Kochloukova

ESTE TRABALHO CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO DEFENDIDA PELO ALUNO LUCAS BARROSO ROCHA, E ORIENTADA PELA PROFA. DRA. DESSISLAVA HRISTOVA KOCHLOUKOVA.

Campinas
2024

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

R582c Rocha, Lucas Barroso, 1999-
Uma conexão entre o multiplicador de Schur e a construção X(G) / Lucas Barroso Rocha. – Campinas, SP : [s.n.], 2024.

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

1. Teoria dos grupos. 2. Álgebra homológica. I. Kochloukova, Dessislava Hristova, 1970-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações Complementares

Título em outro idioma: A connection between the Schur multiplier and the construction X(G)
Palavras-chave em inglês:
Group theory
Homological algebra
Área de concentração: Matemática
Titulação: Mestre em Matemática
Banca examinadora:
Dessislava Hristova Kochloukova [Orientador]
Luis Augusto de Mendonça
Igor dos Santos Lima
Data de defesa: 08-03-2024
Programa de Pós-Graduação: Matemática

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0009-0009-3502-1251
- Currículo Lattes do autor: https://lattes.cnpq.br/5313005911288468

Dissertação de Mestrado defendida em 08 de março de 2024 e aprovada pela banca examinadora composta pelos Profs. Drs.

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

Prof(a). Dr(a). LUIS AUGUSTO DE MENDONÇA

Prof(a). Dr(a). IGOR DOS SANTOS LIMA

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

AGRADECIMENTOS

Agradeço ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo apoio financeiro durante os 24 meses de duração do projeto de pesquisa (processo 130407/2022-4).

RESUMO

Neste texto, serão apresentados diversos resultados básicos em Teoria de Grupos e Álgebra Homológica com o intuito de demonstrar algumas propriedades das construções $\mathscr{X}(G)$ e $\nu(G)$, respectivamente introduzidas nos artigos *On weak permutability between groups*, de S. Sidki, e *On a Construction Related to the Non-abelian Tensor Square of a Group*, de N. Rocco. Em particular, será demonstrado que o multiplicador de Schur de um grupo G é isomorfo a um subquociente de $\mathscr{X}(G)$, e será estabelecida uma cota superior para o expoente de $\mathscr{X}(G)$ caso G seja finito. Além disso, será demonstrado que algumas propriedades do grupo G são preservadas pelas construções $\mathscr{X}(G)$ e $\nu(G)$.

Palavras-chave: Teoria de Grupos; Álgebra Homológica.

ABSTRACT

In this paper, several basic results in Group Theory and Homological Algebra will be shown with the purpose of proving some properties of the constructions $\mathscr{X}(G)$ and $\nu(G)$, respectively introduced in the articles *On weak permutability between groups*, by S. Sidki, and *On a Construction Related to the Non-abelian Tensor Square of a Group*, by N. Rocco. In particular, it will be proven that the Schur multiplier of a group G is isomorphic to a subquotient of $\mathscr{X}(G)$, and an upper bound will be established for the exponent of $\mathscr{X}(G)$ in case G is finite. Furthermore, it will be shown that some properties of the group G are preserved by the constructions $\mathscr{X}(G)$ and $\nu(G)$.

Keywords: Group Theory; Homological Algebra.

LISTA DE SÍMBOLOS

$\emptyset$: conjunto vazio

$\mathbb{N}$: conjunto dos números naturais (incluindo o 0)

$\mathbb{Z}$: conjunto dos números inteiros

$\mathbb{Q}$: conjunto dos números racionais

$A \backslash B$: diferença entre os conjuntos A e B

$A \sqcup B$: união disjunta (formal) dos conjuntos A e B

$|X|$: cardinalidade do conjunto X

$f|_X$: restrição da função f ao conjunto X

id_X ou 1_X: função identidade do conjunto X

$exp(G)$: expoente do grupo G

$A \leq B$: A é um subgrupo de B

$A \lhd B$: A é um subgrupo normal de B

$ker(\phi)$: kernel (núcleo) do morfismo ϕ

$im(\phi)$: imagem do morfismo ϕ

$a|b$: a divide b

$MDC(a, b)$: maior divisor comum entre a e b

A/B : quociente (de grupos ou módulos) de A por B

$A \simeq B$: A é isomorfo a B (como grupo, anel ou módulo)

$A \rtimes B$: produto semidireto do grupo A pelo grupo B

SUMÁRIO

INTRODUÇÃO

No artigo *On weak permutability between groups* (referência [1]), Sidki define a construção $\mathscr{X}(G)$ (em que G é um grupo) como o grupo

$$\mathscr{X}(G) := \frac{G * G^{\psi}}{\langle [g, g^{\psi}] : g \in G \rangle^{G * G^{\psi}}},$$

em que G^{ψ} é isomorfo a G e $*$ denota o produto livre de grupos. Além disso, no artigo *On a Construction Related to the Non-abelian Tensor Square of a Group* (referência [2]), Rocco introduz a construção $\nu(G)$, correlata a $\mathscr{X}(G)$, como o grupo

$$\nu(G) := \frac{G * G^{\psi}}{\langle [g_1, g_2^{\psi}]^{g_3}[g_1^{g_3}, (g_2^{g_3})^{\psi}]^{-1}, [g_1, g_2^{\psi}]^{g_3^{\psi}}[g_1^{g_3}, (g_2^{g_3})^{\psi}]^{-1} : g_1, g_2, g_3 \in G \rangle^{G * G^{\psi}}}.$$

Neste texto, serão desenvolvidos, de maneira acessível porém rigorosa, os fundamentos da Álgebra Homológica com o intuito de estudar o multiplicador de Schur de um grupo (denotado por $M(G)$) e sua conexão com extensões stem. Com auxílio desses resultados, serão redemonstradas, de maneira mais detalhada, diversas proposições a respeito de $\mathscr{X}(G)$ apresentadas no artigo de Sidki, que, por sua vez, serão utilizadas para demonstrar propriedades da construção $\nu(G)$. Dentre esses resultados, destacam-se os seguintes:

1. Existe um homomorfismo sobrejetivo $\phi : W(G)/R(G) \to M(G)$, em que $W(G)$ e $R(G)$ são subgrupos de $\mathscr{X}(G)$.

2. Se G é um grupo finito, então $exp(\mathscr{X}(G))$ é finito e:

$$exp(\mathscr{X}(G)) \mid exp(M(G/G'))exp(M(G'))exp(G')exp(G).$$

3. As construções $\mathscr{X}(G)$ e $\nu(G)$ satisfazem as seguintes propriedades:

   (a) G é um grupo solúvel $\Longrightarrow$ $\mathscr{X}(G)$ e $\nu(G)$ são grupos solúveis;

   (b) G é um grupo perfeito $\Longrightarrow$ $\mathscr{X}(G)$ e $\nu(G)$ são grupos perfeitos;

(c) G é um grupo finito $\implies$ $\mathscr{X}(G)$ e $\nu(G)$ são grupos finitos;

(d) G é um p-grupo finito (p primo) $\implies$ $\mathscr{X}(G)$ e $\nu(G)$ são p-grupos finitos.

Este texto está dividido em sete capítulos (subdivididos em seções), que estão organizados da seguinte forma: o primeiro capítulo apresenta brevemente alguns resultados preliminares em Teoria de Grupos; o segundo e o terceiro capítulos fornecem as bases teóricas sobre categorias e módulos necessárias para o estudo da Álgebra Homológica; o quarto capítulo introduz os principais resultados e ferramentas da Álgebra Homológica; o quinto capítulo utiliza os resultados do capítulo anterior para estudar grupos de homologia, o multiplicador de Schur e extensões stem; o sexto capítulo analisa a construção $\mathscr{X}(G)$; e, por fim, o sétimo e último capítulo apresenta brevemente algumas propriedades de $\nu(G)$ e um isomorfismo entre quocientes de $\nu(G)$ e $\mathscr{X}(G)$. A teoria apresentada nos capítulos 2, 3 e 4, bem como nas seções 5.1 e 5.2, é fortemente baseada no livro *An Introduction to Homological Algebra* (referência [3]), de Joseph Rotman.

1 Grupos e apresentações

Neste capítulo, serão apresentados alguns resultados de Teoria de Grupos, em particular sobre comutadores, grupos livres, apresentações de grupos e produtos livres. Para esse fim, diversos resultados e definições básicas sobre grupos serão omitidos.

1.1 Comutadores e subgrupos

Nesta seção, serão apresentados resultados básicos sobre conjugação, comutadores e subgrupos. Algumas demonstrações serão omitidas.

Definição 1.1.1. *Sejam H um grupo e $h_1, h_2 \in H$. Definem-se:*

1. $h_1^{h_2} := h_2^{-1}h_1h_2$;

2. $h_1^{-h_2} := (h_1^{-1})^{h_2}$;

3. $[h_1, h_2] := h_1^{-1}h_2^{-1}h_1h_2$.

Lema 1.1.2. *Seja H um grupo e $h_1, h_2, h_3 \in H$. Então:*

1. $(h_1h_2)^{h_3} = h_1^{h_3}h_2^{h_3}$;

2. $(h_1^{h_2})^{h_3} = h_1^{h_2h_3}$;

3. $(h_1^{h_2})^{-1} = (h_1^{-1})^{h_2}$;

4. $[h_1, h_2] = h_1^{-1}h_1^{h_2} = (h_2^{-1})^{h_1}h_2$;

5. $[h_1, h_2]^{-1} = [h_2, h_1]$;

6. $[h_1, h_2]^{h_3} = [h_1^{h_3}, h_2^{h_3}]$;

7. $[h_1, h_2]^{h_2^{-1}} = [h_2^{-1}, h_1]$;

8. $[h_1h_2, h_3] = [h_1, h_3]^{h_2}[h_2, h_3]$;

9. $[h_1, h_2h_3] = [h_1, h_3][h_1, h_2]^{h_3}$;

10. $[[h_1, h_2^{-1}], h_3]^{h_2}[[h_2, h_3^{-1}], h_1]^{h_3}[[h_3, h_1^{-1}], h_2]^{h_1} = 1.$

Demonstração. Segue da definição de conjugação e comutadores. *QED.*

Definição 1.1.3. *Sejam G um grupo, H um subgrupo de G e $R \subseteq G$. Definem-se os seguintes subgrupos de G:*

1. $\langle R \rangle := \{\prod_{j\in J} r_j \in G : J$ *finito,* $\{r_j, r_j^{-1}\} \cap R \neq \emptyset \ \forall\ j \in J\}$;

2. $R^H := \langle r^h : h \in H, r \in \langle R \rangle \rangle$.

Lema 1.1.4. *Sejam G e H grupos, $\phi : G \to H$ um homomorfismo e $R \subseteq ker(\phi)$. Então:*

$$\langle R \rangle \subseteq R^G \subseteq ker(\phi).$$

Demonstração. Segue da definição anterior. *QED.*

Definição 1.1.5. *Sejam G um grupo e A, B subgrupos de G. Definem-se os seguintes subgrupos de G:*

1. $[A, B] := \langle \{[a, b] : a \in A, b \in B\} \rangle$ *(denominado* ***subgrupo comutador*** *de A e B);*

2. $A' := [A, A]$ *(denominado* ***subgrupo comutador*** *de A);*

3. $Z(G) := \{g \in G : [g, h] = 1_G \ \forall\ h \in G\}$ *(denominado* ***centro*** *do grupo G).*

Além disso, define-se recursivamente $A^{(0)} := A$ e $A^{(n+1)} := (A^{(n)})'$ para todo $n \in \mathbb{N}$.

Lema 1.1.6. *Sejam G, H grupos, $\phi : G \to H$ um homomorfismo e A, B subgrupos de G. Então, $\phi([A, B]) = [\phi(A), \phi(B)]$. Em particular, se H é abeliano, então $[A, B] \subseteq ker(\phi)$.*

Demonstração. Como ϕ é um homomorfismo, então:

$$\phi([a, b]) = \phi(a^{-1}b^{-1}ab) = \phi(a)^{-1}\phi(b)^{-1}\phi(a)\phi(b) = [\phi(a), \phi(b)] \ \forall\ a \in A \ \forall\ b \in B. \quad (1)$$

Além disso, por definição, segue que:

$$\phi([A, B]) = \langle \{\phi([a, b]) : a \in A, b \in B\} \rangle, \quad (2)$$

$$[\phi(A), \phi(B)] = \langle \{[\phi(a), \phi(b)] : a \in A, b \in B\} \rangle. \ (3)$$

Por (1), (2) e (3), segue que $\phi([A, B]) = [\phi(A), \phi(B)]$. Em particular, se H é abeliano, então $\phi([A, B]) = [\phi(A), \phi(B)] \subseteq [H, H] = 0$, logo $[A, B] \subseteq ker(\phi)$. *QED.*

Lema 1.1.7. *Sejam G um grupo e A, B subgrupos de G. Então:*

1. $[A, B] \lhd \langle A, B \rangle$. Em particular, se $\langle A, B \rangle = G$, então $[A, B] \lhd G$.

2. Se $B \lhd A$, então $[A, B] \lhd A$ e $[A, B] \lhd B$.

Demonstração.

1. Sejam $a \in A$ e $b \in B$. Como

$$x^{-1}[a, b]x = [ax, b][b, x] \in [A, B] \ \forall \ x \in A,$$

$$x^{-1}[a, b]x = [x, a][a, bx] \in [A, B] \ \forall \ x \in B,$$

então $x^{-1}[a, b]x \in [A, B]$ para todo $x \in \langle A, B \rangle$. Assim, $[A, B] \lhd \langle A, B \rangle$.

2. Sejam $a \in A$ e $b \in B$. Como $B \lhd A$, então $a^{-1}b^{-1}a \in B$, logo:

$$[a, b] = (a^{-1}b^{-1}a)b \in B.$$

Portanto, $[A, B] \leq B \leq A \leq \langle A, B \rangle$. Pelo item 1, segue que $[A, B] \lhd A$ e $[A, B] \lhd B$.

QED.

Lema 1.1.8. *Sejam H um grupo, X, Y subgrupos de H e $n \in \mathbb{N}$. Então, para todo $x_1, ..., x_n \in X$ e $y_1, ..., y_n \in Y$, existe $h \in [X, Y]$ tal que $x_1y_1...x_ny_n = hx_1...x_ny_1...y_n$.*

Demonstração. Vale a identidade

$$xy = [x^{-1}, y^{-1}]yx \ \forall \ x \in X \ \forall \ y \in Y. \ (1)$$

Por (1), segue que:

$$x_1y_1x_2y_2 = [x_1^{-1}, y_1^{-1}]y_1x_1x_2y_2 \ \forall\ x_1, x_2 \in X\ \forall\ y_1, y_2 \in Y;$$

$$x_1y_1x_2y_2 = [x_1^{-1}, y_1^{-1}][y_1^{-1}, (x_1x_2)^{-1}]x_1x_2y_1y_2 \ \forall\ x_1, x_2 \in X\ \forall\ y_1, y_2 \in Y. \quad (2)$$

Defina $\eta(x_1, x_2, y_1, y_2) := [x_1^{-1}, y_1^{-1}][y_1^{-1}, (x_1x_2)^{-1}]$. Por definição, $\eta(x_1, x_2, y_1, y_2) \in [X, Y]$ e $x_1y_1x_2y_2 = \eta(x_1, x_2, y_1, y_2)x_1x_2y_1y_2$ (por (2)). Portanto, o lema vale para $n = 2$.

Seja $k \in \mathbb{N}$ par tal que o lema é valido para $n = k$. Assim, existe $h_1 \in [X, Y]$ tal que $x_1y_1...x_ky_k = h_1x_1...x_ky_1...y_k$. Logo:

$$x_1y_1...x_ky_kx_{k+1}y_{k+1}x_{k+2}y_{k+2} = h_1x_1...x_ky_1...y_kx_{k+1}y_{k+1}x_{k+2}y_{k+2}.$$

Seja $h_2 := \eta(x_1...x_k, y_1...y_k, x_{k+1}, y_{k+1})$. Logo:

$$x_1y_1...x_ky_kx_{k+1}y_{k+1}x_{k+2}y_{k+2} = h_1h_2x_1...x_kx_{k+1}y_1...y_ky_{k+1}x_{k+2}y_{k+2}.$$

Seja $h_3 := \eta(x_1...x_{k+1}, y_1...y_{k+1}, x_{k+2}, y_{k+2})$. Logo:

$$x_1y_1...x_ky_kx_{k+1}y_{k+1}x_{k+2}y_{k+2} = h_1h_2h_3x_1...x_kx_{k+1}x_{k+2}y_1...y_ky_{k+1}y_{k+2}.$$

Portanto, $h := h_1h_2h_3 \in [X, Y]$ satisfaz $x_1y_1...x_{k+2}y_{k+2} = hx_1...x_{k+2}y_1...y_{k+2}$. Por indução, o lema vale para todo $n \in \mathbb{N}$ par. Para $n \in \mathbb{N}$ ímpar, o lema vale para $n + 1$ com a escolha $x_{n+1} = y_{n+1} = 1_H$, logo também vale para n. Portanto, o lema vale para todo $n \in \mathbb{N}$. *QED.*

1.2 Grupos livres, produtos livres e apresentações de grupos

Nesta seção, serão introduzidos alguns resultados resultados básicos e definições da Teoria Geométrica de Grupos. Em particular, serão apresentados os conceitos de grupo livre, produto livre de grupos e apresentação de grupo.

A teoria apresentada nesta seção é baseada no capítulo 1 do livro *Combinatorial group theory : a topological approach* (referência [4]), de Daniel Cohen.

Definição 1.2.1. *Seja G um grupo. Então, G é dito* ***livre*** *se existem um conjunto X e uma função $i : X \to G$ tais que, para todo grupo H e para toda função $f : X \to H$, existe um único homomorfismo $\phi : G \to H$ tal que $\phi i = f$ (nesse caso, X é dito uma* ***base*** *para G).*

Lema 1.2.2. *Seja G um grupo livre com base X (munido da aplicação $i : X \to G$). Então, i é injetiva.*

Demonstração. Seja $\mathbb{Z}^X$ o conjunto das funções de X em $\mathbb{Z}$ munido da soma usual de funções. Assim, $\mathbb{Z}^X$ é um grupo abeliano. Dado $x \in X$, seja $\delta_x : X \to \mathbb{Z}$ a função tal que $\delta_x(x) = 1$ e $\delta_x(y) = 0$ para todo $x \in X \backslash \{x\}$. Então, a função $f : X \to \mathbb{Z}^X$ dada por $x \mapsto \delta_x$ é injetiva. Como G é um grupo livre com base X, então existe um homomorfismo $\phi : G \to \mathbb{Z}^X$ tal que $\phi i = f$; como f é injetiva, então i é injetiva. *QED.*

Como $i : X \to G$ é injetiva, então, pelo restante do texto, $i(X)$ será identificado com X.

Lema 1.2.3. *Sejam G, H grupos livres com base X (munidos das aplicações $i : X \to G$ e $j : X \to H$). Então, $G \simeq H$.*

Demonstração. Como G, H são livres com base X (munidos das funções $i : X \to G$ e $j : X \to H$), existem homomorfismos $\phi : G \to H$ e $\psi : H \to G$ tais que $\phi i = j$ e $\psi j = i$. Como $\psi\phi : G \to G$ é um homomorfismo tal que $\psi\phi i = id_G \circ i$ e G é livre com base X (munido da aplicação $i : X \to G$), então $\psi\phi = id_G$. Analogamente, $\phi\psi = id_H$, logo $G \simeq H$. *QED.*

Teorema 1.2.4. *Seja X um conjunto. Então, existe um grupo livre $\mathcal{F}(X)$ com base X.*

Demonstração. Seja X^{-1} um conjunto disjunto de X munido de uma bijeção $\psi : X \to X^{-1}$. Defina $x^{-1} := \psi(x)$ para todo $x \in X$ e $y^{-1} := \psi^{-1}(y)$ para todo $y \in X^{-1}$. Seja

$$M(X) := \{\emptyset\} \cup \bigcup_{n \in \mathbb{N} \backslash \{0\}} (X \cup X^{-1})^n.$$

Dado $g = (x_1, ..., x_n) \in M(X)$ tal que $n > 2$ e $x_i = x_{i+1}^{-1}$ para algum $i \in \{1, ..., n-1\}$, define-se a *redução elementar* de g na i-ésima coordenada como o elemento $(y_1, ..., y_{n-2})$, em que $y_j = x_j$ se $j < i$ e $y_j = x_{j+2}$ se $j \geq i$; se $g = (x, x^{-1})$, em que $x \in X \cup X^{-1}$, então define-se a *redução elementar* de g como $\emptyset$. Considere a seguinte relação binária em $M(X)$: $g \sim h$ se, e somente se, $g = h$ ou existem $g_1, ..., g_n \in M(X)$, com $g_1 = g$ e $g_n = h$, tais que, para todo $i \in \{1, ..., n-1\}$, g_{i+1} é uma redução elementar de g_i ou vice-versa. Por definição, $\sim$ é uma relação de equivalência em $M(X)$. Assim, seja $\mathcal{F}(X) := M(X)/\sim$ e defina:

$$* : M(X) \times M(X) \to M(X) \ \mid \ (x_1, ..., x_n) * (y_1, ..., y_k) = (x_1, ..., x_n, y_1, ..., y_k).$$

Por definição, $*$ é associativa. Por definição de $\sim$, segue que, se $u, u', v, v' \in M(X)$, então $u * v \sim u * v'$ e $u * v' \sim u' * v'$, logo $u * v \sim u' * v'$ (pois $\sim$ é uma relação de equivalência). Portanto, está bem definida e é associativa a seguinte operação binária em $\mathcal{F}(X)$:

$$\cdot : \mathcal{F}(X) \times \mathcal{F}(X) \to \mathcal{F}(X) \ \mid \ [(x_1, ..., x_n)] \cdot [(y_1, ..., y_k)] = [(x_1, ..., x_n, y_1, ..., y_k)].$$

Por definição, $(\mathcal{F}(X), \cdot)$ é um grupo cujo elemento neutro é $[\emptyset]$ e no qual a inversão é dada por $[(x_1, ..., x_n)]^{-1} = [(x_n^{-1}, ..., x_1^{-1})]$ para todo $[(x_1, ..., x_n)] \in \mathcal{F}(X)$. Seja $i : X \to \mathcal{F}(X)$ dada por $x \mapsto [(x)]$.

Sejam H um grupo e $f : X \to H$ uma função. Defina $\phi : X \cup X^{-1} \to H$ tal que $\phi|_X = f$ e $\phi(x) = (f(x^{-1}))^{-1}$ para todo $x \in X^{-1}$. Seja $F : \mathcal{F}(X) \to H$ dada por:

$$[(x_1, ..., x_n)] \mapsto \prod_{i=1}^{n} \phi(x_i).$$

Por definição, F está bem definida, é um homomorfismo e $Fi = f$. Se $F' : \mathcal{F}(X) \to H$ é um homomorfismo tal que $F'i = f$, então $F'([(x)]) = \phi(x)$ para todo $x \in X \cup X^{-1}$. Logo, para todo $[(x_1, ..., x_n)] \in \mathcal{F}(X)$, vale que:

$$F'([(x_1, ..., x_n)]) = F'\left(\prod_{i=1}^{n}[(x_i)]\right) = \prod_{i=1}^{n} F'([(x_i)]) = \prod_{i=1}^{n} \phi(x_i) = F([(x_1, ..., x_n)]).$$

Portanto, $\mathcal{F}(X)$ (munido da aplicação i) é um grupo livre com base X. *QED.*

Pela demonstração anterior, segue que X gera $\mathcal{F}(X)$.

Definição 1.2.5. *Seja G um grupo. Uma **apresentação** de G é um par (X, R), em que X é um conjunto e R é um subconjunto de $\mathcal{F}(X)$, tal que $G \simeq \mathcal{F}(X)/R^{\mathcal{F}(X)}$; nesse caso, denota-se $G = \langle X|R\rangle$, X é denominado **conjunto de geradores** de G e R é denominado **conjunto de relatores** de G.*

Definição 1.2.6. *Seja G um grupo. Então, G é dito **finitamente gerado (f.g.)** se G possui uma apresentação (X, R) tal que X é finito.*

Proposição 1.2.7. *Seja G um grupo. Então, G possui uma apresentação.*

Demonstração. Como $\mathcal{F}(G)$ é livre com base G (munido da aplicação $i : G \to \mathcal{F}(G)$), então existe um homomorfismo $\phi : \mathcal{F}(G) \to G$ tal que $\phi i = id_G$; em particular, $im(\phi) = G$. Logo, pelo Primeiro Teorema do Isomorfismo, $ker(\phi)$ é um subgrupo normal de $\mathcal{F}(G)$ e $\mathcal{F}(G)/ker(\phi) \simeq G$. Portanto, $(G, ker(\phi))$ é uma apresentação para G. *QED.*

Lema 1.2.8. *Sejam X um conjunto e R um subconjunto de $\mathcal{F}(X)$. Então, existe um único grupo G (a menos de isomorfismo) tal que $G = \langle X|R\rangle$.*

Demonstração. Segue da definição de apresentação de um grupo. *QED.*

Definição 1.2.9. *Seja $\mathcal{G} = (G_j)_{j\in J}$ uma família de grupos. Um **produto livre** para $\mathcal{G}$ é um grupo G, munido de homomorfismos $i_j : G_j \to G$ para todo $j \in J$, tal que, para todo grupo H e para toda família de homomorfismos $(f_j)_{j\in J}$ (em que $f_j : G_j \to H$ para todo $j \in J$), existe um único homomorfismo $*_{j\in J} f_j : G \to H$ tal que $f_j = (*_{j\in J} f_j)i_j$ para todo $j \in J$.*

Lema 1.2.10. *Seja $\mathcal{G} = (G_j)_{j\in J}$ uma família de grupos. Seja G um produto livre para $\mathcal{G}$, munido de homomorfismos $i_j : G_j \to G$ para todo $j \in J$. Então, i_j é injetivo para todo $j \in J$.*

Demonstração. Sejam $k \in J$ e $f_k : G_k \to G_k$ o homomorfismo identidade. Para todo $j \in J$ tal que $j \neq k$, seja $f_j : G_j \to G_k$ o homomorfismo trivial. Como G é um produto livre para $\mathcal{G}$, então existe um homomorfismo $f : G \to G_k$ tal que $fi_k = f_k$; como f_k é injetivo e $fi_k = f_k$, então i_k é injetivo. *QED.*

Como $i_j : G_j \to G$ é injetivo para todo $j \in J$, então, pelo restante do texto, G_j será identificado com $i_j(G_j)$ para todo $j \in J$.

Lema 1.2.11. *Seja $\mathcal{G} = (G_j)_{j\in J}$ uma família de grupos. Se G_1 e G_2 são produtos livres para $\mathcal{G}$, então $G_1 \simeq G_2$.*

Demonstração. A demonstração é análoga à do Lema 1.2.3. *QED.*

Teorema 1.2.12. *Seja $\mathcal{G} = (G_j = \langle X_j | R_j \rangle)_{j\in J}$ uma família de grupos. Então, $*_{j\in J} G_j := \langle \sqcup_{j\in J} X_j | \sqcup_{j\in J} R_j \rangle$ é um produto livre para $\mathcal{G}$.*

Demonstração. Sejam $X := \sqcup_{j\in J} X_j$, $R := \sqcup_{j\in J} R_j$, $F_j = \mathcal{F}(X_j)$, $F := \mathcal{F}(X)$, $G := F/R^F$. Dado $j \in J$, seja $\lambda_j : F_j \to G$ o homomomorfismo tal que $x \mapsto xR^F$ para todo $x \in X$; como $R_j \subseteq R$, então $R_j \subseteq ker(\lambda_j)$, logo $R_j^{F_j} \subseteq ker(\lambda_j)$ (pelo Lema 1.1.4). Assim, para todo $j \in J$, existe um homomorfismo $i_j : G_j \to G$ tal que $xR_j^{F_j} \mapsto xR^F$ para todo $x \in X$.

Sejam H um grupo e $(f_j)_{j\in J}$ uma família de homomorfismos, em que $f_j : G_j \to H$ para todo $j \in J$. Seja $\phi : F \to H$ o homomorfismo tal que $\phi(x_j) = f_j(x_j)$ para todo $x_j \in X_j$ e para todo $j \in J$. Como $R_j \subseteq ker(f_j)$ para todo $j \in J$, então $R \subseteq ker(\phi)$, logo $R^F \subseteq ker(\phi)$ (pelo Lema 1.1.4). Assim, existe um homomorfismo $f : G \to H$ tal que $f(x_j R^F) = f_j(x_j)$ para todo $x_j \in X_j$ e para todo $j \in J$. Como X_j gera G_j para todo $j \in J$ e $fi_j, f_j : G_j \to H$ são homomorfismos tais que $fi_j|_{X_j} = f_j|_{X_j}$ para todo $j \in J$, então $fi_j = f_j$ para todo $j \in J$. Se $g : G \to H$ é um homomorfismo tal que $gi_j = f_j$ para todo $j \in J$, então $gi_j = fi_j$ para todo $j \in J$, logo $g|_X = f|_X$, portanto $g = f$ (pois X gera G). Assim, $G = F/R^F = \langle \sqcup_{j\in J} X_j | \sqcup_{j\in J} R_j \rangle$ é um produto livre para $\mathcal{G}$. *QED.*

2 Módulos, funtores e sequências exatas

Neste capítulo, serão apresentados os resultados e definições básicos sobre módulos, funtores, produtos, coprodutos e sequências exatas, com destaque para os funtores Hom e produto tensorial.

2.1 Módulos

Nesta seção, serão apresentados os resultados e definições básicas sobre módulos. Para esse fim, as definições e resultados básicos sobre anéis e grupos serão omitidos.

Pelo restante do texto, o termo **anel** será utilizado como sinônimo de **anel com unidade**.

Definição 2.1.1. *Dado um anel R, um R-**módulo à esquerda** é um conjunto M (denotado por ${}_RM$), munido de uma aplicação $+ : M \times M \to M$ e de uma aplicação $\cdot : R \times M \to M \mid (r, m) \mapsto rm$, tal que:*

1. *$(M, +)$ é grupo abeliano;*

2. *$1_R m = m \; \forall \; m \in M$;*

3. *$r_1(r_2 m) = (r_1 r_2)m \; \forall \; r_1, r_2 \in R \; \forall \; m \in M$;*

4. *$(r_1 + r_2)m = (r_1 m) + (r_2 m) \; \forall \; r_1, r_2 \in R \; \forall \; m \in M$;*

5. *$r(m_1 + m_2) = (rm_1) + (rm_2) \; \forall \; r \in R \; \forall \; m_1, m_2 \in M$.*

Definição 2.1.2. *Dado um anel R, um R-**módulo à direita** é um conjunto M (denotado por M_R), munido de uma aplicação $+ : M \times M \to M$ e de uma aplicação $\cdot : M \times R \to M \mid (m, r) \mapsto mr$, tal que:*

1. *$(M, +)$ é grupo abeliano;*

2. *$m1_R = m \; \forall \; m \in M$;*

3. *$(mr_1)r_2 = m(r_1 r_2) \; \forall \; r_1, r_2 \in R \; \forall \; m \in M$;*

4. $m(r_1 + r_2) = (mr_1) + (mr_2)\ \forall\ r_1, r_2 \in R\ \forall\ m \in M$;

5. $(m_1 + m_2)r = (m_1r) + (m_2r)\ \forall\ r \in R\ \forall\ m_1, m_2 \in M$.

Definição 2.1.3. *Dado um anel R (munido de um produto $\cdot : R \times R \to R$), define-se o **anel oposto** a R, denotado por R^{op}, como o grupo abeliano R munido do produto $* : R \times R \to R$ dado por $(r_1, r_2) \mapsto r_2 \cdot r_1$.*

Se R é um anel comutativo, então a função identidade $1_R : R \to R^{op}$ é um isomorfismo de anéis. Além disso, dado um anel R, todo R-módulo à esquerda M pode ser interpretado como um R^{op}-módulo à direita (e vice-versa) por meio da identificação $rm \cong mr$ para todo $r \in R$ e para todo $m \in M$.

Definição 2.1.4. *Dados R, S anéis, um (R, S)-**bimódulo** é um conjunto M (denotado por ${}_RM_S$) tal que:*

1. *M é um R-módulo à esquerda;*

2. *M é um S-módulo à direita;*

3. $r(ms) = (rm)s\ \forall\ r \in R\ \forall\ s \in S\ \forall\ m \in M$.

Em particular, todo anel R é um (R, R)-bimódulo. Além disso, todo grupo abeliano (aditivo) G é um $\mathbb{Z}$-módulo à esquerda munido da ação $\cdot : \mathbb{Z} \times G \to G$ definida indutivamente por $0_{\mathbb{Z}} \cdot g = 0_G$ e $(z + 1_{\mathbb{Z}}) \cdot g = (z \cdot g) + g$ para todo $g \in G$ e para todo $z \in \mathbb{Z}$ (uma ação análoga pode ser definida à direita). Com essa ação, todo R-módulo à direita é um $(\mathbb{Z}, R)$-bimódulo e todo R-módulo à esquerda é um $(R, \mathbb{Z})$-bimódulo.

Pelo restante da seção, todos os módulos considerados serão R-módulos à esquerda (todos os resultados e definições são análogos para R-módulos à direita).

Definição 2.1.5. *Dados um anel R e M, N R-módulos à esquerda, uma função $\phi : M \to N$ é dita um R-**homomorfismo** (ou **homomorfismo de R-módulos à esquerda**) se:*

1. $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)\ \forall\ m_1, m_2 \in M$;

2. $\phi(rm) = r\phi(m)\ \forall\ r \in R\ \forall\ m \in M$.

Um homomorfismo bijetivo de módulos é dito um ***isomorfismo*** *de módulos.*

Definição 2.1.6. *Sejam R um anel e A um R-módulo à esquerda. Um subconjunto S de A é dito um* ***submódulo*** *de A se:*

$$s_1 + rs_2 \in S\ \forall\ r \in R\ \forall\ s_1, s_2 \in S.$$

Se S e T são submódulos de A, então a ***soma*** *de S e T é definida como:*

$$S + T := \{s + t \in A : s \in S, t \in T\}.$$

Proposição 2.1.7. *Sejam R um anel, A um R-módulo à esquerda e S, T submódulos de A. Então, $S + T$ e $S \cap T$ são submódulos de A.*

Demonstração. Segue da definição de submódulo e soma de submódulos. *QED.*

Proposição 2.1.8. *Sejam R um anel, A um R-módulo à esquerda e S, T submódulos de A tais que $S + T = A$ e $S \cap T = \{0\}$. Então, para todo $a \in A$, existe um único par $(a_s, a_t) \in S \times T$ tal que $a_s + a_t = a$.*

Demonstração. Fixe $a \in A$ e sejam $s, s' \in S$ e $t, t' \in T$ tais que $s + t = s' + t' = a$. Logo, $(s - s') + (t - t') = 0$, portanto $s - s' = -(t - t')$. Como $s - s' \in S$, $-(t - t') \in T$ e $s - s' = -(t - t')$, então $s - s' \in S \cap T = \{0\}$, logo $s = s'$. Analogamente, $t = t'$. *QED.*

Definição 2.1.9. *Sejam R um anel, A um R-módulo à esquerda e S um subconjunto de A. Então, o conjunto*

$$\langle S \rangle := \left\{ \sum_{s \in S'} r_s s \;\middle|\; S' \subseteq S \ finito,\ r_s \in R\ \forall\ s \in S' \right\}.$$

é denominado ***submódulo gerado por*** *S (em outras palavras, diz-se que S* ***gera*** *o submódulo $\langle S \rangle$). Se existe um conjunto finito X tal que $A = \langle X \rangle$, então A é dito um R-módulo* ***finitamente gerado****. Além disso, dado $a \in A$, denota-se $\langle \{a\} \rangle$ por $\langle a \rangle$ ou Ra.*

Proposição 2.1.10. *Sejam R um anel, A um R-módulo à esquerda e S um subconjunto de A. Então, $\langle S\rangle$ é um submódulo de A.*

Demonstração. Segue das definições de submódulo e de submódulo gerado por S. *QED.*

Proposição 2.1.11. *Sejam R um anel, A, B R-módulos à esquerda, S um subconjunto de A e $\phi : A \to B, \psi : A \to B$ R-homomorfismos tais que $\phi|_S = \psi|_S$. Então, $\phi|_{\langle S\rangle} = \psi|_{\langle S\rangle}$.*

Demonstração. Dados $S' \subseteq S$ finito e $r_s \in R \ \forall\ s \in S'$, tem-se que:

$$\phi\left(\sum_{s\in S'} r_s s\right) = \sum_{s\in S'} r_s\phi(s) = \sum_{s\in S'} r_s\psi(s) = \psi\left(\sum_{s\in S'} r_s s\right).$$

Logo, $\phi|_{\langle S\rangle} = \psi|_{\langle S\rangle}$. *QED.*

Definição 2.1.12. *Sejam R um anel, A um R-módulo à esquerda e S um subconjunto de A. Então, o* ***quociente*** *de A por S, denotado por A/S, é definido da seguinte forma:*

$$a + S := \{a + s : s \in S\} \ \forall\ a \in A,$$

$$A/S := \{a + S : a \in A\}.$$

Proposição 2.1.13. *Sejam R um anel, A um R-módulo à esquerda e S um submódulo de A. Então, estão bem definidas as aplicações*

$$+ : A/S \times A/S \to A/S \ \mid\ (a + S, a' + S) \mapsto (a + a') + S,$$

$$\cdot : R \times A/S \to A/S \ \mid\ (r, a + S) \mapsto (ra) + S.$$

e A/S é um R-módulo à esquerda munido com essas aplicações.

Demonstração. Segue das definições de módulo, submódulo e quociente. *QED.*

Definição 2.1.14. *Sejam R um anel, A, B R-módulos à esquerda e $\phi : A \to B$ um R-homomorfismo. Então, definem-se:*

1. ***kernel*** *(ou* ***núcleo****) de ϕ: $ker(\phi) := \{a \in A : \phi(a) = 0\}$;*

2. ***imagem*** *de* ϕ*:* $im(\phi) := \{\phi(a) : a \in A\}$ *(também denotada por* $\phi(A)$*);*

3. ***cokernel*** *(ou* ***conúcleo****) de* ϕ*:* $coker(\phi) := B/im(\phi)$*.*

Se $im(\phi) = \{0\}$*, então* ϕ *é dito um* ***morfismo nulo*** *e é denotado por* 0*.*

Proposição 2.1.15. *Sejam* R *um anel,* A, B R*-módulos à esquerda e* $\phi : A \to B$ *um* R*-homomorfismo. Então:*

1. $ker(\phi)$ *é submódulo de* A*;*

2. $im(\phi)$ *é submódulo de* B*;*

3. $coker(\phi)$ *é um* R*-módulo à esquerda;*

4. ϕ *é injetiva se, e somente se,* $ker(\phi) = \{0\}$*;*

5. ϕ *é sobrejetiva se, e somente se,* $coker(\phi) = \{0\}$*.*

Demonstração. Os itens 1 e 2 seguem das definições de submódulo, kernel e imagem. O item 3 segue da Proposição 2.1.13 e dos itens 1 e 2. Os itens 4 e 5 seguem das definições de módulo, kernel e cokernel. *QED.*

Os dois resultados a seguir são denominados Teoremas do Isomorfismo e serão utilizados frequentemente ao longo do texto. Resultados análogos são válidos para grupos em vez de módulos.

Teorema 2.1.16. *Sejam* A, B *módulos e* $\phi : A \to B$ *um homomorfismo. Então, a aplicação* $\overline{\phi} : A/ker(\phi) \to im(\phi)$ *dada por* $a + ker(\phi) \mapsto \phi(a)$ *está bem definida e é um isomorfismo de módulos.*

Demonstração. Por definição de kernel, ϕ é constante em todo conjunto da forma $a+ker(\phi)$, logo $\overline{\phi}$ está bem definida. Além disso, como ϕ é um homomorfismo de módulos, então $\overline{\phi}$ também é. Por definição, $\overline{\phi}$ é sobrejetiva. Se $\overline{\phi}(a + ker(\phi)) = 0$, então $\phi(a) = 0$, logo $a \in ker(\phi)$, portanto $a + ker(\phi) = 0 + ker(\phi)$; assim, $ker(\overline{\phi}) = 0$, logo $\overline{\phi}$ é injetiva. Portanto, $\overline{\phi}$ é um isomorfismo de módulos. *QED.*

Teorema 2.1.17. *Sejam A um módulo e A_1, A_2 submódulos de A tais que $A_2 \subseteq A_1$. Então, $(A/A_2)/(A_1/A_2) \simeq A/A_1$.*

Demonstração. Seja $\phi : A/A_2 \to A/A_1$ dada por $a+A_2 \mapsto a+A_1$. Como $A_2 \subseteq A_1$, então ϕ está bem definida e é um homomorfismo sobrejetivo de módulos tal que $ker(\phi) = A_1/A_2$. Pelo Teorema 2.1.16, conclui-se que $(A/A_2)/(A_1/A_2) \simeq A/A_1$. *QED.*

2.2 Categorias e funtores

Nesta seção, serão apresentadas as definições básicas sobre categorias e funtores. Para esse fim, os conceitos de *classe*, *conjunto* e *elemento* serão tomados como primitivos.

Definição 2.2.1. *Uma **categoria** $\mathcal{C}$ é formada pelos seguintes constituintes:*

- *Uma classe $\mathcal{O}b(\mathcal{C})$, cujos elementos são denominados* objetos*;*
- *Para todo $A, B \in \mathcal{O}b(\mathcal{C})$, um conjunto $Hom_{\mathcal{C}}(A, B)$, cujos elementos são denominados* morfismos *(um morfismo $f \in Hom_{\mathcal{C}}(A, B)$ é denotado por $f : A \to B$);*
- *Para todo $A, B, C \in \mathcal{O}b(\mathcal{C})$, uma função*

$$\cdot : Hom_{\mathcal{C}}(A, B) \times Hom_{\mathcal{C}}(B, C) \to Hom_{\mathcal{C}}(A, C),$$

  denominada composição de morfismos*, dada por $(f, g) \mapsto gf$.*

que satisfazem as seguintes propriedades:

1. *Para todo $A \in \mathcal{O}b(\mathcal{C})$, existe um morfismo $1_A \in Hom_{\mathcal{C}}(A, A)$, denominado **morfismo identidade** de A, tal que, para todo $B \in \mathcal{O}b(\mathcal{C})$, segue que:*

$$1_A f = f \ \forall \ f \in Hom_{\mathcal{C}}(B, A), \ \ g1_A = g \ \forall \ g \in Hom_{\mathcal{C}}(A, B);$$

2. *Se $A, B, C, D \in \mathcal{O}b(\mathcal{C})$, $f \in Hom_{\mathcal{C}}(A, B)$, $g \in Hom_{\mathcal{C}}(B, C)$ e $h \in Hom_{\mathcal{C}}(C, D)$, então $h(gf) = (hg)f$.*

Por definição, segue que, para cada $A \in \mathcal{O}b(\mathcal{C})$, existe um único morfismo identidade.

Definição 2.2.2. *Sejam $\mathcal{C}$ uma categoria e $A, B \in \mathcal{O}b(\mathcal{C})$. Então, um morfismo $f \in Hom_{\mathcal{C}}(A, B)$ é dito um **isomorfismo** em $\mathcal{C}$ se existe $g \in Hom_{\mathcal{C}}(B, A)$ tal que $fg = 1_B$ e $gf = 1_A$ (nesse caso, g é único, é denominado **morfismo inverso** de f e é denotado por f^{-1}). Se existe um isomorfismo $f \in Hom_{\mathcal{C}}(A, B)$, então os objetos A e B são ditos **isomorfos entre si** em $\mathcal{C}$ (nesse caso, denota-se $A \simeq B$).*

Definição 2.2.3. *Dadas $\mathcal{C}$ e $\mathcal{D}$ categorias, um **funtor covariante** $F : \mathcal{C} \to \mathcal{D}$ é um mapa que associa cada objeto $A \in \mathcal{O}b(\mathcal{C})$ a um objeto $FA \in \mathcal{O}b(\mathcal{D})$ e que associa cada morfismo $f \in Hom_{\mathcal{C}}(A, B)$ a um morfismo $Ff \in Hom_{\mathcal{D}}(FA, FB)$ (para todo $A, B \in \mathcal{O}b(\mathcal{C})$), de modo que:*

1. $F1_A = 1_{FA} \ \forall \ A \in \mathcal{O}b(\mathcal{C})$;
2. $F(gf) = (Fg)(Ff) \ \forall \ f \in Hom_{\mathcal{C}}(A, B) \ \forall \ g \in Hom_{\mathcal{C}}(B, C) \ \forall \ A, B, C \in \mathcal{O}b(\mathcal{C})$.

*Em particular, se $\mathcal{D} = \mathcal{C}$, $FA = A$ para todo objeto A de $\mathcal{C}$ e $Ff = f$ para todo morfismo f de $\mathcal{C}$, então F é denominado **funtor identidade de** $\mathcal{C}$ e é denotado por $1_{\mathcal{C}}$.*

Definição 2.2.4. *Dadas $\mathcal{C}$ e $\mathcal{D}$ categorias, um **funtor contravariante** $F : \mathcal{C} \to \mathcal{D}$ é um mapa que associa cada objeto $A \in \mathcal{O}b(\mathcal{C})$ a um objeto $FA \in \mathcal{O}b(\mathcal{D})$ e que associa cada morfismo $f \in Hom_{\mathcal{C}}(A, B)$ a um morfismo $Ff \in Hom_{\mathcal{D}}(FB, FA)$ (para todo $A, B \in \mathcal{O}b(\mathcal{C})$), de modo que:*

1. $F1_A = 1_{FA} \ \forall \ A \in \mathcal{O}b(\mathcal{C})$;
2. $F(gf) = (Ff)(Fg) \ \forall \ f \in Hom_{\mathcal{C}}(A, B) \ \forall \ g \in Hom_{\mathcal{C}}(B, C) \ \forall \ A, B, C \in \mathcal{O}b(\mathcal{C})$.

Proposição 2.2.5. *Dadas categorias $\mathcal{C}, \mathcal{D}, \mathcal{E}$ e funtores $F : \mathcal{C} \to \mathcal{D}$ e $G : \mathcal{D} \to \mathcal{E}$, existe um único funtor $GF : \mathcal{C} \to \mathcal{E}$ tal que $(GF)X = G(FX)$ para todo objeto X de $\mathcal{C}$ e $(GF)f = G(Ff)$ para todo morfismo f de $\mathcal{C}$; além disso, GF é covariante se F e G têm a mesma variância e GF é contravariante se F e G têm variâncias distintas.*

Demonstração. Segue da definição de funtor. *QED.*

Proposição 2.2.6. *Sejam $\mathcal{C}, \mathcal{D}$ categorias, $A, B \in \mathcal{O}b(\mathcal{C})$, $f \in Hom_{\mathcal{C}}(A, B)$, $F : \mathcal{C} \to \mathcal{D}$ um funtor covariante e $G : \mathcal{C} \to \mathcal{D}$ um funtor contravariante. Se f é isomorfismo em $\mathcal{C}$, então Ff e Gf são isomorfismos em $\mathcal{D}$, com $(Ff)^{-1} = F(f^{-1})$ e $(Gf)^{-1} = G(f^{-1})$.*

Demonstração. Suponha que f é isomorfismo em $\mathcal{C}$. Então, existe $f^{-1} \in Hom_{\mathcal{C}}(B, A)$ tal que $ff^{-1} = 1_B$ e $f^{-1}f = 1_A$. Como $F : \mathcal{C} \to \mathcal{D}$ é um funtor covariante, então:

$$(Ff)(Ff^{-1}) = F(ff^{-1}) = F(1_B) = 1_{FB},\ (Ff^{-1})(Ff) = F(f^{-1}f) = F(1_A) = 1_{FA}.$$

Logo, $Ff \in Hom_{\mathcal{D}}(FA, FB)$ é um isomorfismo em $\mathcal{D}$ e $(Ff)^{-1} = F(f^{-1})$. Como $G : \mathcal{C} \to \mathcal{D}$ é um funtor contravariante, então:

$$(Gf)(Gf^{-1}) = G(f^{-1}f) = G1_A = 1_{GA},\ (Gf^{-1})(Gf) = G(ff^{-1}) = G1_B = 1_{GB}.$$

Logo, $Gf \in Hom_{\mathcal{D}}(GB, GA)$ é um isomorfismo em $\mathcal{D}$ e $(Gf)^{-1} = G(f^{-1})$. *QED.*

Definição 2.2.7. *Seja $\mathcal{C}$ uma categoria. A* ***categoria oposta*** *a $\mathcal{C}$, denotada por $\mathcal{C}^{op}$, é a categoria determinada pelas seguintes propriedades:*

- *$\mathcal{O}b(\mathcal{C}^{op}) = \mathcal{O}b(\mathcal{C})$;*
- *Para todo $X, Y \in \mathcal{O}b(\mathcal{C})$, existe uma bijeção $\phi : Hom_{\mathcal{C}}(Y, X) \to Hom_{\mathcal{C}^{op}}(X, Y)$ dada por $f \mapsto f^{op}$;*
- *Para todo $A, B, C \in \mathcal{O}b(\mathcal{C})$, a função composição*

$$\cdot : Hom_{\mathcal{C}^{op}}(A, B) \times Hom_{\mathcal{C}^{op}}(B, C) \to Hom_{\mathcal{C}^{op}}(A, C) \ \mid\ (f, g) \mapsto gf$$

  satisfaz a seguinte propriedade:

$$(gf)^{op} = f^{op}g^{op}\ \forall\ f \in Hom_{\mathcal{C}}(A, B)\ \forall\ g \in Hom_{\mathcal{C}}(B, C);$$

- *Para todo $A \in \mathcal{O}b(\mathcal{C})$, $(1_A)^{op}$ é o morfismo identidade de A em $\mathcal{C}^{op}$.*

Toda proposição que seja válida para todas as categorias é válida para suas respectivas opostas, de modo que todo resultado ou construção geral sobre categorias apresenta um *dual* no contexto das categorias opostas, que pode ser definido ou demonstrado de maneira análoga ao original ao inverter a ordem dos morfismos e de sua composição. Por exemplo, funtores covariantes e contravariantes são construções duais; ou seja, todo funtor covariante $F : \mathcal{C} \to \mathcal{D}$ pode ser identificado com o funtor contravariante $F^{op} : \mathcal{C}^{op} \to \mathcal{D}$ dado por $F^{op}(f^{op}) := Ff$ para todo morfismo f de $\mathcal{C}$. Também vale ressaltar que o conceito de categoria oposta é seu próprio dual, ou seja, $(\mathcal{C}^{op})^{op} = \mathcal{C}$ para toda categoria $\mathcal{C}$. Assim, ao longo deste texto, quando dois resultados duais forem enunciados, a prova de um deles será omitida.

A seguir, definem-se as categorias de interesse para propósitos deste texto.

Definição 2.2.8.

1. ***Set***: *A categoria cujos objetos são os conjuntos, cujos morfismos são as funções e em que a composição de morfismos é a composição usual de funções.*

2. ***Grp***: *A categoria cujos objetos são os grupos, cujos morfismos são os homomorfismos de grupos e em que a composição de morfismos é a composição usual de funções.*

3. ***Ab***: *A categoria cujos objetos são os grupos abelianos, cujos morfismos são os homomorfismos de grupos e em que a composição de morfismos é a composição usual de funções.*

4. ***Ring***: *A categoria cujos objetos são os anéis com unidade, cujos morfismos são os homomorfismos de anéis que preservam a unidade e em que a composição de morfismos é a composição usual de funções.*

5. $_R$***Mod***: *A categoria cujos objetos são os* R*-módulos à esquerda, cujos morfismos são os* R*-homomorfismos de módulos à esquerda e em que a composição de morfismos é a composição usual de funções.*

6. *$\mathbf{Mod}_R$: A categoria cujos objetos são os R-módulos à direita, cujos morfismos são os R-homomorfismos de módulos à direita e em que a composição de morfismos é a composição usual de funções.*

Nestas categorias, um morfismo é um isomorfismo se, e somente se, ele é bijetivo (nesse caso, o morfismo inverso é igual à função inversa).

Definição 2.2.9. *Uma categoria $\mathcal{C}$ é dita **pré-aditiva** se, para todo $A, B, C \in \mathcal{O}b(\mathcal{C})$, tem-se que:*

1. *$Hom_{\mathcal{C}}(A, B)$ é um grupo abeliano (aditivo);*

2. *$f(g+h) = fg + fh \ \forall \ g, h \in Hom_{\mathcal{C}}(A, B) \ \forall \ f \in Hom_{\mathcal{C}}(B, C)$;*

3. *$(f+g)h = fh + gh \ \forall \ h \in Hom_{\mathcal{C}}(A, B) \ \forall \ f, g \in Hom_{\mathcal{C}}(B, C)$.*

Para todo anel R, as categorias $\mathbf{Ab}$, ${}_R\mathbf{Mod}$ e $\mathbf{Mod}_R$ são pré-aditivas.

Definição 2.2.10. *Dadas categorias pré-aditivas $\mathcal{C}, \mathcal{D}$, um funtor $F : \mathcal{C} \to \mathcal{D}$ é dito **aditivo** se, para todo $A, B \in \mathcal{O}b(\mathcal{C})$, segue que:*

$$F(f+g) = Ff + Fg \ \forall \ f, g \in Hom_{\mathcal{C}}(A, B).$$

Um grupo ou módulo unitário é único a menos de isomorfismo, é denominado **objeto trivial** e é denotado por 0. Em particular, todo funtor aditivo mapeia todo objeto trivial em um objeto trivial, e mapeia todo morfismo nulo em um morfismo nulo.

2.3 Produtos e coprodutos

Nesta seção, serão definidos os conceitos de produto e coproduto em uma categoria e serão demonstradas propriedades de produtos e coprodutos de módulos.

Por toda a seção, R denotará um anel arbitrário.

Definição 2.3.1. *Sejam $\mathcal{C}$ uma categoria e $(X_j)_{j \in J}$ uma família de objetos de $\mathcal{C}$. Um **produto** para $(X_j)_{j \in J}$ em $\mathcal{C}$ é um objeto $\prod_{j \in J} X_j$ de $\mathcal{C}$, munido de uma família $(p_j)_{j \in J}$*

*de morfismos de $\mathcal{C}$, em que $p_k \in Hom_{\mathcal{C}}(\prod_{j\in J} X_j, X_k)$ e é denominada k-**ésima projeção canônica** para todo $k \in J$, que satisfaz a seguinte propriedade universal:*

Para todo $A \in \mathcal{O}b(\mathcal{C})$ e para toda família de morfismos $(f_j)_{j\in J}$ tal que $f_j \in Hom_{\mathcal{C}}(A, X_j)$ para todo $j \in J$, existe um único morfismo $f \in Hom_{\mathcal{C}}(A, \prod_{j\in J} X_j)$ tal que $f_j = p_j f$ para todo $j \in J$.

Equivalentemente, o seguinte diagrama comuta (para todo $k \in J$):

$$\begin{tikzcd} A \arrow[r, dashed, "f"] \arrow[dr, "f_k"'] & \prod_{j\in J} X_j \arrow[d, "p_k"] \\ & X_k \end{tikzcd}$$

Definição 2.3.2. *Sejam $\mathcal{C}$ uma categoria e $(X_j)_{j\in J}$ uma família de objetos de $\mathcal{C}$. Um **coproduto** para $(X_j)_{j\in J}$ em $\mathcal{C}$ é um objeto $\coprod_{j\in J} X_j$ de $\mathcal{C}$, munido de uma família $(i_j)_{j\in J}$ de morfismos de $\mathcal{C}$, em que $i_k \in Hom_{\mathcal{C}}(X_k, \coprod_{j\in J} X_j)$ e é denominada k-**ésima injeção canônica** para todo $k \in J$, que satisfaz a seguinte propriedade universal:*

Para todo $A \in \mathcal{O}b(\mathcal{C})$ e para toda família de morfismos $(f_j)_{j\in J}$ tal que $f_j \in Hom_{\mathcal{C}}(X_j, A)$ para todo $j \in J$, existe um único morfismo $f \in Hom_{\mathcal{C}}(\coprod_{j\in J} X_j, A)$ tal que $f_j = f i_j$ para todo $j \in J$.

Equivalentemente, o seguinte diagrama comuta (para todo $k \in J$):

$$\begin{tikzcd} A & \coprod_{j\in J} X_j \arrow[l, dashed, "f"'] \\ & X_k \arrow[ul, "f_k"] \arrow[u, "i_k"'] \end{tikzcd}$$

Em particular, se R é um anel e $\mathcal{C} \in \{\mathbf{Ab}, {}_R\mathbf{Mod}, \mathbf{Mod}_R\}$, então um coproduto $\coprod_{j\in J} X_j$ em $\mathcal{C}$ é também chamado de **soma direta** e denotado por $\bigoplus_{j\in J} X_j$; se um objeto Y de $\mathcal{C}$ é isomorfo a X_k para algum $k \in J$, então Y é dito um **somando direto** de $\bigoplus_{j\in J} X_j$.

Os conceitos de produto e coproduto são duais, ou seja, um produto em uma categoria é um coproduto em sua categoria oposta (e vice-versa).

O conceito de coproduto na categoria **Grp** coincide com o conceito de produto livre.

Lema 2.3.3. *Sejam $\mathcal{C}$ uma categoria e $(X_j)_{j\in J}$ uma família de objetos de $\mathcal{C}$. Se P e P' são produtos para $(X_j)_{j\in J}$ em $\mathcal{C}$, então $P \simeq P'$.*

Demonstração. Sejam $p_j : P \to X_j$ e $p'_j : P' \to X_j$ as projeções canônicas. Como P é um produto para $(X_j)_{j\in J}$, então existe um morfismo $\phi : P' \to P$ tal que $p'_j = p_j\phi$ para todo $j \in J$. Analogamente, como P' é um produto para $(X_j)_{j\in J}$, então existe um morfismo $\psi : P \to P'$ tal que $p_j = p'_j\psi$ para todo $j \in J$. Portanto, $p'_j = p'_j\psi\phi$ e $p_j = p_j\phi\psi$ para todo $j \in J$. Como $p_j 1_P = p_j = p_j(\phi\psi)$ para todo $j \in J$ e P é um produto para $(X_j)_{j\in J}$, então $\phi\psi = 1_P$. Analogamente, $\psi\phi = 1_{P'}$, logo $P \simeq P'$. *QED.*

Lema 2.3.4. *Sejam $\mathcal{C}$ uma categoria e $(X_j)_{j\in J}$ uma família de objetos de $\mathcal{C}$. Se C e C' são coprodutos para $(X_j)_{j\in J}$ em $\mathcal{C}$, então $C \simeq C'$.*

Demonstração. A demonstração é dual à do Lema 2.3.3. *QED.*

Pelo restante da seção, será suposto, durante as demonstrações, que $\mathcal{C} = {}_R\mathbf{Mod}$ (o caso $\mathcal{C} = \mathbf{Mod}_R$ é análogo).

Teorema 2.3.5. *Sejam $\mathcal{C} \in \{\boldsymbol{Ab}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R\}$ e $(X_j)_{j\in J}$ uma família de objetos de $\mathcal{C}$. Então, a família $(X_j)_{j\in J}$ admite um produto $\prod_{j\in J} X_j$ em $\mathcal{C}$.*

Demonstração. Defina

$$\prod_{j\in J} X_j := \left\{ \phi : J \to \bigsqcup_{j\in J} X_j \;\middle|\; \phi(j) \in X_j \ \forall\, j \in J \right\},$$

$$p_k : \prod_{j\in J} X_j \to X_k \;\Big|\; \phi \mapsto \phi(k) \;\forall\; k \in J.$$

Defina $+ : \prod_{j\in J} X_j \times \prod_{j\in J} X_j \to \prod_{j\in J} X_j$ e $\cdot : R \times \prod_{j\in J} X_j \to \prod_{j\in J} X_j$ de modo que, para todo $r \in R$ e para todo $\phi, \psi \in \prod_{j\in J} X_j$, tem-se que:

$$(\phi + \psi)(j) = \phi(j) + \psi(j) \;\forall\; j \in J \;,\; (r \cdot \phi)(j) = r \cdot \phi(j) \;\forall\; j \in J.$$

Assim, $\prod_{j\in J} X_j$ é um R-módulo à esquerda (munido de $+$ e $.$). Por definição:

$$p_k \in Hom(\prod_{j\in J} X_j, A) \;\forall\; k \in J.$$

Sejam $A \in \mathcal{O}b(\mathcal{C})$ e $(f_j)_{j\in J}$ uma família tal que $f_j \in Hom_{\mathcal{C}}(A, X_j)$ para todo $j \in J$. Defina

$$f : A \to \prod_{j\in J} X_j \;\Big|\; a \mapsto f(a),$$

$$f(a) : J \to \coprod_{j\in J} X_j \;\Big|\; j \mapsto f_j(a).$$

Segue da definição que $f_j = p_j f$ para todo $j \in J$. Além disso, como $f_j \in Hom_{\mathcal{C}}(A, X_j)$ para todo $j \in J$, então $f \in Hom_{\mathcal{C}}(A, \prod_{j\in J})$. Por fim, se $g \in Hom_{\mathcal{C}}(A, \prod_{j\in J})$ e $f_j = p_j g$ para todo $j \in J$, então $f(a)(j) = f_j(a) = g(a)(j)$ para todo $j \in J$ e para todo $a \in A$, logo $f = g$. Portanto, $\prod_{j\in J} X_j$ é um produto para $(X_j)_{j\in J}$ em $\mathcal{C}$. *QED.*

Denota-se $\phi \in \prod_{j\in J} X_j$ por $(\phi(j))_{j\in J}$. Segue da demonstração anterior que p_j é sobrejetiva para todo $j \in J$.

Teorema 2.3.6. *Sejam $\mathcal{C} \in \{\boldsymbol{Ab}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R\}$ e $(X_j)_{j\in J}$ uma família de objetos de $\mathcal{C}$. Então, a família $(X_j)_{j\in J}$ admite um coproduto $\coprod_{j\in J} X_j$ em $\mathcal{C}$.*

Demonstração. Defina

$$i_k : X_k \to \prod_{j\in J} X_j \;\Big|\; x \mapsto i_k(x) \;\forall\; k \in J,$$

$$i_k(x) : J \to \coprod_{j\in J} X_j \;\Big|\; j \mapsto \begin{cases} x, & se\ j = k \\ 0, & se\ j \neq k \end{cases},$$

$$S = \{i_j(x) : j \in J, x \in X_j\}.$$

Defina $\coprod_{j\in J} X_j := \langle S \rangle$ (como submódulo de $\prod_{j\in J} X_j$). Por definição:

$$i_k \in Hom_{\mathcal{C}}(A, \coprod_{j\in J} X_j)\ \forall\ k \in J.$$

Sejam $A \in \mathcal{O}b(\mathcal{C})$ e $(f_j)_{j\in J}$ uma família tal que $f_j \in Hom_{\mathcal{C}}(X_j, A)$ para todo $j \in J$. Defina $F : S \to A$ dada por $i_j(x) \mapsto f_j(x)$. Como $f_j \in Hom_{\mathcal{C}}(X_j, A)$ para todo $j \in J$ e

$$i_j(x) = i_k(y) \iff j = k\ ,\ x = y,$$

então F está bem definida e pode ser estendida a um R-homomorfismo

$$f : \langle S \rangle \to A.$$

Segue da definição que $f_j = fi_j$ para todo $j \in J$. Por fim, se $g \in Hom_{\mathcal{C}}(\langle S \rangle, A)$ e $f_j = gi_j$ para todo $j \in J$, então $f|_S = g|_S$, logo $f = g$ (pela Proposição 2.1.11). Portanto, $\coprod_{j\in J} X_j$ é um coproduto para $(X_j)_{j\in J}$ em $\mathcal{C}$. *QED.*

Segue da demonstração anterior que i_j é injetiva para todo $j \in J$. Segue das demonstrações dos Teoremas 2.3.5 e 2.3.6 que o produto e o coproduto de uma família finita de módulos são iguais.

A seguir, apresentam-se algumas propriedades do produto e do coproduto.

Proposição 2.3.7. *Sejam $\mathcal{C} \in \{\boldsymbol{Ab}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R\}$, $(X_j)_{j\in J}$, $(Y_j)_{j\in J}$ famílias de objetos de $\mathcal{C}$ e $(f_j)_{j\in J}$ uma família tal que $f_j \in Hom_{\mathcal{C}}(X_j, Y_j)$ para todo $j \in J$. Então, existe um único morfismo $\prod_{j\in J} f_j \in Hom_{\mathcal{C}}(\prod_{j\in J} X_j, \prod_{j\in J} Y_j)$ tal que $\mu_k\left(\prod_{j\in J} f_j\right) = f_k\lambda_k$ para todo $k \in J$, em que $\lambda_k : \prod_{j\in J} X_j \to X_k$ e $\mu_k : \prod_{j\in J} Y_j \to Y_k$ são as k-ésimas projeções para todo $k \in J$. Além disso:*

1. $\prod_{j\in J}(rf_j) = r\left(\prod_{j\in J} f_j\right)\ \forall\ r \in R$;

2. *Se* $X_j = Y_j$ *para todo* $j \in J$, *então* $\prod_{j\in J} 1_{X_j} = 1_X$;

3. $\prod_{j\in J} f_j$ *é injetiva se, e somente se,* f_k *é injetiva para todo* $k \in J$;

4. $\prod_{j\in J} f_j$ *é sobrejetiva se, e somente se,* f_k *é sobrejetiva para todo* $k \in J$.

Demonstração. A existência e unicidade de $\prod_{j\in J} f_j$ e os itens 1 e 2 seguem da definição de produto. Os itens 3 e 4 seguem da construção explícita do produto no Teorema 2.3.5. *QED.*

Proposição 2.3.8. *Sejam* $\mathcal{C} \in \{\boldsymbol{Ab}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R\}$, $(X_j)_{j\in J}$, $(Y_j)_{j\in J}$ *famílias de objetos de* $\mathcal{C}$ *e* $(f_j)_{j\in J}$ *uma família tal que* $f_j \in Hom_{\mathcal{C}}(X_j, Y_j)$ *para todo* $j \in J$. *Então, existe um único morfismo* $\coprod_{j\in J} f_j \in Hom_{\mathcal{C}}(\coprod_{j\in J} X_j, \coprod_{j\in J} Y_j)$ *tal que* $\left(\coprod_{j\in J} f_j\right)\lambda_k = \mu_k f_k$ *para todo* $k \in J$, *em que* $\lambda_k : X_k \to \coprod_{j\in J} X_j$ *e* $\mu_k : Y_k \to \coprod_{j\in J} Y_j$ *são as* k*-ésimas injeções para todo* $k \in J$. *Além disso:*

1. $\coprod_{j\in J}(rf_j) = r\left(\coprod_{j\in J} f_j\right)\ \forall\ r \in R$;

2. *Se* $X_j = Y_j$ *para todo* $j \in J$, *então* $\coprod_{j\in J} 1_{X_j} = 1_X$;

3. $\coprod_{j\in J} f_j$ *é injetiva se, e somente se,* f_k *é injetiva para todo* $k \in J$;

4. $\coprod_{j\in J} f_j$ *é sobrejetiva se, e somente se,* f_k *é sobrejetiva para todo* $k \in J$.

Demonstração. A existência e unicidade de $\coprod_{j\in J} f_j$ e os itens 1 e 2 seguem da definição de coproduto. Os itens 3 e 4 seguem da construção explícita do coproduto no Teorema 2.3.6. *QED.*

Lema 2.3.9. *Sejam* M *um* R*-módulo e* A, B *submódulos de* M *tais que* $A + B = M$ *e* $A \cap B = 0$. *Então,* $M \simeq A \oplus B$. *(Nesse caso, denota-se* $M = A \oplus B$*).*

Demonstração. Sejam $\alpha : A \to M$ e $\beta : B \to M$ as inclusões. Como $A + B = M$ e $A \cap B = 0$, então (pela Proposição 2.1.8), para todo $m \in M$, existe um único par $(m_a, m_b) \in A \times B$ tal que $m = m_a + m_b$. Sejam X um R-módulo à esquerda e $f : A \to X$

e $g : B \to X$ homomorfismos. Seja $h : M \to X$ dada por $(m_a, m_b) \mapsto f(m_a) + g(m_b)$; assim, h está bem definida e é um homomorfismo tal que $f = h\alpha$ e $g = h\beta$. Se $h' : M \to X$ é um homomorfismo tal que $f = h\alpha$ e $g = h\beta$, então:

$$h'(m_a + m_b) = h'(m_a) + h'(m_b) = f(m_a) + g(m_b) = h(m_a + m_b) \ \forall \ (m_a, m_b) \in A \times B.$$

logo $h' = h$. Portanto, $M \simeq A \oplus B$. *QED.*

Lema 2.3.10. *Sejam A, B R-módulos ambos à esquerda (ou ambos à direita), e $i : A \to B$ um homomorfismo injetivo. Então, A é um somando direto de B se, e somente se, existe um homomorfismo $p : B \to A$ tal que $pi = 1_A$.*

Demonstração.

1. Suponha que A é um somando direto de B. Logo, existe um módulo C tal que $i(A) \oplus C = B$. Seja $\lambda : i(A) \to B$ a injeção canônica. Pela propriedade universal do coproduto, existe um homomorfismo $\pi : B \to i(A)$ tal que $1_{i(A)} = \pi\lambda$. Seja $p = i^{-1}\pi\lambda$. Logo, $p : B \to A$ é um homomorfismo tal que $pi = 1_A$.

2. Suponha que existe um homomorfismo $p : B \to A$ tal que $pi = 1_A$. Logo:

$$ker(p) \cap i(A) = 0.$$

   Além disso, como $im(ip) \subseteq i(A)$, $im(1_B - ip) \subseteq ker(p)$ e $1_B = ip + (1_B - ip)$, então $B = ker(p) + i(A)$. Como $ker(p) \cap i(A) = 0$ e $B = ker(p) + i(A)$, então, pelo Lema 2.3.9, $B = ker(p) \oplus i(A)$. Logo, A é um somando direto de B.

QED.

Lema 2.3.11. *Sejam A, B, C R-módulos todos à esquerda (ou todos à direita) e $p_A : C \to A$, $p_B : C \to B$, $i_A : A \to C$, $i_B : B \to C$ homomorfismos tais que $p_A i_A = 1_A$, $p_B i_B = 1_B$ e $i_A p_A + i_B p_B = 1_C$. Então, $A \oplus B \simeq C$, $ker(p_A) = im(i_B)$ e $ker(p_B) = im(i_A)$.*

Demonstração. Como $i_A p_A + i_B p_B = 1_C$, então $im(i_A) + im(i_B) = C$. Como $p_A i_A = 1_A$, então $i_A p_A i_A = i_A$, logo $i_B p_B i_A = 0$ (pois $i_A p_A + i_B p_B = 1_C$); como i_B é injetiva, então

$p_B i_A = 0$, logo $im(i_A) \cap im(i_B) = 0$ (pois $p_B i_B = 1_B$). Como $im(i_A) + im(i_B) = C$ e $im(i_A) \cap im(i_B) = 0$, então $im(i_A) \oplus im(i_B) = C$ (pelo Lema 2.3.9), logo $A \oplus B \simeq C$ (pois i_A, i_B são injetivas, visto que $p_A i_A = 1_A$ e $p_B i_B = 1_B$). Como $im(i_A) + im(i_B) = C$, $p_B i_B = 1_B$ e $p_B i_A = 0$, então $ker(p_B) = im(i_A)$; analogamente, $ker(p_A) = im(i_B)$. *QED.*

Proposição 2.3.12. *Sejam $\mathcal{C} \in \{\boldsymbol{Ab}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R\}$, $T : \mathcal{C} \to \boldsymbol{Ab}$ um funtor aditivo e $A, B \in \mathcal{O}b(\mathcal{C})$. Então, $T(A \oplus B) \simeq T(A) \oplus T(B)$. Além disso, se $p_A : A \oplus B \to A$ e $p_B : A \oplus B \to B$ são as projeções canônicas, e $i_A : A \to A \oplus B$ e $i_B : B \to A \oplus B$ são as injeções canônicas, então $ker(Tp_A) = im(Ti_B)$ e $ker(Tp_B) = im(Ti_A)$.*

Demonstração. Suponha que T é covariante (o caso contravariante é análogo). Seja $C = A \oplus B$. Pelas construções explícitas do produto e coproduto, segue que:

$$p_A i_A = 1_A,\ p_B i_B = 1_B,\ i_A p_A + i_B p_B = 1_C.$$

Como T é um funtor aditivo, então:

$$(Tp_A)(Ti_A) = 1_{TA},\ (Tp_B)(Ti_B) = 1_{TB},\ (Ti_A)(Tp_A) + (Ti_B)(Tp_B) = 1_{TC}.$$

Assim, pelo Lema 2.3.11, segue que:

$$ker(Tp_A) = im(Ti_B),\ ker(Tp_B) = im(Ti_A),\ T(C) = T(A) \oplus T(B).$$

Portanto, $T(A \oplus B) = T(A) \oplus T(B)$. *QED.*

2.4 Grupos abelianos livres

Nesta seção, serão apresentados resultados importantes sobre grupos abelianos livres.

A teoria apresentada nesta seção é baseada na seção 1.7 do livro *Algebra* (referência [5]), de Serge Lang.

Definição 2.4.1. *Um grupo G é dito* ***abeliano livre*** *se existe um grupo livre F tal que $G \simeq F/F'$. Se X é uma base de F, então $p(X)$ é dita uma* ***base*** *de G, em que $p : F \to F/F'$ é dada por $u \mapsto uF'$.*

Lema 2.4.2. *Sejam F um grupo livre com base X e $p : F \to F/F'$ dada por $u \mapsto uF'$. Então, $p|_X$ é injetiva.*

Demonstração. Sejam $M(X)$, $\mathcal{F}(X)$ e $\sim$ conforme definidos no Teorema 1.2.4. Pelo Lema 1.2.3 e pelo Teorema 1.2.4, segue que $F \simeq \mathcal{F}(X)$ (pelo restante da demonstração, F será identificado com $\mathcal{F}(X)$). Seja $x \in X$. Defina:

$$I_x : M(X) \to \mathbb{Z} \ \mid \ (x_1, ..., x_n) \mapsto |\{i \in \{1, ..., n\} : x_i = x\}| - |\{i \in \{1, ..., n\} : x_i = x^{-1}\}|.$$

Por definição, se $g, h \in M(X)$ são tais que h é redução elementar de g, então $I_x(g) = I_x(h)$. Logo, dados $g, h \in M(X)$ tais que $g \sim h$, vale que $I_x(g) = I_x(h)$. Portanto, a seguinte função está bem definida:

$$i_x : \mathcal{F}(X) \to \mathbb{Z} \ \mid \ [g] \mapsto I_x(g).$$

Por definição, $i_x(gh) = i_x(g)+i_x(h)$ para todo $g, h \in \mathcal{F}(X)$, logo i_x é um homomorfismo de grupos. Como $\mathbb{Z}$ é abeliano, então $\mathcal{F}(X)' \subseteq ker(i_x)$ (pelo Lema 1.1.6). Sejam $x_1, x_2 \in X$ tais que $x_1 \neq x_2$; assim, $i_{x_1}(x_1x_2^{-1}) = 1$, logo $x_1x_2^{-1} \notin ker(i_{x_1})$, portanto $x_1x_2^{-1} \notin \mathcal{F}(X)'$, o que implica que $p|_X$ é injetiva. *QED.*

Como $p|_X$ é injetiva, então, pelo restante do texto, $p(X)$ será identificado com X.

Proposição 2.4.3. *Seja X um conjunto. Então, existe um grupo abeliano livre G com base X.*

Demonstração. Segue do Teorema 1.2.4 e do Lema 2.4.2. *QED.*

Proposição 2.4.4. *Sejam G um grupo abeliano livre com base X, H um grupo abeliano e $f : X \to H$ uma função. Então, existe um único homomorfismo de grupos $\overline{f} : G \to H$ tal que $\overline{f}|_X = f$.*

Demonstração. Seja F um grupo livre com base Y tal que $G \simeq F/F'$. Seja $p : F \to F/F'$ dada por $u \mapsto uF'$. Como F é um grupo livre, então existe um homomorfismo $\phi : F \to H$ tal que $\phi|_Y = fp|_Y$. Como H é abeliano, então $F' \subseteq ker(\phi)$, logo a função $\overline{f} : F/F' \to H \mid uF' \mapsto \phi(u)$ está bem definida e é um homomorfismo. Como $\phi|_Y = fp|_Y$ e $p(Y) = X$, então $\overline{f}|_X = f$. Suponha que $g : F/F' \to H$ é um homomorfismo tal que $g|_X = f$. Então, $g|_X = \overline{f}|_X$, logo $gp|_X = \overline{f}p|_X$. Como F é livre, então $gp = \overline{f}p$, logo $g = \overline{f}$ (pois p é sobrejetiva). *QED.*

Proposição 2.4.5. *Sejam A um grupo abeliano, B um grupo abeliano livre e $\phi : A \to B$ um homomorfismo sobrejetivo. Então, existe um homomorfismo $\gamma : B \to A$ tal que $\phi\gamma = 1_B$ e $A = ker(\phi) \oplus \gamma(B)$.*

Demonstração. Seja X uma base de B (como grupo abeliano livre). Como $\phi : A \to B$ é sobrejetivo, então existe uma função $\lambda : X \to A$ tal que $\phi\lambda = 1_X$. Como B é grupo abeliano livre com base X, então existe um homomorfismo $\gamma : B \to A$ tal que $\gamma|_X = \lambda$; além disso, como $\phi\lambda = 1_X$, então $\phi\gamma = 1_B$. Como $\phi\gamma = 1_B$, então $\phi\gamma(b) = 0 \iff b = 0$, logo $ker(\phi) \cap \gamma(B) = 0$. Além disso, como $\phi\gamma = 1_B$, então $\phi(1_A - \gamma\phi) = 0$, logo $(1_A - \gamma\phi)(A) \subseteq ker(\phi)$. Como $1_A = (1_A - \gamma\phi) + \gamma\phi$ e $(1_A - \gamma\phi)(A) \subseteq ker(\phi)$, então $A = \ker(\phi) + \gamma(B)$. Como $ker(\phi) \cap \gamma(B) = 0$ e $A = \ker(\phi) + \gamma(B)$, então, pelo Lema 2.3.9, $A = ker(\phi) \oplus \gamma(B)$. *QED.*

Proposição 2.4.6. *Sejam A um grupo abeliano livre finitamente gerado com base α e B um subgrupo de A. Então, B é um grupo abeliano livre. Além disso, se β é base de B, então $|\beta| \leq |\alpha|$.*

Demonstração. Se $|\alpha| = 1$, então $A \simeq \mathbb{Z}$, logo $B = 0$ ou $B \simeq \mathbb{Z}$, portanto B é um grupo abeliano livre e $|\beta| \leq 1 = |\alpha|$. Suponha, por hipótese indutiva, que todo subgrupo de um grupo abeliano livre cuja base tem cardinalidade n é um grupo abeliano livre cuja base tem cardinalidade menor ou igual a n. Suponha que $|\alpha| = n + 1$. Assim, existem $x_1, ..., x_{n+1} \in A$ tais que $A \simeq \oplus_{i=1}^{n+1}\mathbb{Z}x_i$. Seja $\psi : \oplus_{i=1}^{n+1}\mathbb{Z}x_i \to \mathbb{Z}x_{n+1}$ dada por:

$$(z_1, ..., z_{n+1}) \mapsto z_{n+1}.$$

Assim, $ker(\psi) = (\oplus_{i=1}^{n}\mathbb{Z}x_i) \oplus 0 \simeq \oplus_{i=1}^{n}\mathbb{Z}x_i$, logo $B \cap ker(\psi)$ é isomorfo a um subgrupo de $\oplus_{i=1}^{n}\mathbb{Z}x_i$, portanto $B \cap ker(\psi)$ é subgrupo de um grupo abeliano livre cuja base tem cardinalidade n. Por hipótese indutiva, $B \cap ker(\psi)$ é grupo abeliano livre, e, se β' é base de $B \cap ker(\psi)$, então $|\beta'| \leq n$. Pela Proposição 2.4.5, existe um homomorfismo $\gamma : \mathbb{Z}x_i \to A$ tal que $\psi\gamma = 1_{\mathbb{Z}x_{n+1}}$ e $A = ker(\psi) \oplus \gamma(\mathbb{Z}x_{n+1})$; em particular, $\gamma(\mathbb{Z}x_{n+1}) \simeq 0$ ou $\gamma(\mathbb{Z}x_{n+1}) \simeq \mathbb{Z}$, e $B = (B \cap ker(\psi)) \oplus (B \cap \gamma(\mathbb{Z}x_{n+1}))$. Assim, $B \simeq (B \cap ker(\psi)) \oplus 0$ ou $B \simeq (B \cap ker(\psi)) \oplus \mathbb{Z}$, logo B é grupo abeliano livre e, se β é base de B, então:

$$|\beta| \leq |\beta'| + 1 \leq n + 1 = |\alpha|.$$

Por indução (na cardinalidade da base), fica demonstrado o Lema. *QED.*

Corolário 2.4.7. *Sejam A um grupo abeliano finitamente gerado e B um subgrupo de A. Então, B é finitamente gerado.*

Demonstração. Como A é finitamente gerado, existem F um grupo livre finitamente gerado e $R \lhd F$ tais que $A \simeq F/R$. Como A é abeliano, então $F' \subseteq R$, logo:

$$A \simeq (F/F')/(R/F').$$

Como B é um subgrupo de A, então existe um subgrupo G de F/F' tal que $B \simeq G/(R/F')$. Como F/F' é um grupo abeliano livre finitamente gerado, então G é finitamente gerado (pela Proposição 2.4.6), logo B é finitamente gerado. *QED.*

Teorema 2.4.8. *Sejam A um grupo abeliano livre e B um subgrupo de A. Então, B é um grupo abeliano livre.*

Demonstração. Suponha que B não é trivial. Seja $X = (x_i)_{i \in I}$ uma base de A. Dado $J \subseteq I$, sejam A_J o subgrupo (livre) de A gerado por $(x_j)_{j \in J}$ e $B_J := B \cap A_J$. Seja $\mathcal{L}$ o conjunto das triplas (J, J', f), em que $\emptyset \neq J' \subseteq J \subseteq I$ e $f : J' \to B_J$ é uma função injetiva tal que $f(J')$ é base de B_J (como grupo abeliano livre). Como $B \neq 0$, então $0 \neq B_J \subseteq A_J$ para algum $J \subseteq I$, logo $\mathcal{L} \neq \emptyset$ (pela Proposição 2.4.6). Seja $\leq$ a relação de ordem parcial em $\mathcal{L}$ dada por:

$$(J, J', f) \leq (K, K', g) \iff J \subseteq K, \ J' \subseteq K', \ g|_{J'} = f.$$

Se $C = (J_\lambda, J'_\lambda, f_\lambda)_{\lambda \in \Lambda}$ é uma cadeia em $(\mathcal{L}, \leq)$, então (J, J', f) é uma cota superior para C, em que $J = \cup_{\lambda \in \Lambda} J_\lambda$, $J' = \cup_{\lambda \in \Lambda} J'_\lambda$ e $f : J' \to B_J$ é tal que $f(j) = f_\lambda(j)$ se $j \in J'_\lambda$ (f está bem definida pois $(J_\lambda, J'_\lambda, f_\lambda)_{\lambda \in \Lambda}$ é cadeia). Assim, pelo Lema de Zorn (Corolário 2.5 do Apêndice 2 da referência [5]), $(\mathcal{L}, \leq)$ admite um elemento maximal (J, J', f).

Seja $i \in I$. Suponha, por absurdo, que $B_{J \cup \{i\}} \neq B_J$. Portanto:

$$S := \{\alpha \in \mathbb{Z} \mid \exists\ y \in B_J : \alpha x_i + y \in B\} \neq \{0\}.$$

Por definição, S é subgrupo de $\mathbb{Z}$, logo existe $\mu \in \mathbb{Z} \backslash \{0\}$ tal que $S = \mathbb{Z}\mu$. Seja $y \in B_J$ tal que $f_i := \mu x_i + y \in B$. Seja $z \in B_{J \cup \{i\}}$. Por definição de $B_{J \cup \{i\}}$ e S, existem $\alpha \in S$ e $b \in B_J$ tais que $z = \alpha x_i + u$. Assim, existe $\beta \in \mathbb{Z}$ tal que $z - \beta f_i \in A_J$. Como $z, f_i \in B$, então $z - \beta f_i \in B$, logo $z - \beta f_i \in B_J$. Portanto, $B_J + \mathbb{Z} f_i = B_{J \cup \{i\}}$. Como $B_J \cap \mathbb{Z} f_i = 0$, então, pelo Lema 2.3.9, $B_J \oplus \mathbb{Z} f_i = B_{J \cup \{i\}}$, logo $f'(J' \cup \{i\})$ é base de $B_{J \cup \{i\}}$, em que $f' : J' \cup \{i\} \to B_{J \cup \{i\}}$ é tal que $f'|_{J'} = f$ e $f'(i) = f_i$. Assim, $(J \cup \{i\}, J' \cup \{i\}, f') \in \mathcal{L}$ e $(J, J', f) \leq (J \cup \{i\}, J' \cup \{i\}, f')$; logo, pela maximalidade de (J, J', f), segue que $(J, J', f) = (J \cup \{i\}, J' \cup \{i\}, f')$, portanto $B_{J \cup \{i\}} = B_J$, o que é uma contradição. Logo:

$$B_{J \cup \{i\}} = B_J.$$

Como $B_{J \cup \{i\}} = B_J$, então $(J \cup \{i\}, J', f) \in \mathcal{L}$ e $(J, J', f) \leq (J \cup \{i\}, J', f)$; logo, pela maximalidade de (J, J', f), segue que $(J, J', f) = (J \cup \{i\}, J', f)$, portanto $i \in J$. Assim, conclui-se que $J = I$. Como $(J, J', f) \in \mathcal{L}$, então, por definição de $\mathcal{L}$, $B_J = B_I = B$ é um grupo abeliano livre. *QED.*

2.5 O funtor Hom

Nesta seção, será construído o funtor Hom.

Definição 2.5.1. *Sejam $\mathcal{C}$ uma categoria, $A, X, Y \in \mathcal{O}b(\mathcal{C})$ e $f \in Hom_{\mathcal{C}}(X, Y)$. O* ***pushforward*** *de f com respeito a A é definido como o morfismo*

$$f_* : Hom_{\mathcal{C}}(A, X) \to Hom_{\mathcal{C}}(A, Y) \ \mid \ g \mapsto fg.$$

Além disso, o ***pullback*** *de f com respeito a A é definido como o morfismo*

$$f^* : Hom_{\mathcal{C}}(Y, A) \to Hom_{\mathcal{C}}(X, A) \ \mid \ g \mapsto gf.$$

Proposição 2.5.2. *Sejam $\mathcal{C}$ uma categoria, $X, Y, Z \in \mathcal{O}b(\mathcal{C})$, $f \in Hom_{\mathcal{C}}(X, Y)$ e $g \in Hom_{\mathcal{C}}(Y, Z)$. Então, $(gf)_* = g_* f_*$ e $(gf)^* = f^* g^*$.*

Demonstração. Seja $A \in \mathcal{O}b(\mathcal{C})$. Por definição, tem-se que:

$$(gf)_*(\phi) = (gf)\phi = g(f\phi) = g(f_*(\phi)) = g_*(f_*(\phi)) = (g_* f_*)(\phi) \ \forall \ \phi \in Hom_{\mathcal{C}}(A, X),$$

$$(gf)^*(\phi) = \phi(gf) = (\phi g)f = (g^*(\phi))f = f^*(g^*(\phi)) = (f^* g^*)(\phi) \ \forall \ \phi \in Hom_{\mathcal{C}}(A, X).$$

Portanto, $(gf)_* = g_* f_*$ e $(gf)^* = f^* g^*$. *QED.*

Proposição 2.5.3. *Sejam R um anel, $\mathcal{C} \in \{\boldsymbol{Ab}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R\}$, $A, X, Y \in \mathcal{O}b(\mathcal{C})$ e $f, g \in Hom_{\mathcal{C}}(X, Y)$. Então:*

$$f_* \in Hom_{\boldsymbol{Ab}}(Hom_{\mathcal{C}}(A, X), Hom_{\mathcal{C}}(A, Y)),$$

$$f^* \in Hom_{\boldsymbol{Ab}}(Hom_{\mathcal{C}}(Y, A), Hom_{\mathcal{C}}(X, A)).$$

Além disso, $(f + g)_* = f_* + g_*$ e $(f + g)^* = f^* + g^*$.

Demonstração. Por definição, tem-se que:

$$f_*(\phi + \psi) = f(\phi + \psi) = f\phi + f\psi = f_*(\phi) + f_*(\psi) \ \forall \ \phi, \psi \in Hom_{\mathcal{C}}(A, X),$$

$$f^*(\phi + \psi) = (\phi + \psi)f = \phi f + h\psi = f^*(\phi) + f^*(\psi) \ \forall \ \phi, \psi \in Hom_{\mathcal{C}}(Y, A).$$

Portanto:

$$f_* \in Hom_{\mathbf{Ab}}(Hom_{\mathcal{C}}(A, X), Hom_{\mathcal{C}}(A, Y)),$$

$$f^* \in Hom_{\mathbf{Ab}}(Hom_{\mathcal{C}}(Y, A), Hom_{\mathcal{C}}(X, A)).$$

Além disso:

$$(f + g)_*(\phi) = (f + g)\phi = f\phi + g\phi = f_*(\phi) + g_*(\phi) = (f_* + g_*)(\phi) \ \forall \ \phi \in Hom_{\mathcal{C}}(A, X),$$

$$(f + g)^*(\phi) = \phi(f + g) = \phi f + \phi g = f^*(\phi) + g^*(\phi) = (f^* + g^*)(\phi) \ \forall \ \phi \in Hom_{\mathcal{C}}(Y, A).$$

Logo, $(f + g)_* = f_* + g_*$ e $(f + g)^* = f^* + g^*$. *QED.*

Teorema 2.5.4. *Sejam R um anel, $\mathcal{C} \in \{\boldsymbol{Ab}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R\}$ e $A \in \mathcal{O}b(\mathcal{C})$. Então, existe um funtor covariante aditivo $Hom_{\mathcal{C}}(A, -) : \mathcal{C} \to \boldsymbol{Ab}$ tal que:*

$$X \in \mathcal{O}b(\mathcal{C}) \mapsto Hom_{\mathcal{C}}(A, X),$$

$$f \in Hom_{\mathcal{C}}(X, Y) \mapsto f_* \in Hom_{\boldsymbol{Ab}}(Hom_{\mathcal{C}}(A, X), Hom_{\mathcal{C}}(A, Y)).$$

Além disso, existe um funtor contravariante aditivo $Hom_{\mathcal{C}}(-, A) : \mathcal{C} \to \boldsymbol{Ab}$ tal que:

$$X \in \mathcal{O}b(\mathcal{C}) \mapsto Hom_{\mathcal{C}}(X, A),$$

$$f \in Hom_{\mathcal{C}}(X, Y) \mapsto f^* \in Hom_{\boldsymbol{Ab}}(Hom_{\mathcal{C}}(Y, A), Hom_{\mathcal{C}}(X, A)).$$

Demonstração. Segue das Proposições 2.5.2 e 2.5.3. *QED.*

Conforme demonstrado a seguir, os funtores $Hom(A, -)$ e $Hom(-, B)$ tomam valores na categoria dos módulos se A e B são bimódulos.

Teorema 2.5.5. *Sejam R e S anéis. Então:*

1. *Se ${}_RA_S$ e ${}_RB$, então $Hom_{{}_R\boldsymbol{Mod}}(A, B)$ é um S-módulo à esquerda munido da apli-*

cação $\cdot : S \times Hom_{_R\boldsymbol{Mod}}(A,B) \to Hom_{_R\boldsymbol{Mod}}(A,B)$ *dada por:*

$$(s \cdot f)(a) = f(as) \ \forall \ s \in S \ \forall \ a \in A \ \forall \ f \in Hom_{_R\boldsymbol{Mod}}(A,B);$$

2. *Se* $_RA_S$ *e* B_S*, então* $Hom_{\boldsymbol{Mod}_S}(A,B)$ *é um* R*-módulo à direita munido da aplicação* $\cdot : Hom_{\boldsymbol{Mod}_S}(A,B) \times R \to Hom_{\boldsymbol{Mod}_S}(A,B)$ *dada por:*

$$(f \cdot r)(a) = f(ra) \ \forall \ r \in R \ \forall \ a \in A \ \forall \ f \in Hom_{_R\boldsymbol{Mod}}(A,B);$$

3. *Se* A_R *e* $_SB_R$*, então* $Hom_{\boldsymbol{Mod}_R}(A,B)$ *é um* S*-módulo à esquerda munido da aplicação* $\cdot : S \times Hom_{\boldsymbol{Mod}_R}(A,B) \to Hom_{\boldsymbol{Mod}_R}(A,B)$ *dada por:*

$$(s \cdot f)(a) = sf(a) \ \forall \ s \in S \ \forall \ a \in A \ \forall \ f \in Hom_{_R\boldsymbol{Mod}}(A,B);$$

4. *Se* $_SA$ *e* $_SB_R$*, então* $Hom_{_S\boldsymbol{Mod}}(A,B)$ *é um* R*-módulo à direita munido da aplicação* $\cdot : Hom_{_S\boldsymbol{Mod}}(A,B) \times R \to Hom_{_S\boldsymbol{Mod}}(A,B)$ *dada por:*

$$(f \cdot r)(a) \mapsto f(a)r \ \forall \ r \in R \ \forall \ a \in A \ \forall \ f \in Hom_{_R\boldsymbol{Mod}}(A,B).$$

Demonstração. Segue das definições de módulo e homomorfismo de módulos. QED.

Corolário 2.5.6. *Sejam* R, S *anéis,* A *um* (R,S)*-bimódulo e* B *um* (R,S)*-bimódulo. Então:*

1. $Hom_{_R\boldsymbol{Mod}}(A,-) : {_R\boldsymbol{Mod}} \to {_S\boldsymbol{Mod}}$;
2. $Hom_{\boldsymbol{Mod}_S}(A,-) : \boldsymbol{Mod}_S \to \boldsymbol{Mod}_R$;
3. $Hom_{\boldsymbol{Mod}_R}(-,B) : \boldsymbol{Mod}_R \to {_S\boldsymbol{Mod}}$;
4. $Hom_{_S\boldsymbol{Mod}}(-,B) : {_S\boldsymbol{Mod}} \to \boldsymbol{Mod}_R$.

Demonstração. Pelo Teorema 2.5.5, segue que o funtor Hom mapeia módulos em módulos. Além disso, pela Definição 2.5.1 e pelo Teorema 2.5.5, segue que o funtor Hom mapeia homomorfismos de módulos em homomorfismos de módulos. *QED.*

Teorema 2.5.7. *Sejam* $\mathcal{C} \in \{\boldsymbol{Ab}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R\}$, $A \in \mathcal{O}b(\mathcal{C})$, $(X_j)_{j\in J}$ *uma família de objetos de* $\mathcal{C}$ *e* $p_k : \prod_{j\in J} X_j \to X_k$ *a* k*-ésima projeção para todo* $k \in J$*. Então, o mapa*

$$\theta : Hom_{\mathcal{C}}\left(A, \prod_{j\in J} X_j\right) \to \prod_{j\in J} Hom_{\mathcal{C}}(A, X_j) \;\Big|\; \phi \mapsto (p_j\phi)_{j\in J}$$

é um isomorfismo de grupos abelianos.

Demonstração. Dados $\phi, \psi \in Hom_{\mathcal{C}}\left(A, \prod_{j\in J} X_j\right)$, tem-se que

$$\theta(\phi + \psi) = (p_j(\phi + \psi))_{j\in J} = (p_j\phi + p_j\psi)_{j\in J} = (p_j\phi)_{j\in J} + (p_j\psi)_{j\in J} = \theta(\phi) + \theta(\psi),$$

logo θ é um homomorfismo de grupos. Seja $(\phi_j)_{j\in J} \in \prod_{j\in J} Hom_{\mathcal{C}}(A, X_j)$. Pela propriedade universal do produto, existe $\phi \in Hom(A, \prod_{j\in J} X_j)$ tal que $\phi_j = p_j\phi$ para todo $j \in J$, ou seja, $\theta(\phi) = (\phi_j)_{j\in J}$. Logo, θ é sobrejetiva.

Seja $\psi \in ker(\theta)$. Assim, $\theta(\psi) = 0$, logo $p_j\psi = 0$ para todo $j \in J$, portanto o seguinte diagrama comuta (para todo $k \in J$):

$$\begin{tikzcd}
A \arrow[r, dashed, shift left, "\psi"] \arrow[r, dashed, shift right, "0"'] \arrow[dr, "0"'] & \prod_{j\in J} X_j \arrow[d, "p_k"] \\
 & X_k
\end{tikzcd}$$

Pela propriedade universal do produto, segue que $\psi = 0$. Como $\psi \in ker(\theta) \to \psi = 0$, então $ker(\theta) = \{0\}$, logo θ é injetiva. Portanto, θ é um isomorfismo de grupos.

QED.

Teorema 2.5.8. *Sejam $\mathcal{C} \in \{\boldsymbol{Ab}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R\}$, $B \in \mathcal{O}b(\mathcal{C})$, $(X_j)_{j\in J}$ uma família de objetos de $\mathcal{C}$ e $i_k : X_k \to \coprod_{j\in J} X_j$ a k-ésima injeção para todo $k \in J$. Então, o mapa*

$$\theta : Hom_{\mathcal{C}}\left(\coprod_{j\in J} X_j, B\right) \to \prod_{j\in J} Hom_{\mathcal{C}}(X_j, B) \;\Big|\; \phi \mapsto (\phi i_j)_{j\in J}$$

é um isomorfismo de grupos abelianos.

Demonstração. A demonstração é dual à do Teorema 2.5.7. *QED.*

2.6 O funtor *produto tensorial*

Nesta seção, será construído o funtor *produto tensorial.*

Definição 2.6.1. *Sejam R um anel, A um R-módulo à direita, B um R-módulo à esquerda e G um grupo abeliano. Uma função $f : A \times B \to G$ é dita R-**biaditiva** se:*

1. $f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b)\ \forall\ a_1, a_2 \in A\ \forall\ b \in B$;
2. $f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2)\ \forall\ a \in A\ \forall\ b_1, b_2 \in B$;
3. $f(ar, b) = f(a, rb)\ \forall\ a \in A\ \forall\ b \in B\ \forall\ r \in R$.

Definição 2.6.2. *Sejam R um anel, A um R-módulo à direita e B um R-módulo à esquerda. Um **produto tensorial** para (A, B) é um grupo abeliano $A \otimes_R B$, munido de uma aplicação R-biaditiva*

$$\phi : A \times B \to A \otimes_R B \ \mid\ (a, b) \mapsto a \otimes b,$$

que satisfaz a seguinte propriedade universal:

Para todo grupo abeliano G e para toda função R-biaditiva $\psi : A \times B \to G$, existe único homomorfismo de grupos $\overline{\psi} : A \otimes_R B \to G$ tal que $\psi = \overline{\psi}\phi$.

Equivalentemente, o seguinte diagrama comuta:

$$\begin{tikzcd}
A \times B \arrow[r, "\phi"] \arrow[dr, "\psi"'] & A \otimes_R B \arrow[d, dashed, "\overline{\psi}"] \\
 & G
\end{tikzcd}$$

Lema 2.6.3. *Sejam R um anel, A um R-módulo à direita e B um R-módulo à esquerda. Se T e T' são produtos tensoriais para (A, B), então T e T' são isomorfos como grupos abelianos.*

Demonstração. Suponha que T e T', munidos das aplicações R-biaditivas $\phi : A \times B \to T$ e $\psi : A \times B \to T'$, são produtos tensoriais para (A, B). Como T é produto tensorial para (A, B) (munido da aplicação $\phi : A \times B \to T$) e $\psi : A \times B \to T'$ é aplicação R-biaditiva, então existe um homomorfismo de grupos $\overline{\psi} : T \to T'$ tal que $\psi = \overline{\psi}\phi$. Como T' é produto tensorial para (A, B) (munido da aplicação $\psi : A \times B \to T'$) e $\phi : A \times B \to T$ é aplicação R-biaditiva, então existe um homomorfismo de grupos $\overline{\phi} : T' \to T$ tal que $\phi = \overline{\phi}\psi$. Como $\psi = \overline{\psi}\phi$ e $\phi = \overline{\phi}\psi$, então $\phi = \overline{\phi}\,\overline{\psi}\,\phi$. Portanto, o seguinte diagrama comuta:

$$\begin{tikzcd}
A \times B \arrow[r, "\phi"] \arrow[dr, "\phi"'] & T \arrow[d, dashed, shift right, "1_T"'] \arrow[d, dashed, shift left, "\overline{\phi}\,\overline{\psi}"] \\
 & T
\end{tikzcd}$$

Pela propriedade universal do produto tensorial, segue que $\overline{\phi}\,\overline{\psi} = 1_T$. Analogamente, demonstra-se que $\overline{\psi}\,\overline{\phi} = 1_{T'}$. Portanto, T e T' são isomorfos como grupos abelianos. *QED.*

Teorema 2.6.4. *Sejam R um anel, A um R-módulo à direita e B um R-módulo à esquerda. Então, (A, B) admite um produto tensorial $A \otimes_R B$.*

Demonstração. Seja H um grupo abeliano livre (aditivo) com base $A \times B$ (cuja existência é assegurada pela Proposição 2.4.3). Defina:

$$S_1 = \{(a_1 + a_2, b) - (a_1, b) - (a_2, b) : a_1, a_2 \in A, b \in B\},$$

$$S_2 = \{(a, b_1 + b_2) - (a, b_1) - (a, b_2) : a \in A, b_1, b_2 \in B\},$$

$$S_3 = \{(ar, b) - (a, rb) : r \in R, a \in A, b \in B\}.$$

Seja S o subgrupo de H gerado por $S_1 \cup S_2 \cup S_3$ e seja $A \otimes_R B := H/S$. Como H é um grupo abeliano, então $A \otimes_R B$ é um grupo abeliano. Seja $\phi : A \times B \to A \otimes_R B$ dada por $(a, b) \mapsto (a, b) + S$. Por definição, ϕ é uma aplicação R-biaditiva e $im(\phi)$ gera $A \otimes_R B$ como grupo abeliano.

Sejam G um grupo abeliano e $f : A \times B \to G$ uma função R-biaditiva. Como $f : A \times B \to G$ e H é grupo abeliano livre com base $A \times B$, então f admite uma única extensão a um homomorfismo $f' : H \to G$ (pela Proposição 2.4.4). Como $f' : H \to G$ é homomorfismo, então $S_1 \cup S_2 \cup S_3 \subseteq ker(f')$, logo $S \subseteq ker(f')$. Assim, para todo $x \in H$, f' é constante no conjunto $x + S$. Portanto, a função

$$\overline{f} : A \otimes_R B \to G \ \mid \ x + S \mapsto f'(x)$$

está bem definida e satisfaz $f = f'|_{A \times B} = \overline{f}\phi$; além disso, como $f' : H \to G$ é homomorfismo, então $\overline{f} : A \otimes_R B \to G$ é homomorfismo. Por fim, como $A \otimes_R B = H/S$ e H é grupo abeliano livre com base $A \times B$, então $im(\phi) = \{x + S : x \in A \times B\}$ gera $A \otimes_R B$.

Seja $g : A \otimes_R B \to G$ um homomorfismo tal que $f = g\phi$. Como $f = \overline{f}\phi$ e $f = g\phi$, então $\overline{f}\phi = g\phi$, logo $\overline{f}|_{im(\phi)} = g|_{im(\phi)}$. Como $\overline{f}, g \in Hom_{\mathbf{Ab}}(A \otimes_R B, G)$, $im(\phi)$ gera o grupo $A \otimes_R B$ e $\overline{f}|_{im(\phi)} = g|_{im(\phi)}$, então $\overline{f} = g$. Logo, $\overline{f} : A \otimes_R B \to G$ é o único homomorfismo tal que $f = \overline{f}\phi$. Portanto, o grupo abeliano $A \otimes_R B$, munido da aplicação R-biaditiva $\phi : A \times B \to A \otimes_R B$, é um produto tensorial para (A, B). *QED.*

Segue da demonstração anterior que o conjunto $\{a \otimes b : a \in A, b \in B\}$ gera

$A \otimes_R B$ como grupo abeliano (em que $a \otimes b := \phi(a,b)$).

Proposição 2.6.5. *Sejam R um anel, A um R-módulo à direita e B um R-módulo à esquerda. Então, $A \otimes_R B \simeq B \otimes_{R^{op}} A$.*

Demonstração. Como o mapa $\phi : A \times B \to B \otimes_{R^{op}} A$ dado por $(a,b) \mapsto b \otimes a$ é R-biaditivo, então existe um homomorfismo $\overline{\phi} : A \otimes_R B \to B \otimes_{R^{op}} A$ tal que:

$$\overline{\phi}(a \otimes b) = b \otimes a \ \forall \ (a,b) \in A \times B.$$

Analogamente, existe um homomorfismo $\overline{\psi} : B \otimes_{R^{op}} A \to A \otimes_R B$ tal que:

$$\overline{\psi}(b \otimes a) = a \otimes b \ \forall \ (a,b) \in A \times B.$$

Assim, $\overline{\psi}\,\overline{\phi}(a \otimes b) = a \otimes b$ para todo $(a,b) \in A \times B$, logo $\overline{\psi}\,\overline{\phi} = 1_{A \otimes_R B}$ (pois o conjunto $\{a \otimes b : (a,b) \in A \times B\}$ gera $A \otimes_R B$ como grupo abeliano). Analogamente, $\overline{\phi}\,\overline{\psi} = 1_{B \otimes_{R^{op}} A}$, logo $\phi : A \times B \to B \otimes_{R^{op}} A$ é um isomorfismo. *QED.*

Proposição 2.6.6. *Sejam R um anel, A um R-módulo à direita e B um R-módulo à esquerda. Então, $A \otimes_R R \simeq A$ e $R \otimes_R B \simeq B$.*

Demonstração. Seja $\phi : R \times B \to B$ dado por $(r,b) \mapsto rb$; por definição, ϕ é R-biaditiva. Portanto, existe um homomorfismo de grupos $\overline{\phi} : R \otimes_R B \to B$ tal que:

$$\overline{\phi}(r \otimes b) = rb \ \forall \ (r,b) \in R \times B.$$

Além disso, $\overline{\phi}$ é um isomorfismo pois admite inversa $\xi : \overline{\phi} : B \to R \otimes_R B$ dada por $b \mapsto 1_R \otimes b$. Analogamente, demonstra-se que $A \otimes_R R \simeq A$. *QED.*

Proposição 2.6.7. *Sejam R um anel, A, A' R-módulos à direita, B, B' R-módulos à esquerda, $f \in Hom_{\boldsymbol{Mod}_R}(A, A')$ e $g \in Hom_{{}_R\boldsymbol{Mod}}(B, B')$. Então, existe um único homomorfismo $f \otimes g : A \otimes_R B \to A' \otimes_R B'$ tal que:*

$$(f \otimes g)(a \otimes b) = f(a) \otimes g(b) \ \forall \ (a,b) \in A \times B.$$

Demonstração. Seja $\psi : A \times B \to A' \otimes_R B'$ dada por $(a,b) \mapsto f(a) \otimes g(b)$. Como $f \in Hom_{\mathbf{Mod}_R}(A, A')$, $g \in Hom_{{}_R\mathbf{Mod}}(B, B')$ e $A' \otimes_R B'$ é um produto tensorial, então $\psi : A \times B \to A' \otimes_R B'$ é uma aplicação R-biaditiva. Portanto, pela propriedade universal de $A \otimes_R B$, existe um único homomorfismo $f \otimes g : A \otimes_R B \to A' \otimes_R B'$ tal que:

$$(f \otimes g)(a \otimes b) = \psi(a,b) = f(a) \otimes g(b) \ \forall \ (a,b) \in A \times B.$$

QED.

Proposição 2.6.8. *Sejam R um anel, A_1, A_2, A_3 R-módulos à direita, B_1, B_2, B_3 R-módulos à esquerda, $f \in Hom_{\boldsymbol{Mod}_R}(A_1, A_2)$, $f' \in Hom_{\boldsymbol{Mod}_R}(A_2, A_3)$, $g \in Hom_{{}_R\boldsymbol{Mod}}(B_1, B_2)$ e $g' \in Hom_{{}_R\boldsymbol{Mod}}(B_2, B_3)$. Então:*

$$(f' \otimes g')(f \otimes g) = (f'f) \otimes (g'g).$$

Demonstração. Como $\{a \otimes b : (a,b) \in A_1 \times B_1\}$ gera $A_1 \otimes_R B_1$ como grupo abeliano, então, por definição, segue que $(f' \otimes g')(f \otimes g) = (f'f) \otimes (g'g)$. *QED.*

Proposição 2.6.9. *Sejam R um anel, A, A' R-módulos à direita, B, B' R-módulos à esquerda, $f, f' \in Hom_{\boldsymbol{Mod}_R}(A, A')$ e $g, g' \in Hom_{{}_R\boldsymbol{Mod}}(B, B')$. Então:*

$$(f + f') \otimes g = f \otimes g + f' \otimes g, \ f \otimes (g + g') = f \otimes g + f \otimes g'.$$

Demonstração. Como $\{a \otimes b : (a,b) \in A \times B\}$ gera $A \otimes_R B$ e:

$$(a + a') \otimes b = a \otimes b + a' \otimes b \ \forall \ a, a' \in A \ \forall \ b \in B,$$

$$a \otimes (b + b') = a \otimes b + a \otimes b' \ \forall \ a \in A \ \forall \ b, b' \in B.$$

então, por definição, segue que:

$$(f + f') \otimes g = f \otimes g + f' \otimes g, \ f \otimes (g + g') = f \otimes g + f \otimes g'.$$

QED.

Teorema 2.6.10. *Sejam R um anel, A um R-módulo à direita e B um R-módulo à esquerda. Então, existe um funtor covariante aditivo $A\otimes_R : {}_R\boldsymbol{Mod} \to \boldsymbol{Ab}$ tal que:*

$$X \in \mathcal{O}b({}_R\boldsymbol{Mod}) \mapsto A \otimes_R X \in \mathcal{O}b(\boldsymbol{Ab}),$$

$$f \in Hom_{{}_R\boldsymbol{Mod}}(X, Y) \mapsto 1_A \otimes f \in Hom_{\boldsymbol{Ab}}(A \otimes_R X, A \otimes_R Y).$$

Além disso, existe um funtor covariante aditivo $\otimes_R B : \boldsymbol{Mod}_R \to \boldsymbol{Ab}$ tal que:

$$X \in \mathcal{O}b(\boldsymbol{Mod}_R) \mapsto X \otimes_R B \in \mathcal{O}b(\boldsymbol{Ab}),$$

$$f \in Hom_{\boldsymbol{Mod}_R}(X, Y) \mapsto f \otimes 1_B \in Hom_{\boldsymbol{Ab}}(X \otimes_R B, Y \otimes_R B).$$

Demonstração. Segue das Proposições 2.6.7 e 2.6.8 que $A\otimes_R$ e $\otimes_R B$ são funtores covariantes, e segue da Proposição 2.6.9 que esses funtores são aditivos. *QED.*

Conforme demonstrado a seguir, se A e B são bimódulos, os funtores $A\otimes$ e $\otimes B$ tomam valores na categoria dos módulos.

Teorema 2.6.11. *Sejam R, S anéis. Então:*

1. *Se ${}_SA_R$ e ${}_RB$, defina $\lambda_s : A \to A$ dada por $a \mapsto sa$ para todo $s \in S$; então, $A \otimes_R B$ é um S-módulo à esquerda munido da aplicação $\cdot : S \times (A \otimes_R B) \to A \otimes_R B$ dada por:*
$$(s, t) \mapsto (\lambda_s \otimes 1_B)(t);$$

2. *Se A_R e ${}_RB_S$, defina $\mu_s : B \to B$ dada por $b \mapsto bs$ para todo $s \in S$; então, $A \otimes_R B$ é um S-módulo à direita munido da aplicação $\cdot : (A \otimes_R B) \times S \to A \otimes_R B$ dada por:*
$$(t, s) \mapsto (1_A \otimes \mu_s)(t).$$

Demonstração.

1. Como B é um (R,S)-bimódulo, então $\lambda_s : A \to A$ é um R-homomorfismo para todo $s \in S$. Portanto, pela Proposição 2.6.7, segue que $\lambda_s \otimes 1_B : A \otimes_R B \to A \otimes_R B$ é um homomorfismo de grupos para todo $s \in S$. Logo, $A \otimes_R B$ é um S-módulo à esquerda munido da aplicação $\cdot$.

2. A demonstração é análoga à do item 1.

QED.

Corolário 2.6.12. *Sejam R, S anéis, A um (S,R)-bimódulo e B um (R,S)-bimódulo. Então:*

1. $A\otimes_R : {}_R\boldsymbol{Mod} \to {}_S\boldsymbol{Mod}$;

2. $\otimes_R B : \boldsymbol{Mod}_R \to \boldsymbol{Mod}_S$.

Demonstração. Pelo Teorema 2.6.11, o funtor produto tensorial mapeia módulos em módulos. Além disso, pela Proposição 2.6.8 e pelo Teorema 2.6.11, segue que o funtor produto tensorial mapeia homomorfismos de módulos em homomorfismos de módulos. *QED.*

Teorema 2.6.13. *Sejam $A \in \boldsymbol{Mod}_R$, $B \in {}_R\boldsymbol{Mod}$, $(X_j)_{j\in J}$ uma família de objetos de ${}_R\boldsymbol{Mod}$ e $(Y_j)_{j\in J}$ uma família de objetos de $\boldsymbol{Mod}_R$. Então, existem homomorfismos de grupos abelianos dados por:*

$$\theta : A \otimes_R \left(\coprod_{j\in J} X_j\right) \to \coprod_{j\in J}(A \otimes_R X_j) \;\Big|\; a \otimes (x_j)_{j\in J} \mapsto (a \otimes x_j)_{j\in J},$$

$$\eta : \left(\coprod_{j\in J} Y_j\right) \otimes_R B \to \coprod_{j\in J}(Y_j \otimes_R B) \;\Big|\; (y_j)_{j\in J} \otimes b \mapsto (y_j \otimes b)_{j\in J}.$$

Além disso, esses mapas são isomorfismos de grupos abelianos.

Demonstração. Como o mapa

$$\varphi : A \times \left(\coprod_{j\in J} X_j\right) \to \coprod_{j\in J}(A \otimes_R X_j) \;\Big|\; (a, (x_j)_{j\in J}) \mapsto (a \otimes x_j)_{j\in J}$$

é R-biaditivo, então, pela propriedade universal do produto tensorial, existe um único homomorfismo de grupos θ tal que

$$\theta : A \otimes_R \left(\coprod_{j\in J} X_j \right) \to \coprod_{j\in J} (A \otimes_R X_j) \;\Big|\; a \otimes (x_j)_{j\in J} \mapsto (a \otimes x_j)_{j\in J}.$$

Seja $\lambda_k : X_k \to \coprod_{j\in J} X_j$ a k-ésima injeção para todo $k \in J$. Como o mapa

$$\psi_k : A \times X_k \to A \otimes_R \left(\coprod_{j\in J} X_j \right) \;\Big|\; (a, x) \mapsto a \otimes \lambda_k(x)$$

é R-biaditivo para todo $k \in J$, então, pela propriedade universal do produto tensorial, existe, para todo $k \in J$, um único homomorfismo de grupos $\overline{\psi}_k$ tal que

$$\overline{\psi}_k : A \otimes_R X_k \to A \otimes_R \left(\coprod_{j\in J} X_j \right) \;\Big|\; a \otimes x \mapsto a \otimes \lambda_k(x).$$

Seja $i_k : A \otimes_R X_k \to \coprod_{j\in J} (A \otimes_R X_j)$ a k-ésima injeção para todo $k \in J$. Pela propriedade universal do coproduto, existe único homomorfismo $\psi : \coprod_{j\in J} (A \otimes_R X_j) \to A \otimes_R \left(\coprod_{j\in J} X_j \right)$ tal que $\overline{\psi}_j = \psi i_j$ para todo $j \in J$. Logo:

$$\psi : \coprod_{j\in J} (A \otimes_R X_j) \to A \otimes_R \left(\coprod_{j\in J} X_j \right) \;\Big|\; (a \otimes x_j)_{j\in J} \mapsto a \otimes (x_j)_{j\in J}.$$

Defina

$$\phi : A \times \left(\coprod_{j\in J} X_j \right) \to A \otimes_R \left(\coprod_{j\in J} X_j \right) \;\Big|\; (a, (x_j)_{j\in J}) \mapsto a \otimes_R (x_j)_{j\in J}.$$

Por definição de θ e ψ, o diagrama

$$\begin{tikzcd}
\coprod_{j\in J}(A\otimes_R X_j) & & \coprod_{j\in J}(A\otimes_R X_j) \arrow[ll, dashed, shift right, "\theta\psi"'] \arrow[ll, dashed, shift left, "id"] \\
& & A\otimes_R X_k \arrow[ull, "i_k"] \arrow[u, "i_k"']
\end{tikzcd}$$

comuta para todo $k \in J$; logo, pela propriedade universal do coproduto, segue que $\theta\phi = id$. Além disso, o diagrama

$$\begin{tikzcd}
A \times \left(\coprod_{j\in J} X_j\right) \arrow[r, "\phi"] \arrow[dr, "\phi"'] & A\otimes_R \left(\coprod_{j\in J} X_j\right) \arrow[d, dashed, shift right, "id"'] \arrow[d, dashed, shift left, "\psi\theta"] \\
& A\otimes_R \left(\coprod_{j\in J} X_j\right)
\end{tikzcd}$$

comuta; logo, pela propriedade universal do produto tensorial, segue que $\phi\theta = id$. Portanto, θ é um isomorfismo de grupos. Analogamente, demonstra-se que η é um isomorfismo de grupos. *QED.*

Proposição 2.6.14. *Suponha que R é finitamente gerado como grupo abeliano. Sejam A um R-módulo à direita finitamente gerado e B um R-módulo à esquerda finitamente gerado. Então, $A \otimes_R B$ é um grupo abeliano finitamente gerado.*

Demonstração. Suponha que R é gerado por $\{r_1, ..., r_p\}$ como grupo abeliano, que A é gerado por $\{a_1, ..., a_n\}$ como R-módulo e que B é gerado por $\{b_1, ..., b_m\}$ como R-módulo. Seja $G := \{a_i \otimes (r_k b_j) : k \in \{1, ..., p\}, i \in \{1, ..., n\}, j \in \{1, ..., m\}\}$. Como $\{a \otimes b : a \in A, b \in B\}$ gera $A \otimes_R B$ como grupo abeliano, então G gera $A \otimes_R B$ como grupo abeliano, logo $A \otimes_R B$ é um grupo abeliano finitamente gerado. *QED.*

2.7 Transformações naturais e funtores adjuntos

Nesta seção, serão introduzidos os conceitos de transformação natural e par adjunto de funtores, e será demonstrado que os funtores produto tensorial e Hom formam um par adjunto.

Por toda a seção, todos os funtores considerados serão covariantes (por dualidade, todas as definições e resultados apresentados podem ser estendidos para funtores contravariantes).

Definição 2.7.1. *Sejam $\mathcal{C}, \mathcal{D}$ categorias e $F, G : \mathcal{C} \to \mathcal{D}$ funtores covariantes. Uma* ***transformação natural*** *$\alpha : F \to G$ é uma família $(\alpha_X)_{X \in \mathcal{O}b(\mathcal{C})}$ (em que, para todo $X \in \mathcal{O}b(\mathcal{C})$, $\alpha_X \in Hom_{\mathcal{D}}(FX, GX)$) tal que:*

$$\alpha_Y(Ff) = (Gf)\alpha_X \ \forall \ X, Y \in \mathcal{O}b(\mathcal{C}) \ \forall \ f \in Hom_{\mathcal{C}}(X, Y).$$

Equivalentemente, o seguinte diagrama comuta:

$$\begin{tikzcd} FX \arrow[r, "Ff"] \arrow[d, "\alpha_X"'] & FY \arrow[d, "\alpha_Y"] \\ GX \arrow[r, "Gf"'] & GY \end{tikzcd}$$

Uma transformação natural $\alpha = (\alpha_X)_{X \in \mathcal{O}b(\mathcal{C})}$ é dita um ***isomorfismo natural*** *se α_X é um isomorfismo em $\mathcal{D}$ para todo objeto X de $\mathcal{C}$; nesse caso, F e G são ditos* ***naturalmente isomorfos*** *e denota-se $F \simeq G$.*

Definição 2.7.2. *Sejam $\mathcal{C}, \mathcal{D}$ categorias e $F : \mathcal{C} \to \mathcal{D}$ e $G : \mathcal{D} \to \mathcal{C}$ funtores covariantes. Uma* ***adjunção*** *entre F e G é uma família $(\tau_{X,Y})_{X \in \mathcal{O}b(\mathcal{C}), Y \in \mathcal{O}b(\mathcal{D})}$ (em que, para todo $X \in \mathcal{O}b(\mathcal{C})$ e para todo $Y \in \mathcal{O}b(\mathcal{D})$, $\tau_{X,Y} : Hom_{\mathcal{D}}(FX, Y) \to Hom_{\mathcal{C}}(X, GY)$ é bijeção) tal que:*

1. *$\tau_{X,Y}(Ff)^* = f^*\tau_{X',Y} \ \forall \ X, X' \in \mathcal{O}b(\mathcal{C}) \ \forall \ Y \in \mathcal{O}b(\mathcal{D}) \ \forall \ f \in Hom_{\mathcal{C}}(X, X')$;*

2. $\tau_{X,Y'} g_* = (Gg)_* \tau_{X,Y}$ $\forall$ $X \in \mathcal{O}b(\mathcal{C})$ $\forall$ $Y, Y' \in \mathcal{O}b(\mathcal{D})$ $\forall$ $g \in Hom_{\mathcal{C}}(Y, Y')$.

Equivalentemente, os seguintes diagramas comutam:

$$\begin{tikzcd} Hom_{\mathcal{D}}(FX,Y) \arrow[d, "\tau_{X,Y}"'] & Hom_{\mathcal{D}}(FX',Y) \arrow[l, "(Ff)^*"'] \arrow[d, "\tau_{X',Y}"] \\ Hom_{\mathcal{C}}(X,GY) & Hom_{\mathcal{C}}(X',GY) \arrow[l, "f^*"] \end{tikzcd}$$

$$\begin{tikzcd} Hom_{\mathcal{D}}(FX,Y) \arrow[r, "g_*"] \arrow[d, "\tau_{X,Y}"'] & Hom_{\mathcal{D}}(FX,Y') \arrow[d, "\tau_{X,Y'}"] \\ Hom_{\mathcal{C}}(X,GY) \arrow[r, "(Gg)_*"'] & Hom_{\mathcal{C}}(X,GY') \end{tikzcd}$$

Se existe uma adjunção entre F e G, então (F, G) é dito um ***par adjunto de funtores****, F é dito um* ***funtor adjunto à esquerda de*** *G e G é dito um* ***funtor adjunto à direita de*** *F.*

Teorema 2.7.3. *Sejam R e S anéis. Dados ${}_RA$, ${}_SB_R$, ${}_SC$, A'_R, ${}_RB'_S$, C'_S, existem isomorfismos de grupos*

$$\tau : Hom_{{}_S\boldsymbol{Mod}}(B \otimes_R A, C) \to Hom_{{}_R\boldsymbol{Mod}}(A, Hom_{{}_S\boldsymbol{Mod}}(B, C)),$$

$$\tau' : Hom_{\boldsymbol{Mod}_S}(A' \otimes_R B', C') \to Hom_{\boldsymbol{Mod}_R}(A', Hom_{\boldsymbol{Mod}_S}(B', C')).$$

Demonstração. Pela Proposição 2.6.12, o grupo abeliano $Hom_{{}_S\mathbf{Mod}}(B \otimes_R A, C)$ está bem definido; pela Proposição 2.5.6, o grupo abeliano $Hom_{{}_R\mathbf{Mod}}(A, Hom_{{}_S\mathbf{Mod}}(B, C))$ está bem definido. Defina

$$\tau : Hom_{{}_S\mathbf{Mod}}(B \otimes_R A, C) \to Hom_{{}_R\mathbf{Mod}}(A, Hom_{{}_S\mathbf{Mod}}(B, C)) \ \mid \ f \mapsto \tau(f),$$

$$\tau(f) : A \to Hom_{{}_S\mathbf{Mod}}(B, C) \ \mid \ a \mapsto \tau(f)(a),$$

$$\tau(f)(a) : B \to C \ \mid \ b \mapsto f(b \otimes a).$$

Segue da definição que os mapas $\tau(f)(a)$ e $\tau(f)$ são homomorfismos de módulos (para todo $a \in A$ e para todo $f \in Hom_{{}_S\mathbf{Mod}}(B \otimes_R A, C)$), e que τ é um homomorfismo de grupos. Dado $g \in Hom_{{}_R\mathbf{Mod}}(A, Hom_{{}_S\mathbf{Mod}}(B, C))$, o mapa

$$g' : B \times A \to C \ \mid \ (b, a) \mapsto g(a)(b)$$

é R-biaditivo; logo, pela propriedade universal do produto tensorial, existe um único $\overline{g} \in Hom_{{}_S\mathbf{Mod}}(B \otimes_R A, C)$ tal que

$$\overline{g} : B \otimes_R A \to C \ \mid \ b \otimes a \mapsto g(a)(b).$$

Defina

$$\eta : Hom_{{}_R\mathbf{Mod}}(A, Hom_{{}_S\mathbf{Mod}}(B, C)) \to Hom_{{}_S\mathbf{Mod}}(B \otimes_R A, C) \ \mid \ g \mapsto \overline{g}.$$

Por definição, η é um homomorfismo de grupos, $\tau\eta = id$ e $\eta\tau = id$. Portanto, τ é um isomorfismo de grupos. Analogamente, demonstra-se que τ' é um isomorfismo de grupos. *QED.*

Corolário 2.7.4. *Sejam R, S anéis, B um (S, R)-bimódulo e B' um (R, S) bimódulo. Então, $(B\otimes_R, Hom_{{}_S\mathbf{Mod}}(B, -))$ e $(\otimes_R B', Hom_{\mathbf{Mod}_S}(B', -))$ são pares adjuntos de funtores.*

Demonstração. Segue do Teorema 2.7.3. *QED.*

2.8 Sequências e funtores exatos

Nesta seção, serão apresentados os conceitos de sequências exatas e funtores exatos, e serão demonstradas as propriedades dos funtores Hom e produto tensorial com respeito a essas construções.

Por toda a seção, todos os funtores considerados serão aditivos.

Definição 2.8.1. *Seja $\mathcal{C}$ uma categoria. Uma* ***sequência de morfismos*** *em $\mathcal{C}$ é uma família $(\phi_n)_{n\in\mathbb{Z}}$, em que $\phi_n \in Hom_{\mathcal{C}}(X_n, X_{n-1})$ para todo $n \in \mathbb{Z}$ e $(X_n)_{n\in\mathbb{Z}}$ é uma família de objetos de $\mathcal{C}$; nesse caso, $(\phi_n)_{n\in\mathbb{Z}}$ é representada da seguinte forma:*

$$\ldots \xrightarrow{\phi_{n+2}} X_{n+1} \xrightarrow{\phi_{n+1}} X_n \xrightarrow{\phi_n} X_{n-1} \xrightarrow{\phi_{n-1}} \ldots\ .$$

Definição 2.8.2. *Sejam R um anel e $\mathcal{C} \in \{\boldsymbol{Grp}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R\}$. Uma sequência de morfismos em $\mathcal{C}$ dada por*

$$\ldots \xrightarrow{\phi_{n+2}} X_{n+1} \xrightarrow{\phi_{n+1}} X_n \xrightarrow{\phi_n} X_{n-1} \xrightarrow{\phi_{n-1}} \ldots$$

é dita ***exata*** *se $im(\phi_{n+1}) = ker(\phi_n)$ para todo $n \in \mathbb{Z}$.*

Lema 2.8.3. *Seja*

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

uma sequência exata. Então, $C \simeq coker(f)$.

Demonstração. Pela exatidão da sequência, segue que $im(g) = C$ e $im(f) = ker(g)$, logo $B/im(f) = B/ker(g)$. Como $coker(f) := B/im(f) = B/ker(g)$, $B/ker(g) \simeq im(g)$ (pelo Teorema 2.1.16) e $im(g) = C$, então $C \simeq coker(f)$. *QED.*

Definição 2.8.4. *Sejam R, S anéis, $\mathcal{C}, \mathcal{D} \in \{\boldsymbol{Grp}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R, {}_S\boldsymbol{Mod}, \boldsymbol{Mod}_S\}$ e $F : \mathcal{C} \to \mathcal{D}$ um funtor covariante. Então, F é dito:*

1. ***exato à esquerda*** *se, para toda sequência exata em $\mathcal{C}$ da forma*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C\ ,$$

a seguinte sequência for exata em $\mathcal{D}$:

$$0 \longrightarrow FA \xrightarrow{Ff} FB \xrightarrow{Fg} FC\ ;$$

2. ***exato à direita*** *se, para toda sequência exata em $\mathcal{C}$ da forma*

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0 \ ,$$

a seguinte sequência for exata em $\mathcal{D}$:

$$FA \xrightarrow{Ff} FB \xrightarrow{Fg} FC \longrightarrow 0 \ .$$

Definição 2.8.5. *Sejam R, S anéis, $\mathcal{C}, \mathcal{D} \in \{\boldsymbol{Grp}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R, {}_S\boldsymbol{Mod}, \boldsymbol{Mod}_S\}$ e $F : \mathcal{C} \to \mathcal{D}$ um funtor contravariante. Então, F é dito:*

1. ***exato à esquerda*** *se, para toda sequência exata em $\mathcal{C}$ da forma*

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0 \ ,$$

a seguinte sequência for exata em $\mathcal{D}$:

$$0 \longrightarrow FC \xrightarrow{Fg} FB \xrightarrow{Ff} FA \ ;$$

2. ***exato à direita*** *se, para toda sequência exata em $\mathcal{C}$ da forma*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \ ,$$

a seguinte sequência for exata em $\mathcal{D}$:

$$FC \xrightarrow{Fg} FB \xrightarrow{Ff} FA \longrightarrow 0 \ .$$

Definição 2.8.6. *Sejam R, S anéis, $\mathcal{C}, \mathcal{D} \in \{\boldsymbol{Grp}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R, {}_S\boldsymbol{Mod}, \boldsymbol{Mod}_S\}$ e $F : \mathcal{C} \to \mathcal{D}$ um funtor (de qualquer variância). Então, F é dito* ***exato*** *se F é exato à esquerda e exato à direita.*

Proposição 2.8.7. *Sejam* R, S *anéis,* $\mathcal{C}, \mathcal{D} \in \{\boldsymbol{Grp}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R, {}_S\boldsymbol{Mod}, \boldsymbol{Mod}_S\}$ *e* $F : \mathcal{C} \to \mathcal{D}$ *um funtor. Então:*

1. *Se* F *é covariante e exato à esquerda, então* F *é exato se, e somente se,* F *mapeia homomorfismos sobrejetivos em homomorfismos sobrejetivos;*

2. *Se* F *é covariante e exato à direita, então* F *é exato se, e somente se,* F *mapeia homomorfismos injetivos em homomorfismos injetivos;*

3. *Se* F *é contravariante e exato à esquerda, então* F *é exato se, e somente se,* F *mapeia homomorfismos injetivos em homomorfismos sobrejetivos;*

4. *Se* F *é contravariante e exato à direita, então* F *é exato se, e somente se,* F *mapeia homomorfismos sobrejetivos em homomorfismos injetivos.*

Demonstração. Segue das definições de exatidão de funtores. *QED.*

Teorema 2.8.8. *Sejam* R *um anel,* $\mathcal{C} \in \{\boldsymbol{Ab}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R\}$ *e* $X \in \mathcal{O}b(\mathcal{C})$. *Então,* $Hom_{\mathcal{C}}(X, -)$ *e* $Hom_{\mathcal{C}}(-, X)$ *são funtores exatos à esquerda.*

Demonstração. Seja

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$$

uma sequência exata. Logo, $ker(f) = 0$ e $im(f) = ker(g)$. Assim:

1. Se $\psi \in ker(f_*)$, então $f\psi = 0$, logo $im(\psi) \subseteq ker(f) = 0$, portanto $\psi = 0$. Assim, $ker(f_*) = 0$.

2. Seja $\phi \in ker(g_*)$. Assim, $g\phi = 0$, logo $im(\phi) \subseteq ker(g) = im(f)$, portanto $im(\phi) \subseteq im(f)$. Como $ker(f) = 0$, então f é injetiva, logo existe $h \in Hom_{\mathcal{C}}(im(f), A)$ tal que $fh = 1_{im(f)}$. Como $im(\phi) \subseteq im(f)$ e $hf = 1_A$, então $f_*(h\phi) = f(h\phi) = (fh)\phi = \phi$, logo $\phi \in im(f_*)$. Assim, $ker(g_*) \subseteq im(f_*)$.

3. Seja $\beta \in im(f_*)$. Logo, existe $\alpha \in Hom_{\mathcal{C}}(X, A)$ tal que $\beta = f_*(\alpha) = f\alpha$. Portanto, $g_*(\beta) = g\beta = g(f\alpha) = (gf)\alpha$. Como $im(f) = ker(g)$, então $gf = 0$, logo $g_*(\beta) = (gf)\alpha = 0$, portanto $\beta \in ker(g_*)$. Assim, $im(f_*) \subseteq ker(g_*)$.

Portanto, a sequência

$$0 \longrightarrow Hom_{\mathcal{C}}(X,A) \xrightarrow{f_*} Hom_{\mathcal{C}}(X,B) \xrightarrow{g_*} Hom_{\mathcal{C}}(X,C)$$

é exata. Logo, $Hom_{\mathcal{C}}(X,-)$ é um funtor exato à esquerda. Analogamente, demonstra-se que $Hom_{\mathcal{C}}(-,X)$ é um funtor exato à esquerda. *QED.*

Proposição 2.8.9. *Sejam R um anel, $\mathcal{C} \in \{\boldsymbol{Ab}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R\}$ e*

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

uma sequência em $\mathcal{C}$ tal que, para todo $X \in \mathcal{O}b(\mathcal{C})$, a sequência

$$0 \longrightarrow Hom_{\mathcal{C}}(C,X) \xrightarrow{g^*} Hom_{\mathcal{C}}(B,X) \xrightarrow{f^*} Hom_{\mathcal{C}}(A,X)$$

é exata. Então, a primeira sequência é exata.

Demonstração. A demonstração é análoga à do Teorema 2.8.8. *QED.*

Um resultado análogo pode ser enunciado para o funtor $Hom(X,-)$.

Teorema 2.8.10. *Sejam R, S anéis, $\mathcal{C}, \mathcal{D} \in \{\boldsymbol{Ab}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R, {}_S\boldsymbol{Mod}, \boldsymbol{Mod}_S\}$, $F : \mathcal{C} \to \mathcal{D}$ e $G : \mathcal{D} \to \mathcal{C}$ funtores covariantes tais que (F,G) é um par adjunto. Então, F é exato à direita e G é exato à esquerda.*

Demonstração. Seja

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

uma sequência exata em $\mathcal{C}$. Seja $(\tau_{X,Y})$ uma adjunção entre F e G.

Por definição, o seguinte diagrama comuta (para todo $Y \in \mathcal{O}b(\mathcal{D})$):

$$\begin{tikzcd} 0 \arrow[r] & Hom_{\mathcal{D}}(FC,Y) \arrow[r, "(Fg)^*"] \arrow[d, "\tau_{C,Y}"] & Hom_{\mathcal{D}}(FB,Y) \arrow[r, "(Ff)^*"] \arrow[d, "\tau_{B,Y}"] & Hom_{\mathcal{D}}(FA,Y) \arrow[d, "\tau_{A,Y}"] \\ 0 \arrow[r] & Hom_{\mathcal{C}}(C,GY) \arrow[r, "g^*"] & Hom_{\mathcal{C}}(B,GY) \arrow[r, "f^*"] & Hom_{\mathcal{C}}(A,GY) \end{tikzcd}$$

Como $Hom_{\mathcal{C}}(,GY)$ é um funtor exato à esquerda (pelo Teorema 2.8.8), então a linha inferior do diagrama é uma sequência exata; como $(\tau_{X,Y})$ é uma família de isomorfismos, então, pela comutatividade do diagrama, segue que a linha superior do diagrama também é uma sequência exata (para todo $Y \in \mathcal{O}b(\mathcal{D})$). Logo, pela Proposição 2.8.9, a sequência

$$FA \xrightarrow{Ff} FB \xrightarrow{Fg} FC \longrightarrow 0$$

é exata. Portanto, F é um funtor exato à direita. Analogamente, demonstra-se que G é um funtor exato à esquerda. *QED.*

Um resultado dual pode ser enunciado para funtores contravariantes.

Teorema 2.8.11. *Sejam R um anel, A um R-módulo à direita e B um R-módulo à esquerda. Então, os funtores $A \otimes_R$ e $\otimes_R B$ são exatos à direita.*

Demonstração. Segue do Corolário 2.7.4 e do Teorema 2.8.10 (considerando A como um $(\mathbb{Z}, R)$-bimódulo e B como um $(R, \mathbb{Z})$-bimódulo). *QED.*

Em geral, o funtor Hom pode não ser exato à direita, e o funtor produto tensorial pode não ser exato à esquerda, conforme ilustram os exemplos a seguir.

Exemplo 2.8.12. *Seja $p : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ dado por $z \mapsto z + 2\mathbb{Z}$. Por definição, p é um homomorfismo sobrejetivo. Considere $p_* : Hom_{\boldsymbol{Ab}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \to Hom_{\boldsymbol{Ab}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$. Seja $\phi \in Hom_{\boldsymbol{Ab}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z})$. Então:*

$$2\phi(1_{\mathbb{Z}/2\mathbb{Z}}) = \phi(2 \cdot 1_{\mathbb{Z}/2\mathbb{Z}}) = \phi(0_{\mathbb{Z}/2\mathbb{Z}}) = 0_{\mathbb{Z}}.$$

Logo, $\phi(1_{\mathbb{Z}/2\mathbb{Z}}) = 0_{\mathbb{Z}}$*, o que implica que* $\phi = 0$*. Logo:*

$$Hom_{\boldsymbol{Ab}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = \{0\}.$$

Por outro lado, tem-se que:

$$Hom_{\boldsymbol{Ab}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = \{0, 1_{\mathbb{Z}/2\mathbb{Z}}\}.$$

Assim, p_* *não é sobrejetiva, logo o funtor* $Hom_{\boldsymbol{Ab}}(\mathbb{Z}/2\mathbb{Z}, -)$ *não é exato à direita.*

Exemplo 2.8.13. *Seja* $i : \mathbb{Z} \to \mathbb{Z}$ *dado por* $z \mapsto 2z$*. Por definição,* i *é um homomorfismo injetivo. Considere* $i \otimes 1_{\mathbb{Z}/2\mathbb{Z}} : \mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \to \mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z})$*. Então:*

$$(i \otimes 1_{\mathbb{Z}/2\mathbb{Z}})(u \otimes v) = i(u) \otimes 1_{\mathbb{Z}/2\mathbb{Z}}(v) = (2u) \otimes v = u \otimes (2v) = u \otimes 0 = 0 \ \forall \ (u, v) \in \mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z}).$$

Portanto, $im(i \otimes 1_{\mathbb{Z}/2\mathbb{Z}}) = 0$*. Por outro lado, pela Proposição 2.6.6, segue que:*

$$\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Assim, $i \otimes 1_{\mathbb{Z}/2\mathbb{Z}}$ *não é injetiva, logo o funtor* $\otimes_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})$ *não é exato à esquerda.*

3 Resoluções e módulos

Neste capítulo, serão estudados as resoluções e módulos livres, projetivos, injetivos e planos, bem como a sua relação com sequências exatas e com os funtores Hom e produto tensorial.

Ao longo de todo o capítulo (salvo menção do contrário), R denotará um anel arbitrário e todos os módulos considerados serão R-módulos à esquerda (todos os resultados e definições são análogos para R-módulos à direita). Além disso, todos os funtores considerados serão aditivos.

3.1 Resoluções e módulos livres

Nesta seção, serão definidos os conceitos de módulo livre e resolução livre, e será demonstrado que todo módulo possui uma resolução livre.

Definição 3.1.1. *Um R-módulo F é dito **livre** se existe um conjunto J tal que $F \simeq \coprod_{j\in J} R$. Se $(x_j)_{j\in J}$ é uma família de elementos de F tal que $F = \coprod_{j\in J} Rx_j$ e $Rx_j \simeq R$ para todo $j \in J$, então $(x_j)_{j\in J}$ é dita uma **base** de F.*

Definição 3.1.2. *Seja A um módulo. Uma **resolução livre** para A é uma sequência exata da forma*

$$... \longrightarrow F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{p} A \longrightarrow 0\ ,$$

em que F_n é um módulo livre para todo $n \in \mathbb{N}$.

Proposição 3.1.3. *Seja X um conjunto. Então, existe um módulo livre F com base X.*

Demonstração. Fixe $x \in X$. Seja R_x um conjunto tal que $x \in R$ e existe uma bijeção $\phi_x : R_x \to R$ tal que $\phi_x(x) = 1_R$. Então, R_x é um R-módulo munido das operações $+$ e $\cdot$ definidas de modo que $a + b := \phi_x^{-1}(\phi_x(a) + \phi_x(b))$ e $r \cdot a := \phi_x^{-1}(r\phi_x(a))$. Com respeito a essa construção, ϕ_x é um isomorfismo de módulos, logo $R_x \simeq R$ e $R_x = Rx$. Portanto, $F := \coprod_{x\in X} R_x$ é um módulo livre com base X. *QED.*

Proposição 3.1.4. *Seja $X = (x_j)_{j\in J}$ uma base de um módulo livre F. Então, para todo módulo B e para toda função $f : X \to B$, existe um único homomorfismo $\overline{f} : F \to B$ tal que $\overline{f}|_X = f$.*

Demonstração. Seja $f_j : Rx_j \to B$ dada por $rx_j \mapsto rf(x_j)$ para todo $j \in J$. Como $F = \coprod_{j\in J} Rx_j$ (pois F é módulo livre com base X) e $f_j \in Hom_{_R\mathbf{Mod}}(Rx_j, B)$ para todo $j \in J$, então, pela propriedade universal do coproduto, existe um único homomorfismo $\overline{f} : F \to B$ tal que $f_j = \overline{f} i_j$ para todo $j \in J$ (em que $i_j : Rx_j \to F$ é a j-ésima injeção para todo $j \in J$), ou seja, existe um único homomorfismo $\overline{f} : F \to B$ tal que $f = \overline{f}|_X$. *QED.*

Teorema 3.1.5. *Seja A um módulo. Então, existem um módulo livre F e um submódulo S de F tais que $A \simeq F/S$.*

Demonstração. Pelo Teorema 3.1.3, existe um módulo livre F com base A. Pelo Teorema 3.1.4, existe um homomorfismo $p : F \to A$ tal que $F(a) = a$ para todo $a \in A$. Em particular, $im(p) = A$. Definindo $S := ker(p)$, segue que $A \simeq F/S$ (pelo Teorema 2.1.16). *QED.*

Corolário 3.1.6. *Seja A um módulo. Então, existem um módulo livre F, um módulo S e homomorfismos $i : S \to F$ e $p : F \to A$ tais que a seguinte sequência é exata:*

$$0 \longrightarrow S \xrightarrow{\ i\ } F \xrightarrow{\ p\ } A \longrightarrow 0 .$$

Demonstração. Defina F, S e p como no Teorema 3.1.5. Seja $i : S \to F$ a inclusão. Assim, $ker(i) = 0$, $ker(p) = S = im(i)$ e $im(p) = A$, logo a sequência anterior é exata. *QED.*

Teorema 3.1.7. *Seja A um módulo. Então, A admite uma resolução livre.*

Demonstração. Pelo Corolário 3.1.6, existe uma sequência exata

$$0 \longrightarrow S_0 \xrightarrow{\ i_0\ } F_0 \xrightarrow{\ p\ } A \longrightarrow 0$$

em que F_0 é livre. Defina $S_{-1} := A$ e $p_0 = p$. Aplicando indutivamente o Corolário 3.1.6, segue que, para todo $n \in \mathbb{N}$, existe uma sequência exata

$$0 \longrightarrow S_n \xrightarrow{i_n} F_n \xrightarrow{p_n} S_{n-1} \longrightarrow 0 \ ,$$

em que F_n é livre. Portanto, i_n é injetiva, $ker(p_n) = im(i_n)$ e p_n é sobrejetiva para todo $n \in \mathbb{N}$. Defina $d_n = i_n p_{n+1}$ para todo $n \in \mathbb{N}$. Assim, para todo $n \in \mathbb{N}$, vale que:

$$\begin{aligned} ker(d_n) &= ker(i_n p_{n+1}) \\ &= ker(p_{n+1}) \ (pois \ i_n \ \acute{e} \ injetiva) \\ &= im(i_{n+1}) \\ &= im(i_{n+1} p_{n+2}) \ (pois \ p_{n+2} \ \acute{e} \ sobrejetiva) \\ &= im(d_{n+1}). \end{aligned}$$

Portanto, a sequência

$$... \longrightarrow F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{p} A \longrightarrow 0$$

é uma resolução livre para A. *QED.*

3.2 Resoluções e módulos projetivos

Nesta seção, serão apresentados os conceitos de módulo projetivo e resolução projetiva, e serão demonstradas algumas de suas propriedades.

Definição 3.2.1. *Seja P um módulo. Então, P é dito* ***projetivo*** *se, para quaisquer módulos B e C, para todo homomorfismo $\alpha : P \to C$ e para todo homomorfismo sobrejetivo $\beta : B \to C$, existe um homomorfismo $\gamma : P \to B$ tal que $\alpha = \beta\gamma$. Equivalentemente, o seguinte diagrama comuta:*

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

Definição 3.2.2. *Seja A um módulo. Uma* **resolução projetiva** *para A é uma sequência exata da forma*

$$\ldots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{p} A \longrightarrow 0 \ ,$$

em que P_n é um módulo projetivo para todo $n \in \mathbb{N}$.

Teorema 3.2.3. *Seja X um módulo. Então, o módulo X é projetivo se, e somente se, o funtor $Hom_{{}_R\boldsymbol{Mod}}(X, -)$ é exato.*

Demonstração.

1. Suponha que o módulo X é projetivo. Sejam B, C módulos e $g : B \to C$ um homomorfismo sobrejetivo. Como g é sobrejetiva e X é projetivo, então, para todo $\alpha \in Hom_{{}_R\mathbf{Mod}}(X, C)$, existe $\gamma \in Hom_{{}_R\mathbf{Mod}}(X, B)$ tal que $\alpha = g\gamma$, ou seja, $\alpha = g_*(\gamma)$; logo, g_* é sobrejetiva. Como $Hom_{{}_R\mathbf{Mod}}(X, -)$ é exato à esquerda (pelo Teorema 2.8.8) e mapeia homomorfismos sobrejetivos em homomorfismos sobrejetivos, então $Hom_{{}_R\mathbf{Mod}}(X, -)$ é exato (pela Proposição 2.8.7).

2. Suponha que o funtor $Hom_{{}_R\mathbf{Mod}}(X, -)$ é exato. Sejam B, C módulos, $\alpha : X \to C$ um homomorfismo e $\beta : B \to C$ um homomorfismo sobrejetivo. Como $\beta : B \to C$ é homomorfismo sobrejetivo e $Hom_{{}_R\mathbf{Mod}}(X, -)$ é exato, então o mapa

$$\beta_* : Hom_{{}_R\mathbf{Mod}}(X, B) \to Hom_{{}_R\mathbf{Mod}}(X, C)$$

é sobrejetivo, logo existe $\gamma \in Hom_{{}_R\mathbf{Mod}}(X, B)$ tal que $\beta\gamma = \alpha$. Portanto, X é projetivo.

QED.

Teorema 3.2.4. *Seja $(A_j)_{j \in J}$ uma família de módulos projetivos. Então, $\coprod_{j \in J} A_j$ é um módulo projetivo.*

Demonstração. Sejam X, Y módulos e $f : X \to Y$ um homomorfismo sobrejetivo. Como $(A_j)_{j \in J}$ é uma família de módulos projetivos, então, pelo Teorema 3.2.3, $Hom_{{}_R\mathbf{Mod}}(A_j, -)$

é exato para todo $j \in J$, logo o mapa

$$f_j := Hom_{{}_R\mathbf{Mod}}(A_j, -)(f) : Hom_{{}_R\mathbf{Mod}}(A_j, X) \to Hom_{{}_R\mathbf{Mod}}(A_j, Y)$$

é sobrejetivo para todo $j \in J$. Assim, pela Proposição 2.3.7, $\prod_{j\in J} f_j$ é sobrejetiva. Defina

$$\theta_Z : Hom_{{}_R\mathbf{Mod}}\left(\coprod_{j\in J} A_j, Z\right) \to \prod_{j\in J} Hom_{{}_R\mathbf{Mod}}(A_j, Z) \;\Big|\; \phi \mapsto (\phi i_j)_{j\in J}$$

para todo módulo Z, em que $i_k : A_k \to \coprod_{j\in J} A_j$ é a k-ésima injeção. Seja

$$f_* := Hom_{{}_R\mathbf{Mod}}(\coprod_{j\in J} A_j, -)(f).$$

Como θ é isomorfismo para todo módulo Z (pelo Teorema 2.5.8) e $f_* = \theta_Y^{-1}(\prod_{j\in J} f_j)\theta_X$, então f_* é sobrejetiva. Como $Hom_{{}_R\mathbf{Mod}}(\coprod_{j\in J} A_j, -)$ é um funtor exato à esquerda (pelo Teorema 2.8.8) e que mapeia morfismos sobrejetivos em morfismos sobrejetivos, então, pela Proposição 2.8.7, $Hom_{{}_R\mathbf{Mod}}(\coprod_{j\in J} A_j, -)$ é exato, logo $\coprod_{j\in J} A_j$ é projetivo (pelo Teorema 3.2.3). *QED.*

Teorema 3.2.5. *Seja A um módulo. Então, A é projetivo se, e somente se, A é um somando direto de um módulo livre. Em particular, todo módulo livre é projetivo, e todo somando direto de um módulo projetivo é projetivo.*

Demonstração.

1. Suponha que A é projetivo. Pelo Corolário 3.1.6, existem um módulo livre F e um homomorfismo sobrejetivo $p : F \to A$. Como A é projetivo e $p : F \to A$ é um homomorfismo sobrejetivo, existe um homomorfismo $\gamma : P \to F$ tal que $p\gamma = 1_P$; em particular, γ é injetivo. Logo, pelo Lema 2.3.10, A é um somando direto de F.

2. Suponha que A é um somando direto de um módulo livre F. Seja S um módulo tal que $F = i(A) \oplus j(S)$ munido das injeções canônicas $i : A \to F$ e $j : S \to F$; seja X uma base de F tal que $X \subseteq i(A) \cup j(S)$. Sejam B, C módulos, $\alpha : A \to C$ um

homomorfismo e $\beta : B \to C$ um homomorfismo sobrejetivo. Como $\beta : B \to C$ é sobrejetivo, existe uma função $\Gamma : V \to B$ tal que $\beta\Gamma = \alpha|_V$ (em que $V := i^{-1}(X \cap i(A))$). Defina

$$g : X \to B \;\Big|\; x \mapsto \begin{cases} \Gamma(i^{-1}(x)), & se\ x \in X \cap i(A) \\ 0, & se\ x \in X \cap j(S) \end{cases}.$$

Como F é um módulo livre com base X, então, pela Proposição 3.1.4, existe um homomorfismo $G : F \to B$ tal que $G|_X = g$. Além disso, pela propriedade universal do coproduto, existe um homomorfismo $a : F \to C$ tal que $\alpha = ai$ e $0 = aj$. Como $\beta G, a \in Hom_{{}_R\mathbf{Mod}}(F, C)$ e $(\beta G)|_X = a|_X$ (por definição), então, pela Proposição 3.1.4, $\beta G = a$. Defina $\gamma = Gi$. Assim, $\beta Gi = ai$, logo $\beta\gamma = \alpha$. Portanto, A é projetivo.

QED.

Corolário 3.2.6. *Seja A um módulo. Então, A admite resolução projetiva.*

Demonstração. Segue do Teorema 3.1.7 e do Teorema 3.2.5. *QED.*

3.3 Resoluções e módulos injetivos

Nesta seção, serão apresentados os conceitos de módulo injetivo e resolução injetiva, e serão demonstradas algumas de suas propriedades.

Definição 3.3.1. *Seja E um módulo. Então, E é dito **injetivo** se, para quaisquer módulos B e C, para todo homomorfismo $\alpha : B \to E$ e para todo homomorfismo injetivo $\beta : B \to C$, existe um homomorfismo $\gamma : C \to E$ tal que $\alpha = \gamma\beta$. Equivalentemente, o seguinte diagrama comuta:*

$$\begin{tikzcd} E & \\ B \arrow[u, "\alpha"] \arrow[r, hook, "\beta"] & C \arrow[ul, dashed, "\gamma"'] \end{tikzcd}$$

Os conceitos de módulo projetivo e injetivo são duais.

Definição 3.3.2. *Seja A um módulo. Uma **resolução injetiva** para A é uma sequência exata da forma*

$$0 \longrightarrow A \xrightarrow{i} E_0 \xrightarrow{d_0} E_{-1} \xrightarrow{d_{-1}} E_{-2} \longrightarrow \dots ,$$

em que E_n é um módulo injetivo para todo $n \in \mathbb{N}$.

Teorema 3.3.3. *Seja X um módulo. Então, o módulo X é injetivo se, e somente se, o funtor $Hom_{_R\boldsymbol{Mod}}(-, X)$ é exato.*

Demonstração. A demonstração é dual à do Teorema 3.2.3. *QED.*

Teorema 3.3.4. *Seja $(A_j)_{j \in J}$ uma família de módulos injetivos. Então, $\prod_{j \in J} A_j$ é um módulo injetivo.*

Demonstração. A demonstração é dual à do Teorema 3.2.4 (usando o Teorema 3.3.3 em vez do Teorema 3.2.3 e usando o Teorema 2.5.7 em vez do Teorema 2.5.8). *QED.*

Teorema 3.3.5. *Seja X um módulo. Então, X é injetivo se, e somente se, para todo ideal à esquerda I de R e para todo homomorfismo $g : I \to X$, existe um homomorfismo $G : R \to X$ tal que $G|_I = g$.*

Demonstração.

1. Suponha que X é injetivo. Então, por definição, para todo ideal à esquerda I de R e para todo homomorfismo $g : I \to X$, existe um homomorfismo $G : R \to X$ tal que $G|_I = g$ (considerando R como um R-módulo à esquerda e I como um submódulo de R).

2. Suponha que para todo ideal à esquerda I de R e para todo homomorfismo $g : I \to X$, existe um homomorfismo $G : R \to X$ tal que $G|_I = g$. Sejam A, B módulos, $f : A \to X$ um homomorfismo e $i : A \to B$ um homomorfismo injetivo. Defina Σ como o conjunto dos pares (B', f'), em que B' é um submódulo de B tal que $i(A) \subseteq B'$ e $f' : B' \to X$ é um homomorfismo tal que $f'i = f$. Seja $\leq$ uma

relação binária em Σ dada por $(B', f') \leq (B'', f'')$ se $B' \subset B''$ e $f''|_{B'} = f'$. Então, $\Sigma \neq \emptyset$ (pois $(i(A), fi^{-1}) \in \Sigma$) e $(\Sigma, \leq)$ é um conjunto parcialmente ordenado. Seja Γ uma cadeia em $(\Sigma, \leq)$. Defina S como o submódulo de B gerado por $\cup_{(B',f')\in\Gamma} B'$ e defina $\phi : S \to X$ tal que $\phi(x) = f'(x)$, em que $(B', f') \in \Gamma$ é tal que $x \in B'$; por definição de Σ, ϕ está bem definida e é um homomorfismo, e (S, ϕ) é uma cota superior para Γ em Σ. Como $\Sigma \neq \emptyset$ e $(\Sigma, \leq)$ é um conjunto parcialmente ordenado em que toda cadeia possui cota superior, então, pelo Lema de Zorn, Σ admite um elemento maximal (M, γ). Sejam $b \in B$ e $I = \{r \in R : rb \in M\}$; por definição, I é um ideal à esquerda de R. Defina $g : I \to X$ dada por $r \mapsto \gamma(rb)$. Como $g : I \to X$ é um homomorfismo, então, por hipótese, existe um homomorfismo $G : R \to X$ tal que $G|_I = g$. Defina $M' = M + Rb$ e $\gamma' : M' \to X$ dada por:

$$m + rb \mapsto \gamma(m) + G(r).$$

Se $m_1, m_2 \in M$ e $r_1, r_2 \in R$ são tais que $m_1 + r_1 b = m_2 + r_2 b$, então $(r_2 - r_1)b = m_1 - m_2 \in M$, logo $G(r_2 - r_1) = \gamma((r_2 - r_1)b) = \gamma(m_1 - m_2)$, portanto $G(r_2) - G(r_1) = \gamma(m_1) - \gamma(m_2)$, ou seja, $\gamma(m_1) + G(r_1) = \gamma(m_2) + G(r_2)$. Assim, γ' está bem definida; além disso, por definição, γ' é um homomorfismo e $\gamma'|_M = \gamma$. Logo, $(M', \gamma') \in \Sigma$ e $(M, \gamma) \leq (M', \gamma')$; como (M, γ) é elemento maximal de Σ, então $M = M' = M + Rb$, portanto $b \in M$. Como $M \subseteq B$ e $b \in M$ para todo $b \in B$, então $M = B$. Assim, $\gamma : B \to X$ é um homomorfismo tal que $\gamma i = f$. Portanto, X é injetivo.

QED.

Definição 3.3.6. *Defina $R^* := \{r \in R : sr \neq 0 \; \forall \; s \in R\backslash\{0\}\}$. Um módulo A é dito* ***divisível*** *se, para todo $(r, a) \in R^* \times A$, existe $a' \in A$ tal que $ra' = a$.*

Proposição 3.3.7. *Sejam A um módulo divisível e B um submódulo de A. Então, A/B é um módulo divisível.*

Demonstração. Sejam $a + B \in A/B$ e $r \in R^*$. Como A é divisível, existe $a' \in A$ tal que $a = ra'$, logo $a + B = r(a' + B)$. Assim, A/B é divisível. *QED.*

Proposição 3.3.8. *Seja $(A_j)_{j\in J}$ uma família de módulos divisíveis. Então, $A := \coprod_{j\in J} A_j$ é um módulo divisível.*

Demonstração. Fixe $r \in R^*$. Como $(A_j)_{j\in J}$ é uma família de módulos divisíveis, então os mapas $r1_{A_j}$ são homomorfismos sobrejetivos para todo $j \in J$. Pela Proposição 2.3.8, segue que $\coprod_{j\in J}(r1_{A_j}) = r\left(\coprod_{j\in J} 1_{A_j}\right) = r1_A$ e $\coprod_{j\in J}(r1_{A_j})$ é sobrejetivo, logo $r1_A$ é sobrejetivo. Assim, dado $a \in A$, existe $a' \in A$ tal que $ra' = a$; logo, A é divisível. *QED.*

Teorema 3.3.9. *Seja A um módulo injetivo. Então, A é divisível.*

Demonstração. Sejam $a \in A$ e $r_0 \in R^*$. Defina $g : Rr_0 \to A$ dada por $rr_0 \mapsto ra$; como $r_0 \in R^*$, g está bem definida e é um homomorfismo. Como A é injetivo, então, pelo Teorema 3.3.5, existe um homomorfismo $G : R \to A$ tal que $G|_{Rr} = g$. Em particular, $a = g(r_0) = G(r_0) = r_0G(1_R)$. Portanto, A é divisível. *QED.*

Teorema 3.3.10. *Sejam D um domínio principal e A um D-módulo à esquerda divisível. Então, A é injetivo.*

Demonstração. Sejam I um ideal à esquerda de D e $g : I \to A$ um homomorfismo. Como D é domínio principal, então $D^* = D\backslash\{0\}$ e existe $d \in D$ tal que $I = Rd$. Se $d = 0$, então $0 : R \to A$ é uma extensão de g; caso contrário, $d \in D^*$. Assim, suponha que $d \in D^*$. Como D é divisível, existe $a \in A$ tal que $da = g(d)$. Defina $G : R \to A \mid r \mapsto ra$. Por definição, G é um homomorfismo e $G|_I = g$. Logo, pelo Teorema 3.3.5, A é injetivo. *QED.*

Lema 3.3.11. *Seja G um $\mathbb{Z}$-módulo à esquerda. Então, existem um $\mathbb{Z}$-módulo à esquerda injetivo E e um $\mathbb{Z}$-homomorfismo injetivo $i : G \to E$.*

Demonstração. Pelo Teorema 3.1.5, existem um módulo livre $F = \coprod_{j\in J} \mathbb{Z}$, um submódulo S de F e um isomorfismo $\phi : G \to F/S$. Seja $\lambda : \mathbb{Z} \to \mathbb{Q}$ a inclusão canônica; pela Proposição 2.3.8, existe um homomorfismo injetivo $\coprod_{j\in J} \lambda : \coprod_{j\in J} \mathbb{Z} \to \coprod_{j\in J} \mathbb{Q}$. Defina $E = \left(\coprod_{j\in J} \mathbb{Q}\right)/S$; como $\mathbb{Q}$ é um $\mathbb{Z}$-módulo divisível, então E é um $\mathbb{Z}$-módulo divisível (pelas Proposições 3.3.7 e 3.3.8). Como E é um $\mathbb{Z}$-módulo divisível e $\mathbb{Z}$ é um domínio principal, então, pelo Teorema 3.3.10, E é um $\mathbb{Z}$-módulo injetivo. Defina $\epsilon : F/S \to E$

dada por $f + S \mapsto (\coprod_{j \in J} \lambda)(f) + S$; ϵ está bem definida e é um homomorfismo injetivo. Defina $i = \epsilon\phi$; logo, $i : G \to E$ é um $\mathbb{Z}$-homomorfismo injetivo. *QED.*

Proposição 3.3.12. *Seja G um $\mathbb{Z}$-módulo divisível. Então, $X := Hom_{\mathbb{Z}\mathbf{Mod}}(R, G)$ é um R-módulo à esquerda injetivo.*

Demonstração. Considerando R como um $(\mathbb{Z}, R)$-bimódulo, segue que X é um R-módulo à esquerda (pelo Corolário 2.5.6). Sejam A, B módulos e $f : A \to B$ um homomorfismo injetivo. Considerando R como um $(R, \mathbb{Z})$-bimódulo, existe uma adjunção $(\tau_{X,Y})$ entre os funtores $R \otimes_R$ e $Hom_{\mathbb{Z}\mathbf{Mod}}(R, -)$ (pelo Corolário 2.7.4). Portanto, o seguinte diagrama comuta:

$$\begin{tikzcd}
Hom_{R\mathbf{Mod}}(B, X) \arrow[r, "f^*"] & Hom_{R\mathbf{Mod}}(A, X) \\
Hom_{\mathbb{Z}\mathbf{Mod}}(R \otimes_R B, G) \arrow[u, "\tau_{B,G}"] \arrow[r, "(1_R \otimes f)^*"'] & Hom_{\mathbb{Z}\mathbf{Mod}}(R \otimes_R A, G) \arrow[u, "\tau_{A,G}"']
\end{tikzcd}$$

Como G é um $\mathbb{Z}$-módulo divisível e $\mathbb{Z}$ é um domínio principal, então G é um $\mathbb{Z}$-módulo injetivo (pelo Teorema 3.3.10), logo o funtor $Hom_{\mathbb{Z}\mathbf{Mod}}(-, G)$ é exato (pelo Teorema 3.3.3). Como $Hom_{\mathbb{Z}\mathbf{Mod}}(-, G)$ é exato, $f : A \to B$ é um homomorfismo injetivo e $R \otimes_R A \simeq A$ e $R \otimes_R B \simeq B$ (pela Proposição 2.6.6), então $(1_R \otimes f)^*$ é sobrejetiva. Portanto, como $\tau_{A,G}, \tau_{B,G}$ são isomorfismos e o diagrama anterior comuta, f^* é sobrejetiva. Como $Hom_{R\mathbf{Mod}}(-, X)$ é um funtor exato à esquerda (pelo Teorema 2.8.8) e mapeia homomorfismos injetivos em homomorfismos sobrejetivos, então $Hom_{R\mathbf{Mod}}(-, X)$ é exato (pela Proposição 2.8.7), logo X é um R-módulo injetivo (pelo Teorema 3.3.3). *QED.*

Teorema 3.3.13. *Seja A um R-módulo. Então, existem um R-módulo injetivo E e um homomorfismo injetivo $i : A \to E$.*

Demonstração. Como A é um $\mathbb{Z}$-módulo à esquerda, existem um $\mathbb{Z}$-módulo à esquerda divisível G e um $\mathbb{Z}$-homomorfismo injetivo $j : A \to G$ (pelo Lema 3.3.11). Dado $a \in A$, defina $f_a : R \to A \mid r \mapsto ra$. Defina $i : A \to Hom_{\mathbb{Z}\mathbf{Mod}}(R, G) \mid a \mapsto jf_a$; por definição,

i é um R-homomorfismo injetivo. Como G é um $\mathbb{Z}$-módulo à esquerda divisível, então $Hom_{_\mathbb{Z}\mathbf{Mod}}(R,G)$ é um R-módulo injetivo (pela Proposição 3.3.12). *QED.*

Corolário 3.3.14. *Seja A um módulo. Então, A admite resolução injetiva.*

Demonstração. A demonstração é análoga à do Teorema 3.1.7: basta aplicar indutivamente o Teorema 3.3.13. *QED.*

3.4 Resoluções e módulos planos

Nesta seção, serão definidos os conceitos de módulo plano e resolução plana, e será demonstrado que todo módulo projetivo é plano.

Definição 3.4.1. *Um R-módulo à esquerda B é dito **plano** se o funtor $\otimes_R B$ é exato; um R-módulo à direita A é dito **plano** se o funtor $A\otimes_R$ é exato.*

Definição 3.4.2. *Seja A um módulo. Uma **resolução plana** para A é uma sequência exata da forma*

$$... \longrightarrow F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{p} A \longrightarrow 0 \ ,$$

em que F_n é um módulo plano para todo $n \in \mathbb{N}$.

Lema 3.4.3. *Um anel R (considerado como R-módulo à esquerda ou à direita) é um R-módulo plano.*

Demonstração. Pela Proposição 2.6.6, $R \otimes_R B \simeq B$ para todo R-módulo à esquerda B e $A \otimes_R R \simeq A$ para todo R-módulo à direita A; portanto, os funtores $R\otimes_R$ e $\otimes_R R$ são exatos, logo o anel R, considerado como R-módulo à esquerda ou à direita, é um R-módulo plano. *QED.*

Teorema 3.4.4. *Seja $(X_j)_{j\in J}$ uma família de R-módulos à esquerda. Então, $X := \coprod_{j\in J} X_j$ é módulo plano se, e somente se, X_j é módulo plano para todo $j \in J$.*

Demonstração. Pelo Teorema 2.8.11, $\otimes_R X$ é exato à direita. Seja

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$$

uma sequência exata de R-módulos à direita. Pelo Teorema 2.6.13, existem isomorfismos $\theta_A, \theta_B, \theta_C$ tais que o seguinte diagrama comuta:

$$\begin{tikzcd}
0 \arrow[r] & A \otimes_R \left(\coprod_{j\in J} X_j\right) \arrow[r, "f\otimes 1_X"] \arrow[d, "\theta_A"] & B \otimes_R \left(\coprod_{j\in J} X_j\right) \arrow[r, "g\otimes 1_X"] \arrow[d, "\theta_B"] & C \otimes_R \left(\coprod_{j\in J} X_j\right) \arrow[d, "\theta_C"] \\
0 \arrow[r] & \coprod_{j\in J}(A \otimes_R X_j) \arrow[r, "\coprod_{j\in J}(f\otimes 1_{X_j})"'] & \coprod_{j\in J}(B \otimes_R X_j) \arrow[r, "\coprod_{j\in J}(g\otimes 1_{X_j})"'] & \coprod_{j\in J}(C \otimes_R X_j)
\end{tikzcd}$$

Logo, a linha superior do diagrama é exata (ou seja, $\otimes_R X$ é exato) se, e somente se, a linha inferior do diagrama é exata. Como $\otimes_R X_j$ é exato à direita para todo $j \in J$ (pelo Teorema 2.8.11) e $\coprod_{j\in J}(f \otimes 1_{X_j})$ é injetiva se, e somente se, $f \otimes 1_{X_j}$ é injetiva para todo $j \in J$ (pela Proposição 2.3.8), então a linha inferior do diagrama é exata se, e somente se, $\otimes_R X_j$ é exato para todo $j \in J$ (pela Proposição 2.8.7). Portanto, $\otimes_R X$ é exato se, e somente se, $\otimes_R X_j$ é exato para todo $j \in J$, ou seja, X é plano se, e somente se, X_j é plano para todo $j \in J$. *QED.*

Proposição 3.4.5. *Seja P um módulo projetivo. Então, P é plano.*

Demonstração. Como P é projetivo, então P é um somando direto de um módulo livre F (pelo Teorema 3.2.5). Como F é livre, então existe um conjunto J tal que $F \simeq \coprod_{j\in J} R$; logo, pelo Lema 3.4.3 e pelo Teorema 3.4.4, F é plano. Como F é plano e P é um somando direto de F, então, pelo Teorema 3.4.4, P é plano. *QED.*

Corolário 3.4.6. *Seja A um módulo. Então, A admite uma resolução plana.*

Demonstração. Segue do Corolário 3.2.6 e da Proposição 3.4.5. *QED.*

4 Álgebra Homológica

Neste capítulo, serão apresentadas as definições e ferramentas básicas da Álgebra Homológica. Em particular, serão estudados os complexos e morfismos de cadeias, os funtores de homologia, a relação de homotopia e os funtores *Ext* e *Tor*.

Ao longo de todo o capítulo (salvo menção do contrário), R denotará um anel arbitrário e todos os módulos considerados serão R-módulos à esquerda (todos os resultados e definições são análogos para R-módulos à direita). Além disso, todos os funtores considerados serão aditivos.

4.1 Complexos de cadeias e funtores de homologia

Nesta seção, serão apresentados os conceitos de complexos de cadeias, morfismos de cadeias e funtores de homologia, e serão demonstradas algumas de suas propriedades.

Definição 4.1.1. *Seja $\mathcal{C} \in \{\boldsymbol{Ab}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R\}$. Uma sequência de morfismos em $\mathcal{C}$ dada por*

$$(X, d) : \ldots \xrightarrow{d_{n+2}} X_{n+1} \xrightarrow{d_{n+1}} X_n \xrightarrow{d_n} X_{n-1} \xrightarrow{d_{n-1}} \ldots$$

*é dita um **complexo (de cadeias)** se $im(d_{n+1}) \subseteq ker(d_n)$ para todo $n \in \mathbb{Z}$ (ou, equivalentemente, se $d_n d_{n+1} = 0$ para todo $n \in \mathbb{Z}$). Os morfismos d_n são denominados **diferenciais**. A sequência (X, d) é também denotada por X ou d.*

Em particular, toda sequência exata em $\mathcal{C}$ é um complexo de cadeias.

Definição 4.1.2. *Dados (X, f) e (Y, g) complexos em $\mathcal{C} \in \{\boldsymbol{Ab}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R\}$, um **morfismo de cadeias** $\phi : f \to g$ é uma família $\phi = (\phi_n)_{n \in \mathbb{Z}}$, em que $\phi_n \in Hom_{\mathcal{C}}(X_n, Y_n)$ para todo $n \in \mathbb{Z}$, tal que $\phi_{n-1} f_n = g_n \phi_n$ para todo $n \in \mathbb{Z}$. Equivalentemente, o seguinte* *diagrama comuta:*

$$\begin{array}{ccccccccc}
\ldots & \xrightarrow{f_{n+2}} & X_{n+1} & \xrightarrow{f_{n+1}} & X_n & \xrightarrow{f_n} & X_{n-1} & \xrightarrow{f_{n-1}} & \ldots \\
 & & \downarrow{\scriptstyle \phi_{n+1}} & & \downarrow{\scriptstyle \phi_n} & & \downarrow{\scriptstyle \phi_{n-1}} & & \\
\ldots & \xrightarrow{g_{n+2}} & Y_{n+1} & \xrightarrow{g_{n+1}} & Y_n & \xrightarrow{g_n} & Y_{n-1} & \xrightarrow{g_{n-1}} & \ldots
\end{array}$$

Proposição 4.1.3. *Dada $\mathcal{C} \in \{\boldsymbol{Ab}, {}_R\boldsymbol{Mod}, \boldsymbol{Mod}_R\}$, existe uma categoria pré-aditiva $\mathcal{C} - \boldsymbol{Comp}$ cujos objetos são os complexos em $\mathcal{C}$ e cujos morfismos são os morfismos de cadeias (dados morfismos $(\phi_n)_{n\in\mathbb{Z}}, (\psi_n)_{n\in\mathbb{Z}}$, definem-se $(\phi_n)_{n\in\mathbb{Z}}(\psi_n)_{n\in\mathbb{Z}} := (\phi_n\psi_n)_{n\in\mathbb{Z}}$ e $(\phi_n)_{n\in\mathbb{Z}} + (\psi_n)_{n\in\mathbb{Z}} := (\phi_n + \psi_n)_{n\in\mathbb{Z}}$).*

Demonstração. Segue das definições de complexos e morfismos de cadeias. *QED.*

Ao longo do texto, a categoria ${}_R$**Mod** – **Comp** será denotada por **Comp**.

Lema 4.1.4. *Um morfismo de cadeias $(\phi_n)_{n\in\mathbb{Z}}$ é um isomorfismo em **Comp** se, e somente se, ϕ_n é um isomorfismo de módulos para todo $n \in \mathbb{Z}$.*

Demonstração. Segue da definição de **Comp**. *QED.*

Definição 4.1.5. *Dado um complexo d em ${}_R\boldsymbol{Mod}$, definem-se:*

1. *o n-**ésimo ciclo** de d como $Z_n(d) := ker(d_n)$;*
2. *a n-**ésima fronteira** de d como $B_n(d) := im(d_{n+1})$;*
3. *o n-**ésimo módulo de homologia** de d como $H_n(d) := Z_n(d)/B_n(d)$.*

Proposição 4.1.6. *Dados f, g complexos em ${}_R\boldsymbol{Mod}$ e um morfismo de cadeias $\phi : f \to g$, o mapa*

$$H_n(\phi) : H_n(f) \to H_n(g) \ \mid \ z_n + B_n(f) \mapsto \phi_n(z_n) + B_n(g)$$

está bem definido e é um homomorfismo de módulos para todo $n \in \mathbb{Z}$.

Demonstração. Segue das definições de módulo de homologia e morfismo de cadeias. *QED.*

Proposição 4.1.7. H_n : ***Comp*** $\to {}_R$***Mod*** *é um funtor covariante aditivo (denominado* n***-ésimo funtor de homologia****) para todo* $n \in \mathbb{Z}$*.*

Demonstração. Segue da definição de H_n. *QED.*

Definição 4.1.8. *Sejam* (X, f) *e* (Y, g) *complexos em* ${}_R$***Mod*** *e* $\phi : f \to g$ *um morfismo de cadeias. Definem-se:*

$$ker(\phi) : ... \xrightarrow{d_{n+2}} ker(\phi_{n+1}) \xrightarrow{d_{n+1}} ker(\phi_n) \xrightarrow{d_n} ker(\phi_{n-1}) \xrightarrow{d_{n-1}} ... \ ,$$
$$im(\phi) : ... \xrightarrow{d'_{n+2}} im(\phi_{n+1}) \xrightarrow{d'_{n+1}} im(\phi_n) \xrightarrow{d'_n} im(\phi_{n-1}) \xrightarrow{d_{n-1}} ... \ .$$

em que $d_n := f_n|_{ker(\phi_n)}$ *e* $d'_n := g_n|_{im(\phi_n)}$ *para todo* $n \in \mathbb{Z}$*.*

Definição 4.1.9. *Sejam* X, Y, Z *complexos em* ${}_R$***Mod*** *e* $\phi : X \to Y$*,* $\psi : Y \to Z$ *morfismos de cadeias. Então, a sequência de morfismos*

$$X \xrightarrow{\phi} Y \xrightarrow{\psi} Z$$

é dita ***exata*** *se* $im(\phi) = ker(\psi)$*.*

Proposição 4.1.10. *Sejam* $(X, f), (Y, g), (Z, h)$ *complexos em* ${}_R$***Mod*** *e* $\phi : X \to Y$*,* $\psi : Y \to Z$ *complexos de cadeias. Então, a sequência*

$$X \xrightarrow{\phi} Y \xrightarrow{\psi} Z$$

é exata se, e somente se, as seguintes sequências são exatas para todo $n \in \mathbb{Z}$*:*

$$X_n \xrightarrow{\phi_n} Y_n \xrightarrow{\psi_n} Z_n \ .$$

Demonstração. Segue da definição de sequência exata de morfismos de cadeias. *QED.*

Teorema 4.1.11. *Sejam* $(X, f), (Y, g), (Z, h)$ *complexos em* ${}_R$***Mod*** *e*

$$0 \longrightarrow X \xrightarrow{i} Y \xrightarrow{p} Z \longrightarrow 0$$

*uma sequência exata de morfismos. Então, para todo $n \in \mathbb{Z}$, existe um homomorfismo (denominado n-**ésimo homomorfismo de conexão**) dado por:*

$$\partial_n : H_n(Z) \to H_{n-1}(X) \ \mid \ z + B_n(Z) \mapsto i_{n-1}^{-1} g_n p_n^{-1}(z) + B_{n-1}(X).$$

Além disso, a seguinte sequência é exata:

$$\ldots \xrightarrow{\partial_{n+1}} H_n(X) \xrightarrow{H_n(i)} H_n(Y) \xrightarrow{H_n(p)} H_n(Z) \xrightarrow{\partial_n} H_{n-1}(X) \xrightarrow{H_{n-1}(i)} \ldots .$$

Demonstração. Segue da Proposição 4.1.10. Os detalhes serão omitidos. *QED.*

Lema 4.1.12. *Suponha que o seguinte diagrama comuta*

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & A_1 \arrow[r, "a_1"] \arrow[d, "f_1"] & A_2 \arrow[r, "a_2"] \arrow[d, "f_2"] & A_3 \arrow[r] \arrow[d, "f_3"] & 0 \\
0 \arrow[r] & B_1 \arrow[r, "b_1"] \arrow[d, "g_1"] & B_2 \arrow[r, "b_2"] \arrow[d, "g_2"] & B_3 \arrow[r] \arrow[d, "g_3"] & 0 \\
0 \arrow[r] & C_1 \arrow[r, "c_1"] \arrow[d] & C_2 \arrow[r, "c_2"] \arrow[d] & C_3 \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

em que as colunas e as duas linhas inferiores são sequências exatas de módulos. Então, a linha superior A do diagrama é uma sequência exata de módulos.

Demonstração. Por hipótese, f_3 é injetiva e $b_2 b_1 = 0$. Pela comutatividade do diagrama, segue que $f_3 a_2 a_1 = b_2 b_1 f_1 = 0$; como f_3 é injetiva, então $a_2 a_1 = 0$. Portanto, a linha superior A do diagrama é um complexo. Como

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

é uma sequência exata de complexos, então, pelo Teorema 4.1.11, segue que a seguinte sequência é exata para todo $n \in \mathbb{Z}$:

$$H_n(C) \xrightarrow{\partial_n} H_{n-1}(A) \xrightarrow{H_{n-1}(f)} H_{n-1}(B) \ .$$

Como $H_n(B) = 0$ e $H_n(C) = 0$ para todo $n \in \mathbb{Z}$ (pois B e C são sequências exatas), então $H_n(A) = 0$ para todo $n \in \mathbb{Z}$, logo A é uma sequência exata. *QED.*

4.2 Homotopia

Nesta seção, será apresentado o conceito de homotopia entre morfismos de cadeias e serão demonstradas algumas de suas propriedades.

Definição 4.2.1. *Sejam*

$$f : \ldots \xrightarrow{f_{n+2}} X_{n+1} \xrightarrow{f_{n+1}} X_n \xrightarrow{f_n} X_{n-1} \xrightarrow{f_{n-1}} \ldots \ ,$$

$$g : \ldots \xrightarrow{g_{n+2}} Y_{n+1} \xrightarrow{g_{n+1}} Y_n \xrightarrow{g_n} Y_{n-1} \xrightarrow{g_{n-1}} \ldots$$

*complexos em ${}_R\boldsymbol{Mod}$ e $\phi = (\phi_n)_{n \in \mathbb{Z}} : f \to g, \psi = (\psi_n)_{n \in \mathbb{Z}} : f \to g$ morfismos de cadeias. Então, ϕ é dito **homotópico** a ψ se existe uma família $s = (s_n)_{n \in \mathbb{Z}}$, em que $s_n \in Hom_{{}_R\boldsymbol{Mod}}(X_n, Y_{n+1})$ para todo $n \in \mathbb{Z}$, tal que:*

$$\phi_n - \psi_n = g_{n+1} s_n + s_{n-1} f_n \ \forall \ n \in \mathbb{Z}.$$

*Nesse caso, s é denominada uma **homotopia** de ϕ em ψ.*

Proposição 4.2.2. *Homotopia é uma relação de equivalência em $Hom_{\boldsymbol{Comp}}(f, g)$ para todo $f, g \in \mathcal{O}b(\boldsymbol{Comp})$.*

Demonstração. Segue da definição de homotopia. *QED.*

Ao longo do texto, a relação de homotopia será denotada por $\sim$.

Proposição 4.2.3. *Sejam $f, g \in \mathcal{O}b(\boldsymbol{Comp})$ e $\phi, \psi \in Hom_{\boldsymbol{Comp}}(f, g)$ tais que $\phi \sim \psi$. Então, $H_n(\phi) = H_n(\psi)$ para todo $n \in \mathbb{Z}$.*

Demonstração. Seja $n \in \mathbb{Z}$. Como $\phi \sim \psi$, então existe uma homotopia $(s_n)_{n\in\mathbb{Z}}$ de ϕ em ψ. Portanto:

$$(\phi_n - \psi_n)(z) = (g_{n+1}s_n)(z) + (s_{n-1}f_n)(z) \ \forall\ z \in Z_n(f).$$

Como $Z_n(f) = ker(f_n)$, então $(s_{n-1}f_n)(z) = 0$ para todo $z \in Z_n(f)$. Logo:

$$(\phi_n - \psi_n)(z) = (g_{n+1}s_n)(z) \ \forall\ z \in Z_n(f).$$

Portanto, $(\phi_n - \psi_n)(z) \in B_n(g)$ para todo $z \in Z_n(f)$, logo $H_n(\phi) = H_n(\psi)$. *QED.*

Corolário 4.2.4. *Seja $X \in \mathcal{O}b(\boldsymbol{Comp})$ tal que $1_X : X \to X$ é homotópico a $0_X : X \to X$. Então, X é uma sequência exata.*

Demonstração. Por definição, $H_n(1_X) = 1_{H_n(X)}$ e $H_n(0_X) = 0_{H_n(X)}$ para todo $n \in \mathbb{Z}$. Como $1_X \sim 0_X$, então, pela Proposição 4.2.3, $1_{H_n(X)} = 0_{H_n(X)}$ para todo $n \in \mathbb{Z}$, logo $H_n(X) = 0$ para todo $n \in \mathbb{Z}$, portanto X é uma sequência exata. *QED.*

Lema 4.2.5. *Sejam $f, g \in \mathcal{O}b(\boldsymbol{Comp})$, $\phi, \psi \in Hom_{\boldsymbol{Comp}}(f, g)$ tais que $\phi \sim \psi$ e $F : \boldsymbol{Comp} \to \boldsymbol{Comp}$ um funtor aditivo. Então, $F\phi \sim F\psi$.*

Demonstração. Segue das definições de homotopia e funtor aditivo. *QED.*

Proposição 4.2.6. *Sejam $T : \boldsymbol{Comp} \to \boldsymbol{Comp}$ um funtor aditivo, $f, g \in \mathcal{O}b(\boldsymbol{Comp})$ e $\phi : f \to g$ e $\psi : g \to f$ morfismos de cadeias tais que $\phi\psi \sim 1_g$ e $\psi\phi \sim 1_f$. Então, $H_n(T\phi)$ é um isomorfismo para todo $n \in \mathbb{Z}$.*

Demonstração. Fixe $n \in \mathbb{Z}$. Como T é um funtor aditivo, $\phi\psi \sim 1_g$ e $\psi\phi \sim 1_f$, então, pela Proposição 4.2.3 e pelo Lema 4.2.5, segue que:

$$H_n(T\phi)H_n(T\psi) = H_n(T(\phi\psi)) = H_n(T1_g) = H_n(1_{Tg}) = 1_{H_n(Tg)},$$

$$H_n(T\psi)H_n(T\phi) = H_n(T(\psi\phi)) = H_n(T1_f) = H_n(1_{Tf}) = 1_{H_n(Tf)}.$$

Logo, $H_n(T\phi)$ é um isomorfismo. *QED.*

Definição 4.2.7. *Seja A um R-módulo. Dado um complexo*

$$d : ... \xrightarrow{d_2} X_1 \xrightarrow{d_1} X_0 \xrightarrow{p} A \longrightarrow 0$$

*em ${}_R\boldsymbol{Mod}$, o **complexo deletado** de d é definido como*

$$d_A : ... \xrightarrow{d_2} X_1 \xrightarrow{d_1} X_0 \xrightarrow{d_0} 0\ .$$

Analogamente, dado um complexo

$$d : 0 \longrightarrow A \xrightarrow{i} Y_0 \xrightarrow{d_0} Y_{-1} \xrightarrow{d_{-1}} Y_{-2} \xrightarrow{d_{-2}} ...$$

*em ${}_R\boldsymbol{Mod}$, o **complexo deletado** de d é definido como*

$$d_A : 0 \xrightarrow{d_1} Y_0 \xrightarrow{d_0} Y_{-1} \xrightarrow{d_{-1}} Y_{-2} \xrightarrow{d_{-2}} ...\ .$$

Teorema 4.2.8. *Sejam*

$$g : ... \xrightarrow{g_3} P_2 \xrightarrow{g_2} P_1 \xrightarrow{g_1} P_0 \xrightarrow{\gamma} A \longrightarrow 0\ ,$$

$$h : ... \xrightarrow{h_3} X_2 \xrightarrow{h_2} X_1 \xrightarrow{h_1} X_0 \xrightarrow{\eta} B \longrightarrow 0$$

complexos em ${}_R\boldsymbol{Mod}$ tais que h é exata e P_n é projetivo para todo $n \in \mathbb{N}$, e seja $f : A \to B$ um homomorfismo. Então, existe um único morfismo de cadeias (a menos de homotopia)

$\phi : g_A \to h_B$ tal que $f\gamma = \eta\phi_0$. Equivalentemente, o seguinte diagrama comuta:

$$\begin{tikzcd}
... \arrow[r, "g_3"] & P_2 \arrow[r, "g_2"] \arrow[d, "\phi_2"] & P_1 \arrow[r, "g_1"] \arrow[d, "\phi_1"] & P_0 \arrow[r, "\gamma"] \arrow[d, "\phi_0"] & A \arrow[r] \arrow[d, "f"] & 0 \\
... \arrow[r, "h_3"] & X_2 \arrow[r, "h_2"] & X_1 \arrow[r, "h_1"] & X_0 \arrow[r, "\eta"] & B \arrow[r] & 0
\end{tikzcd}$$

Um morfismo de cadeias $\phi : g_A \to h_B$ tal que $f\gamma = \eta\phi_0$ é denominado um ***morfismo de cadeias sobre*** *f e é denotado por $\overline{f}$ ou $\overline{f}_{g,h}$.*

Demonstração. Como P_0 é projetivo, $\eta : X_0 \to B$ é um homomorfismo sobrejetivo e $f\gamma : P_0 \to B$ é um homomorfismo, então existe um homomorfismo $\phi_0 : P_0 \to X_0$ tal que $f\gamma = \eta\phi_0$. Suponha, por hipótese indutiva, que, para algum $n \in \mathbb{N}$, existem homomorfismos $\phi_0, ..., \phi_n$, em que $\phi_k : P_k \to X_k$ para todo $k \in \{0, ..., n\}$, tais que $f\gamma = \eta\phi_0$ e $\phi_k g_{k+1} = h_{k+1}\phi_{k+1}$ para todo $k \in \{0, ..., n-1\}$. Como $im(g_{n+1}) \subseteq ker(g_n)$ (pois g é um complexo) e $\phi_{n-1}g_n = h_n\phi_n$, então $im(\phi_n g_{n+1}) \subseteq ker(h_n)$; como $im(h_{n+1}) = ker(h_n)$ (pois h é exata), então $im(\phi_n g_{n+1}) \subseteq im(h_{n+1})$. Como P_{n+1} é projetivo, $h_{n+1} : X_{n+1} \to im(X_{n+1})$ é um homomorfismo sobrejetivo e $\phi_n g_{n+1} : P_{n+1} \to im(X_{n+1})$ é um homomorfismo, então existe um homomorfismo $\phi_{n+1} : P_{n+1} \to X_{n+1}$ tal que $\phi_n g_{n+1} = h_{n+1}\phi_{n+1}$. Por indução, segue que $\phi := (\phi_n)_{n\in\mathbb{N}} : g_A \to h_B$ é um morfismo de cadeias tal que $f\gamma = \eta\phi_0$.

Seja $\psi := (\psi_n)_{n\in\mathbb{N}} : g_A \to h_B$ um morfismo de cadeias tal que $f\gamma = \eta\phi_0$. Suponha, por hipótese indutiva, que, para algum $n \in \mathbb{N}$, existem homomorfismos $s_{-1}, s_0, ..., s_n$, em que $s_k : P_k \to X_{k+1}$ para todo $k \in \{0, ..., n\}$ e $s_{-1} : 0 \to X_0$ é o morfismo nulo, tais que $\phi_k - \psi_k = h_{k+1}s_k + s_{k-1}g_k$ para todo $k \in \{0, ..., n\}$. Logo:

$$\begin{aligned}
h_{n+1}(\phi_{n+1} - \psi_{n+1} - s_n g_{n+1}) &= h_{n+1}(\phi_{n+1} - \psi_{n+1}) - h_{n+1}s_n g_{n+1} \\
&= h_{n+1}(\phi_{n+1} - \psi_{n+1}) - (\phi_n - \psi_n - s_{n-1}g_n)g_{n+1}.
\end{aligned}$$

Como g é um complexo, então $g_n g_{n+1} = 0$. Logo:

$$h_{n+1}(\phi_{n+1} - \psi_{n+1} - s_n g_{n+1}) = h_{n+1}(\phi_{n+1} - \psi_{n+1}) - (\phi_n - \psi_n) g_{n+1}.$$

Como $\phi - \psi : g_A \to h_B$ é um morfismo de cadeias, então:

$$h_{n+1}(\phi_{n+1} - \psi_{n+1}) - (\phi_n - \psi_n) g_{n+1} = 0.$$

Logo:

$$h_{n+1}(\phi_{n+1} - \psi_{n+1} - s_n g_{n+1}) = 0;$$

$$im(\phi_{n+1} - \psi_{n+1} - s_n g_{n+1}) \subseteq ker(h_{n+1}).$$

Como h é exata, então $im(h_{n+2}) = ker(h_{n+1})$. Logo:

$$im(\phi_{n+1} - \psi_{n+1} - s_n g_{n+1}) \subseteq im(h_{n+2}).$$

Como P_{n+1} é projetivo, $h_{n+2} : P_{n+2} \to im(h_{n+2})$ é um homomorfismo sobrejetivo e $\phi_{n+1} - \psi_{n+1} - s_n g_{n+1} : P_{n+1} \to im(h_{n+2})$ é um homomorfismo, então existe um homomorfismo $s_{n+1} : P_{n+1} \to X_{n+2}$ tal que:

$$h_{n+2} s_{n+1} = \phi_{n+1} - \psi_{n+1} - s_n g_{n+1}.$$

Por indução, $s = (s_n)_{n \in \mathbb{N}}$ é uma homotopia de ϕ em ψ, logo $\phi \sim \psi$. *QED.*

Teorema 4.2.9. *Sejam*

$$g : 0 \longrightarrow A \xrightarrow{\gamma} Y_0 \xrightarrow{g_0} Y_{-1} \xrightarrow{g_{-1}} Y_{-2} \xrightarrow{g_{-2}} \dots ,$$

$$h : 0 \longrightarrow B \xrightarrow{\eta} E_0 \xrightarrow{h_0} E_{-1} \xrightarrow{h_{-1}} E_{-2} \xrightarrow{h_{-2}} \dots$$

complexos em ${}_R\boldsymbol{Mod}$ tais que g é exata e E_n é injetivo para todo $n \in \mathbb{N}$, e seja $f : A \to B$ um homomorfismo. Então, existe um único morfismo de cadeias (a menos de homotopia)

$\phi : g_A \to h_B$ tal que $\eta f = \phi_0\gamma$. Equivalentemente, o seguinte diagrama comuta:

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & A & \xrightarrow{\gamma} & Y_0 & \xrightarrow{g_0} & Y_{-1} & \xrightarrow{g_{-1}} & Y_{-2} & \xrightarrow{g_{-2}} & \ldots \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \phi_0} & & \downarrow{\scriptstyle \phi_{-1}} & & \downarrow{\scriptstyle \phi_{-2}} & & \\
0 & \longrightarrow & B & \xrightarrow{\eta} & E_0 & \xrightarrow{h_0} & E_{-1} & \xrightarrow{h_{-1}} & E_{-2} & \xrightarrow{h_{-2}} & \ldots
\end{array}$$

*Um morfismo de cadeias $\phi : g_A \to h_B$ tal que $\eta f = \phi_0\gamma$ é denominado um **morfismo de cadeias sobre** f e é denotado por $\overline{f}$ ou $\overline{f}_{g,h}$.*

Demonstração. A demonstração é dual à do Teorema 4.2.8. *QED.*

4.3 Funtores derivados

Nesta seção, será apresentado o conceito de funtor derivado.

Lema 4.3.1. *Seja $T : {}_R\boldsymbol{Mod} \to {}_R\boldsymbol{Mod}$ um funtor aditivo. Então, T induz um funtor aditivo $T : \boldsymbol{Comp} \to \boldsymbol{Comp}$ tal que:*

1. *$T(f_n)_{n\in\mathbb{Z}} := (Tf_n)_{n\in\mathbb{Z}}$ para todo objeto $(f_n)_{n\in\mathbb{Z}}$ de **Comp**;*

2. *$T(\phi_n)_{n\in\mathbb{Z}} := (T\phi_n)_{n\in\mathbb{Z}}$ para todo morfismo $(\phi_n)_{n\in\mathbb{Z}}$ de **Comp**.*

Demonstração. Segue da definição de funtor aditivo e de **Comp**. *QED.*

Lema 4.3.2. *Seja $T : {}_R\boldsymbol{Mod} \to {}_R\boldsymbol{Mod}$ um funtor e, para todo módulo A, sejam R_A, Q_A resoluções deletadas ambas projetivas ou ambas injetivas de A. Para todo $n \in \mathbb{Z}$, sejam $F_n, G_n : {}_R\boldsymbol{Mod} \to {}_R\boldsymbol{Mod}$ funtores tais que $F_n(A) := H_n(TR_A)$ e $G_n(A) := H_n(TQ_A)$ para todo módulo A, e $F_n(f) := H_n(T\overline{f}_{R_A,R_B})$ e $G_n(f) := H_n(T\overline{f}_{Q_A,Q_B})$ para todo homomorfismo $f : A \to B$. Então, para todo $n \in \mathbb{Z}$, existe um isomorfismo natural $\alpha_n : F_n \to G_n$.*

Demonstração. Suponha que ambas as resoluções são projetivas (a demonstração do caso injetivo é análoga, usando o Teorema 4.2.9), e suponha que T é um funtor covariante (o caso contravariante é análogo). Fixe $n \in \mathbb{Z}$ e defina $F := F_n$ e $G := G_n$. Pela Proposição 4.2.3, pelo Lema 4.2.5 e pelo Teorema 4.2.8, segue que os funtores F e G estão bem definidos e são covariantes e aditivos.

Seja A um módulo. Como R_A, Q_A são resoluções projetivas deletadas de A, então, pelo Teorema 4.2.8, existem morfismos de cadeias $\phi_A = \phi : R_A \to Q_A$ e $\psi : Q_A \to R_A$ sobre 1_A. Portanto, $\psi\phi : R_A \to R_A$ e $\phi\psi : Q_A \to Q_A$ são morfismos de cadeias sobre 1_A; como 1_{R_A} e 1_{Q_A} tambem são morfismos de cadeias sobre 1_A, então, pelo Teorema 4.2.8, segue que $\psi\phi \sim 1_{R_A}$ e $\phi\psi \sim 1_{Q_A}$. Assim, pela Proposição 4.2.6, $\alpha_A := H_n(T\phi_A)$ é um isomorfismo.

Sejam B, C módulos e $f : B \to C$ um homomorfismo. Como R_A, R_B, Q_A, Q_B são resoluções projetivas deletadas, então, pelo Teorema 4.2.8, existem morfismos de cadeias $\theta : R_A \to R_B$ e $\eta : Q_A \to Q_B$ sobre f. Portanto, $\phi_B\theta, \eta\phi_A : R_A \to Q_B$ são morfismos de cadeias sobre f; pelo Teorema 4.2.8, segue que $\phi_B\theta \sim \eta\phi_A$. Assim, pela Proposição 4.2.3 e pelo Lema 4.2.5, segue que:

$$H_n(T(\phi_B\theta)) = H_n(T(\eta\phi_A));$$

$$H_n(T(\phi_B))H_n(T\theta) = H_n(T\eta)H_n(T\phi_A);$$

$$\alpha_B(Ff) = (Gf)\alpha_A.$$

Portanto, $\alpha = (\alpha_A)_{A\in \mathcal{O}b({}_R\mathbf{Mod})} : F \to G$ é um isomorfismo natural. *QED.*

Definição 4.3.3. *Para todo módulo A, sejam P_A uma resolução projetiva deletada de A e E_A uma resolução injetiva deletada de A. Sejam $n \in \mathbb{Z}$ e $T : {}_R\boldsymbol{Mod} \to {}_R\boldsymbol{Mod}$ um funtor aditivo. Se T é covariante, definem-se:*

1. *O **n-ésimo funtor derivado à esquerda de** T, denotado por $L_nT : {}_R\boldsymbol{Mod} \to {}_R\boldsymbol{Mod}$, tal que $(L_nT)A := H_n(TP_A)$ para todo módulo A e $(L_nT)f := H_n(T\overline{f}_{P_A,P_B})$ para todo homomorfismo $f : A \to B$;*

2. *O **n-ésimo funtor derivado à direita de** T, denotado por $R^nT : {}_R\boldsymbol{Mod} \to {}_R\boldsymbol{Mod}$, tal que $(R^nT)A := H_{-n}(TE_A)$ para todo módulo A e $(R^nT)f := H_{-n}(T\overline{f}_{E_A,E_B})$ para todo homomorfismo $f : A \to B$.*

Se T é contravariante, definem-se:

1. *O n-**ésimo funtor derivado à esquerda de** T, denotado por $L_nT : {}_R\boldsymbol{Mod} \to {}_R\boldsymbol{Mod}$, tal que $(L_nT)A := H_{-n}(TE_A)$ para todo módulo A e $(L_nT)f := H_{-n}(T\overline{f}_{E_A,E_B})$ para todo homomorfismo $f : A \to B$;*

2. *O n-**ésimo funtor derivado à direita de** T, denotado por $R^nT : {}_R\boldsymbol{Mod} \to {}_R\boldsymbol{Mod}$, tal que $(R^nT)A := H_n(TP_A)$ para todo módulo A e $(R^nT)f := H_n(T\overline{f}_{P_A,P_B})$ para todo homomorfismo $f : A \to B$.*

Pelo Lema 4.3.2, os funtores derivados estão bem definidos, independem da escolha das resoluções projetivas e injetivas para módulos (a menos de um isomorfismo natural) e são aditivos; além disso, a variância de um funtor derivado é a mesma do funtor original.

Lema 4.3.4. *Seja $T : {}_R\boldsymbol{Mod} \to {}_R\boldsymbol{Mod}$ um funtor aditivo. Então, $L_nT \simeq 0$ e $R^nT \simeq 0$ para todo $n \in \mathbb{Z}$ tal que $n < 0$.*

Demonstração. Suponha que T é covariante (o caso contravariante é análogo). Sejam A um módulo e

$$P_A : ... \xrightarrow{a_3} A_2 \xrightarrow{a_2} A_1 \xrightarrow{a_1} A_0 \xrightarrow{a_0} 0 \xrightarrow{a_{-1}} 0 \xrightarrow{a_{-2}} 0 \xrightarrow{a_{-3}} ...$$

uma resolução projetiva deletada de A. Como $a_k = 0$ para todo $k \in \mathbb{Z}$ tal que $k \leq 0$ e T é aditivo, então $Ta_k = 0$ para todo $k \in \mathbb{Z}$ tal que $k \leq 0$, logo

$$(L_nT)A = ker(Ta_n)/im(Ta_{n+1}) = 0$$

para todo $n \in \mathbb{Z}$ tal que $n < 0$; portanto, como T é aditivo, $L_nT \simeq 0$ para todo $n \in \mathbb{Z}$ tal que $n < 0$. Analogamente, demonstra-se que $R^nT \simeq 0$ para todo $n \in \mathbb{Z}$ tal que $n < 0$. *QED.*

Proposição 4.3.5. *Seja $T : {}_R\boldsymbol{Mod} \to {}_R\boldsymbol{Mod}$ um funtor aditivo. Então:*

1. *Se T é exato à direita, então $L_0T \simeq T$;*

2. *Se T é exato à esquerda, então $R^0T \simeq T$.*

Demonstração.

1. Suponha que T é covariante (o caso contravariante é análogo). Sejam A um módulo e

$$P(A) : ... \longrightarrow A_2 \xrightarrow{a_2} A_1 \xrightarrow{a_1} A_0 \xrightarrow{a} A \longrightarrow 0$$

uma resolução projetiva de A. Como T é exato à direita, então

$$TA_1 \xrightarrow{Ta_1} TA_0 \xrightarrow{Ta} TA \longrightarrow 0$$

é uma sequência exata, logo $ker(Ta) = im(Ta_1)$. Portanto:

$$coker(Ta_1) := TA_0/im(Ta_1) = TA_0/ker(Ta).$$

Pelo Teorema 2.1.16, Ta induz um isomomorfismo $\phi_A : coker(Ta_1) \to TA$ dado por:

$$x + ker(Ta) \mapsto (Ta)(x).$$

Seja

$$P_A : ... \longrightarrow A_2 \xrightarrow{a_2} A_1 \xrightarrow{a_1} A_0 \xrightarrow{a_0} 0$$

a resolução deletada de $P(A)$. Como $ker(Ta_0) = TA_0$ (pois T é aditivo), então:

$$(L_0T)A := ker(Ta_0)/im(Ta_1) = TA_0/im(Ta_1) = coker(Ta_1).$$

Portanto, $\phi_A : (L_0T)A \to TA$ é um isomorfismo.

Sejam B, C módulos e $f : B \to C$ um homomorfismo. Sejam

$$P(B) : ... \longrightarrow B_2 \xrightarrow{b_2} B_1 \xrightarrow{b_1} B_0 \xrightarrow{b} B \longrightarrow 0\ ,$$

$$P(C) : ... \longrightarrow C_2 \xrightarrow{c_2} C_1 \xrightarrow{c_1} C_0 \xrightarrow{c} C \longrightarrow 0$$

resoluções projetivas de B e C, respectivamente. Como $im(Tb_1) = ker(Tb)$, $im(Tc_1) = ker(Tc)$ e $T\overline{f}_0 = (T\overline{f})_0$, então, por definição de $(L_0T)f$, tem-se que:

$$(L_0T)f : (L_0T)B \to (L_0T)C \ \mid \ x + ker(Tb) \mapsto (T\overline{f}_0)(x) + ker(Tc).$$

Por definição de $\overline{f}$, $fb = c\overline{f}_0$, logo $(Tf)(Tb) = (Tc)(T\overline{f}_0)$, portanto:

$$(Tf) \cdot \phi_B = \phi_C \cdot (L_0T)f.$$

Assim, $\phi = (\phi_A)_{A \in \mathcal{O}b({}_R\mathbf{Mod})} : L_0T \to T$ é um isomorfismo natural.

2. A demonstração é análoga à do item 1.

QED.

Lema 4.3.6. *Seja*

$$0 \longrightarrow X \xrightarrow{i} Y \xrightarrow{p} Z \longrightarrow 0$$

uma sequência exata de módulos. Então:

1. *Se Q e R são respectivas resoluções projetivas de X e Z, então existe uma resolução projetiva P de Y tal que a seguinte sequência é exata:*

$$R_X \xrightarrow{\bar{i}} P_Y \xrightarrow{\overline{p}} Q_Z;$$

2. *Se Q e R são respectivas resoluções injetivas de X e Z, então existe uma resolução injetiva E de Y tal que a seguinte sequência é exata:*

$$R_X \xrightarrow{\bar{i}} E_Y \xrightarrow{\overline{p}} Q_Z.$$

Demonstração.

1. Defina $P_0 := Q_0 \oplus R_0 = Q_0 \times R_0$. Pelo Teorema 3.2.4, P_0 é projetivo. Defina

$$i_0 : Q_0 \to P_0 \ \mid \ u \mapsto (u, 0),$$

$$p_0 : Q_0 \to P_0 \ \mid \ (u, v) \mapsto v.$$

Assim, a seguinte sequência é exata:

$$0 \longrightarrow Q_0 \xrightarrow{i_0} P_0 \xrightarrow{p_0} R_0 \longrightarrow 0 \ .$$

Suponha que $Q = (Q, q)$ e $R = (R, r)$. Como R_0 é projetivo, $p : Y \to Z$ é um homomorfismo sobrejetivo e $r_0 : R_0 \to Z$ é um homomorfismo, então existe um homomorfismo $\phi_0 : R_0 \to Y$ tal que $r_0 = p\phi_0$. Defina:

$$f_0 : P_0 \to Y \ \mid \ (u, v) \mapsto (iq_0)(u) + \phi_0(v).$$

Portanto, o seguinte diagrama comuta:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & ker(q_0) \arrow[r, "i_0|_{ker(q_0)}"] \arrow[d] & ker(f_0) \arrow[r, "p_0|_{ker(f_0)}"] \arrow[d] & ker(r_0) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & Q_0 \arrow[r, "i_0"] \arrow[d, "q_0"] & P_0 \arrow[r, "p_0"] \arrow[d, "f_0"] & R_0 \arrow[r] \arrow[d, "r_0"] & 0 \\
0 \arrow[r] & X \arrow[r, "i"] \arrow[d] & Y \arrow[r, "p"] \arrow[d] & Z \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

(em que as setas não nomeadas representam as inclusões e projeções canônicas). Como o diagrama comuta, as colunas são exatas e as duas linhas inferiores são exatas, então, pelo Lema 4.1.12, a linha superior do diagrama é exata. Por indução, definem-se $P_n = Q_n \oplus R_n$, i_n, p_n e f_n para todo $n \in \mathbb{N}$, e obtêm-se uma resolução projetiva (P, f) de Y (via um procedimento similar ao adotado no Teorema 3.1.7) e morfismos $\bar{i} := (i_n)_{n\in\mathbb{N}} : Q_X \to P_Y$ e $\bar{p} = (p_n)_{n\in\mathbb{N}} : P_Y \to R_Z$ tais que a seguinte sequência é exata:

$$R_X \xrightarrow{\bar{i}} P_Y \xrightarrow{\bar{p}} Q_Z \ .$$

2. A demonstração é análoga à do item 1 (usando o Teorema 3.3.4 em vez do Teorema 3.2.4).

QED.

Teorema 4.3.7. *Sejam $T : {}_R\boldsymbol{Mod} \to {}_R\boldsymbol{Mod}$ um funtor aditivo e*

$$0 \longrightarrow X \xrightarrow{i} Y \xrightarrow{p} Z \longrightarrow 0$$

uma sequência exata de módulos. Então:

1. *Se T é covariante, existem sequências exatas da forma*

$$\begin{aligned} \dots \longrightarrow L_nTX \xrightarrow{L_nTi} L_nTY \xrightarrow{L_nTp} L_nTZ \xrightarrow{\partial_n} L_{n-1}TX \longrightarrow \dots \\ \dots \longrightarrow L_0TX \xrightarrow{L_0Ti} L_0TY \xrightarrow{L_0Tp} L_0TZ \longrightarrow 0 \end{aligned}$$

e da forma

$$\begin{aligned} 0 \longrightarrow R^0TX \xrightarrow{R^nTi} R^0TY \xrightarrow{R^nTp} R^0TZ \longrightarrow \dots \\ \dots \longrightarrow R^nTX \xrightarrow{R^nTi} R^nTY \xrightarrow{R^nTp} R^nTZ \xrightarrow{\partial_n} R^{n+1}TX \longrightarrow \dots \ . \end{aligned}$$

2. Se T é contravariante, existem sequências exatas da forma

$$... \longrightarrow L_nTZ \xrightarrow{L_nTp} L_nTY \xrightarrow{L_nTi} L_nTX \xrightarrow{\partial_n} L_{n-1}TZ \longrightarrow ...$$

$$... \longrightarrow L_0TZ \xrightarrow{L_0Tp} L_0TY \xrightarrow{L_0Ti} L_0TX \longrightarrow 0$$

e da forma

$$0 \longrightarrow R^0TZ \xrightarrow{R^nTp} R^0TY \xrightarrow{R^nTi} R^0TX \longrightarrow ...$$

$$... \longrightarrow R^nTZ \xrightarrow{R^nTp} R^nTY \xrightarrow{R^nTi} R^nTX \xrightarrow{\partial_n} R^{n+1}TZ \longrightarrow ... \; .$$

Demonstração.

1. Sejam Q, R respectivas resoluções projetivas de X e Z. Pelo Lema 4.3.6, existe uma resolução projetiva P de Y tal que a sequência

$$0 \longrightarrow R_X \xrightarrow{\bar{i}} P_Y \xrightarrow{\overline{p}} Q_Z \longrightarrow 0$$

é exata e $P_n = Q_n \oplus R_n$ para todo $n \in \mathbb{Z}$. Pela Proposição 2.3.12, a sequência

$$0 \longrightarrow TR_n \xrightarrow{Ti_n} TP_n \xrightarrow{Tp_n} TQ_n \longrightarrow 0$$

é exata para todo $n \in \mathbb{Z}$ (pois T é aditivo), logo a seguinte sequência é exata:

$$0 \longrightarrow TR_X \xrightarrow{T\bar{i}} TP_Y \xrightarrow{T\overline{p}} TQ_Z \longrightarrow 0 \; .$$

Portanto, pelo Teorema 4.1.11, existe uma sequência exata da forma

$$... \longrightarrow L_nTX \xrightarrow{L_nTi} L_nTY \xrightarrow{L_nTp} L_nTZ \xrightarrow{\partial_n} L_{n-1}TX \longrightarrow ... \; .$$

Pelo Lema 4.3.4, a sequência anterior termina em 0. Também pelo Teorema 4.1.11, existe uma sequência exata da forma

$$... \longrightarrow R^nTX \xrightarrow{R^nTi} R^nTY \xrightarrow{R^nTp} R^nTZ \xrightarrow{\partial_n} R^{n+1}TX \longrightarrow ... .$$

Pelo Lema 4.3.4, a sequência anterior começa em 0.

2. A demonstração é análoga à do item 1.

QED.

Teorema 4.3.8. *Sejam A um R-módulo à direita, B, C R-módulos à esquerda e $n \in \mathbb{Z}$. Então:*

1. *Se R e Q são resoluções planas de A e C, respectivamente, então:*

$$H_n(R_A \otimes_R C) \simeq H_n(A \otimes_R Q_C);$$

2. *Se P é uma resolução projetiva de B e E é uma resolução injetiva de C, então:*

$$H_n(Hom_{{}_R\boldsymbol{Mod}}(P_B, C)) \simeq H_n(Hom_{{}_R\boldsymbol{Mod}}(B, E_C)).$$

Demonstração. Teorema 7.8, Teorema 7.9 e Corolário 7.10 da referência [3]. *QED.*

4.4 O funtor Ext

Nesta seção, será construído o funtor Ext.

Definição 4.4.1. *Sejam $n \in \mathbb{Z}$, A, B R-módulos à esquerda, $T = Hom_{{}_R\boldsymbol{Mod}}(A, -)$ e $S = Hom_{{}_R\boldsymbol{Mod}}(-, B)$. Definem-se:*

1. $Ext^n_R(A, -) := R^nT : {}_R\boldsymbol{Mod} \to \boldsymbol{Ab}$;

2. $Ext^n_R(-, B) := R^nS : {}_R\boldsymbol{Mod} \to \boldsymbol{Ab}$.

O funtor $Ext^n_R(A,-)$ é covariante aditivo e o funtor $Ext^n_R(-,B)$ é contravariante aditivo. Segue do Teorema 4.3.8 que $Ext^n_R(A,-)$ aplicado em B é isomorfo a $Ext^n_R(-,B)$ aplicado em A.

Proposição 4.4.2. *Sejam A, B R-módulos à esquerda. Então, para todo $n \in \mathbb{Z}$ tal que $n < 0$, vale que $Ext^n_R(A,-) \simeq 0$ e $Ext^n_R(-,B) \simeq 0$.*

Demonstração. Segue do Lema 4.3.4. *QED.*

Proposição 4.4.3. *Sejam A, B R-módulos à esquerda. Então:*

$$Ext^0_R(A,-) \simeq Hom_{{}_R\boldsymbol{Mod}}(A,-),\ Ext^0_R(-,B) \simeq Hom_{{}_R\boldsymbol{Mod}}(-,B).$$

Demonstração. Segue do Teorema 2.8.8 e da Proposição 4.3.5. *QED.*

Proposição 4.4.4. *Sejam A um R-módulo à esquerda projetivo e B um R-módulo à esquerda injetivo. Então, para todo $n \in \mathbb{Z}$ tal que $n \geq 1$, vale que $Ext^n_R(A,-) \simeq 0$ e $Ext^n_R(-,B) \simeq 0$.*

Demonstração. Como A é projetivo, então

$$P : 0 \longrightarrow A \xrightarrow{1_A} A \longrightarrow 0$$

é uma resolução projetiva de A. Logo, para todo R-módulo à esquerda X, vale que $Ext^n_R(A,X) := H_{-n}(Hom_{{}_R\mathbf{Mod}}(P_A,X)) = 0$ para todo $n \in \mathbb{Z}$ tal que $n \geq 1$. Portanto, $Ext^n_R(A,-) \simeq 0$ para todo $n \in \mathbb{Z}$ tal que $n \geq 1$. Analogamente, $Ext^n_R(-,B) \simeq 0$ para todo $n \in \mathbb{Z}$ tal que $n \geq 1$. *QED.*

4.5 O funtor Tor

Nesta seção, será construído o funtor Tor.

Definição 4.5.1. *Sejam $n \in \mathbb{Z}$, A um R-módulo à direita, B um R-módulo à esquerda, $T = A\otimes_R$ e $S = \otimes_R B$. Definem-se:*

1. $Tor_n^R(A,-) := L_nT : {}_R\boldsymbol{Mod} \to \boldsymbol{Ab}$;

2. $Tor_n^R(-,B) := L_nS : \boldsymbol{Mod}_R \to \boldsymbol{Ab}$.

Os funtores $Tor_n^R(A,-)$ e $Tor_n^R(-,B)$ são covariantes aditivos. Pela Proposição 3.4.5 e pelo Teorema 4.3.8, segue que $Tor_n^R(A,-)$ aplicado em B é isomorfo a $Tor_n^R(-,B)$ aplicado em A, e que $Tor_n^R(A,B)$ pode ser calculado usando resoluções planas em vez de projetivas.

Proposição 4.5.2. *Sejam A um R-módulo à direita e B um R-módulo à esquerda. Então, para todo $n \in \mathbb{Z}$ tal que $n < 0$, vale que $Tor_n^R(A,-) \simeq 0$ e $Tor_n^R(-,B) \simeq 0$.*

Demonstração. Segue do Lema 4.3.4. *QED.*

Proposição 4.5.3. *Sejam A um R-módulo à direita e B um R-módulo à esquerda. Então:*

$$Tor_0^R(A,-) \simeq A\otimes_R,\ Tor_0^R(-,B) \simeq \otimes_R B.$$

Demonstração. Segue do Teorema 2.8.11 e da Proposição 4.3.5. *QED.*

Proposição 4.5.4. *Sejam A um R-módulo à direita e B um R-módulo à esquerda. Então:*

1. *A é plano se, e somente se, $Tor_n^R(A,-) \simeq 0$ para todo $n \in \mathbb{Z}$ tal que $n \geq 1$;*

2. *B é plano se, e somente se, $Tor_n^R(-,B) \simeq 0$ para todo $n \in \mathbb{Z}$ tal que $n \geq 1$.*

Demonstração.

1.
   - Suponha que A é plano. Seja X um R-módulo à esquerda. Como A é plano, então $A\otimes_R$ é exato. Portanto, dada uma resolução plana F de X, $A \otimes_R F$ é uma sequência exata, logo $Tor_n^R(A,X) := H_n(A \otimes_R F_X) = 0$ para todo $n \in \mathbb{Z}$ tal que $n \geq 1$. Portanto, $Tor_n^R(A,-) \simeq 0$ para todo $n \in \mathbb{Z}$ tal que $n \geq 1$.
   - Suponha que $Tor_n^R(A,-) \simeq 0$ para todo $n \in \mathbb{Z}$ tal que $n \geq 1$. Seja

$$0 \longrightarrow X \xrightarrow{i} Y \xrightarrow{p} Z \longrightarrow 0$$

uma sequência exata. Pelo Teorema 4.3.7 e pela Proposição 4.5.3, a seguinte sequência sequência é exata:

$$Tor_1^R(A, Z) \xrightarrow{\partial_1} A \otimes_R X \xrightarrow{1_A \otimes i} A \otimes_R Y \ .$$

Como $Tor_1^R(A, Z) = 0$ e a sequência anterior é exata, então $1_A \otimes i$ é injetiva. Portanto, $A\otimes_R$ preserva homomorfismos injetivos. Assim, pelo Teorema 2.8.11 e pela Proposição 2.8.7, $A\otimes_R$ é exato, logo A é plano.

2. A demonstração é análoga à do item 1.

QED.

5 Grupos de homologia, o multiplicador de Schur e extensões stem

Neste capítulo, serão definidos os grupos de homologia e cohomologia, e serão demonstradas fórmulas explícitas para os grupos de homologia de índices 0, 1 e 2. Além disso, será apresentada uma conexão entre o multiplicador de Schur de um grupo e as suas extensões centrais e stem.

Por todo o capítulo, G denotará um grupo arbitrário (multiplicativo), e seu elemento neutro será denotado por 1 ou 1_G.

5.1 Grupos de homologia

Nesta seção, serão definidos os grupos de homologia e cohomologia, e serão demonstradas fórmulas explícitas para os grupos de homologia de índices 0 e 1.

Definição 5.1.1. *Define-se o* ***anel do grupo*** G*, denotado por* $\mathbb{Z}G$*, como o grupo abeliano (aditivo) livre com base* G *munido da aplicação*

$$\cdot : \mathbb{Z}G \times \mathbb{Z}G \to \mathbb{Z}G \;\Bigg|\; \left(\sum_{g\in G} \lambda_g g, \sum_{h\in G} \mu_h h\right) \mapsto \sum_{(g,h)\in G\times G} \lambda_g \mu_h gh.$$

Por toda a seção, A denotará um $\mathbb{Z}G$-módulo à esquerda arbitrário.

Lema 5.1.2. $(\mathbb{Z}G)^{op}$ *e* $\mathbb{Z}G$ *são anéis isomorfos.*

Demonstração. Denote por $\cdot$ a multiplicação em $\mathbb{Z}G$ e por $*$ a multiplicação em $(\mathbb{Z}G)^{op}$. Seja $\psi : \mathbb{Z}G \to (\mathbb{Z}G)^{op}$ dada por:

$$\sum_{g\in G} z_g g \mapsto \sum_{g\in G} z_g g^{-1}.$$

Como $\mathbb{Z}G$ é grupo abeliano livre com base G, então ψ está bem definida e é um isomorfismo de grupos. Além disso:

$$\psi\left(\left(\sum_{g\in G} x_g g\right)\cdot\left(\sum_{h\in G} y_h h\right)\right) = \psi\left(\sum_{g\in G}\sum_{h\in G} x_g y_h gh\right) = \sum_{g\in G}\sum_{h\in G} x_g y_h (gh)^{-1} =$$

$$\sum_{g\in G}\sum_{h\in G} x_g y_h h^{-1} g^{-1} = \left(\sum_{h\in G} y_h h^{-1}\right)\cdot\left(\sum_{g\in G} x_g g^{-1}\right) =$$

$$\psi\left(\sum_{h\in G} y_h h\right)\cdot\psi\left(\sum_{g\in G} x_g g\right) = \psi\left(\sum_{g\in G} x_g g\right) * \psi\left(\sum_{h\in G} y_h h\right).$$

Portanto, $\psi : \mathbb{Z}G \to (\mathbb{Z}G)^{op}$ é um isomorfismo de anéis. *QED.*

Como todo R-módulo à esquerda pode ser transformado em um R^{op}-módulo à direita (e vice-versa) para todo anel R, então o lema anterior mostra que todo $\mathbb{Z}G$-módulo à esquerda pode ser transformado em um $\mathbb{Z}G$-módulo à direita (e vice-versa).

Proposição 5.1.3. *Sejam M um $\mathbb{Z}G$-módulo à direita e N um $\mathbb{Z}G$-módulo à esquerda. Então, $Tor_n^{\mathbb{Z}G}(M,N) \simeq Tor_n^{\mathbb{Z}G}(N,M)$ para todo $n \in \mathbb{Z}$.*

Demonstração. Sejam $n \in \mathbb{Z}$ e P uma resolução plana de M. Por definição, $Tor_n^{\mathbb{Z}G}(M,N) \simeq H_n(P_M \otimes_{\mathbb{Z}G} N)$. Pela Proposição 2.6.5 e pelo Lema 4.1.4, $P_M \otimes_{\mathbb{Z}G} N \simeq N \otimes_{(\mathbb{Z}G)^{op}} P_M$, logo $Tor_n^{\mathbb{Z}G}(M,N) \simeq H_n(N \otimes_{(\mathbb{Z}G)^{op}} P_M)$. Pelo Lema 5.1.2, $(\mathbb{Z}G)^{op} \simeq \mathbb{Z}G$, logo $Tor_n^{\mathbb{Z}G}(M,N) \simeq H_n(N \otimes_{\mathbb{Z}G} P_M) \simeq Tor_n^{\mathbb{Z}G}(N,M)$. *QED.*

Definição 5.1.4. *Um $\mathbb{Z}G$-módulo à esquerda B é dito **trivial** se $gb = b$ para todo $g \in G$ e para todo $b \in B$.*

Definição 5.1.5. *Seja $n \in \mathbb{Z}$. Considere $\mathbb{Z}$ como um $\mathbb{Z}G$-módulo à esquerda trivial. Definem-se:*

1. *O **n-ésimo grupo de homologia de G com coeficientes em** A como*

$$H_n(G,A) := Tor_n^{\mathbb{Z}G}(\mathbb{Z},A);$$

*2. O n-**ésimo grupo de cohomologia de** G **com coeficientes em** A como*

$$H^n(G, A) := Ext^n_{\mathbb{Z}G}(\mathbb{Z}, A).$$

Definição 5.1.6. *Seja $\phi : \mathbb{Z}G \to \mathbb{Z}$ dada por $\sum_{g\in G} \lambda_g g \mapsto \sum_{g\in G} \lambda_g$. Define-se o **ideal aumentado de** G como $\mathfrak{g} := ker(\phi)$.*

A notação introduzida na definição anterior será utilizada pelo restante do capítulo.

Proposição 5.1.7. *Existe um isomorfismo $\alpha : \mathbb{Z} \otimes_{\mathbb{Z}G} A \to A/\mathfrak{g}A$ tal que:*

$$\alpha(x \otimes a) = xa + \mathfrak{g}A \ \forall \ (x, a) \in \mathbb{Z} \times A.$$

Demonstração. Seja $i : \mathfrak{g} \to \mathbb{Z}G$ a inclusão. Como a sequência

$$\mathfrak{g} \xrightarrow{\ i\ } \mathbb{Z}G \xrightarrow{\ \phi\ } \mathbb{Z} \longrightarrow 0$$

é exata, então, pelo Teorema 2.8.11, a seguinte sequência é exata:

$$\mathfrak{g} \otimes_{\mathbb{Z}G} A \xrightarrow{i\otimes 1_A} \mathbb{Z}G \otimes_{\mathbb{Z}G} A \xrightarrow{\phi\otimes 1_A} \mathbb{Z} \otimes_{\mathbb{Z}G} A \longrightarrow 0\ .$$

Portanto, existe um isomorfismo $\gamma : \mathbb{Z}G \otimes_{\mathbb{Z}G} A/im(i \otimes 1_A) \to \mathbb{Z} \otimes_{\mathbb{Z}G} A$ tal que:

$$\gamma(x \otimes a + im(i \otimes 1_A)) = \phi(x) \otimes a \ \forall \ (x, a) \in \mathbb{Z}G \times A.$$

Pela Proposição 2.6.6, existe um isomorfismo $\xi : A \to \mathbb{Z}G \otimes_{\mathbb{Z}G} A$ tal que:

$$\xi(a) = 1 \otimes a \ \forall \ a \in A\,,\ \xi^{-1}(x \otimes a) = xa \ \forall \ (x, a) \in \mathbb{Z}G \times A.$$

Assim, $\xi(\mathfrak{g}A) = im(i \otimes 1_A)$. Portanto, o seguinte mapa é um isomorfismo:

$$\overline{\xi} : A/\mathfrak{g}A \to (\mathbb{Z}G \otimes_{\mathbb{Z}G} A)/im(i \otimes 1_A) \ \mid \ a + \mathfrak{g}A \mapsto 1 \otimes a + im(i \otimes 1_A).$$

Assim, $\psi := \gamma\overline{\xi} : A/\mathfrak{g}A \to \mathbb{Z} \otimes_{\mathbb{Z}G} A$ dado por $a + \mathfrak{g}A \mapsto 1 \otimes a$ é um isomorfismo. Em particular, ψ admite uma inversa $\alpha : \mathbb{Z} \otimes_{\mathbb{Z}G} A \to A/\mathfrak{g}A$ tal que:

$$\alpha(x \otimes a) = xa + \mathfrak{g}A \ \forall \ (x, a) \in \mathbb{Z} \times A.$$

QED.

Teorema 5.1.8. *$H^0(G, A) \simeq Hom_{\mathbb{Z}G\textbf{\textit{Mod}}}(\mathbb{Z}, A)$ e $H_0(G, A) \simeq \mathbb{Z} \otimes_{\mathbb{Z}G} A \simeq A/\mathfrak{g}A$. Em particular, se A é trivial, então $H_0(G, A) \simeq A$.*

Demonstração. Pela Proposição 5.1.7, $\mathbb{Z} \otimes_{\mathbb{Z}G} A \simeq A/\mathfrak{g}A$. Além disso, segue da Proposição 4.4.3 e da Proposição 4.5.3 que $H^0(G, A) \simeq Hom_{\mathbb{Z}G\mathbf{Mod}}(\mathbb{Z}, A)$ e $H_0(G, A) \simeq \mathbb{Z} \otimes_{\mathbb{Z}G} A$. Em particular, se A é $\mathbb{Z}G$-trivial, então $\mathfrak{g}A = 0$, logo $H_0(G, A) \simeq A/\mathfrak{g}A \simeq A$. *QED.*

Lema 5.1.9. *$\mathfrak{g}$ é um grupo abeliano livre com base $G - 1 := \{g - 1 : g \in G\}$.*

Demonstração. Dado $u = \sum_{g \in G} u_g g \in \mathbb{Z}G$, $u \in \mathfrak{g} \iff \sum_{g \in G} u_g = 0$, ou seja, $u \in \mathfrak{g} \iff u = \sum_{g \in G} u_g(g - 1)$. Portanto, $\mathfrak{g} = \langle G - 1 \rangle$. Dados $u = \sum_{g \in G} u_g(g - 1) \in \mathfrak{g}$ e $v = \sum_{g \in G} v_g(g - 1) \in \mathfrak{g}$, segue que $u = \sum_{g \in G} u_g g$ e $v = \sum_{g \in G} v_g g$, logo $u = v \iff u_g = v_g$ para todo $g \in G$ (pois $\mathbb{Z}G$ é grupo abeliano livre com base G). Portanto, $\mathfrak{g}$ é um grupo abeliano livre com base $G - 1$. *QED.*

Teorema 5.1.10. *$H_1(G, \mathbb{Z}) \simeq \mathfrak{g}/\mathfrak{g}^2 \simeq G/G'$.*

Demonstração. Sejam $T = \mathbb{Z} \otimes_{\mathbb{Z}G}$ e $i : \mathfrak{g} \to \mathbb{Z}G$ a inclusão. Como a sequência

$$0 \longrightarrow \mathfrak{g} \xrightarrow{\ i\ } \mathbb{Z}G \xrightarrow{\ \phi\ } \mathbb{Z} \longrightarrow 0$$

é exata, então, pelo Teorema 4.3.7, a seguinte sequência é exata:

$$H_1(G, \mathbb{Z}G) \xrightarrow{L_1 T\phi} H_1(G, \mathbb{Z}) \xrightarrow{\partial_1} H_0(G, \mathfrak{g}) \xrightarrow{L_0 Ti} H_0(G, \mathbb{Z}G) \xrightarrow{L_0 T\phi} H_0(G, \mathbb{Z}) \longrightarrow 0\ .$$

Como $H_0(G, \mathbb{Z}G) \simeq \mathbb{Z} \otimes_{\mathbb{Z}G} \mathbb{Z}G$ (pelo Teorema 5.1.8) e $\mathbb{Z} \otimes_{\mathbb{Z}G} \mathbb{Z}G \simeq \mathbb{Z}$ (pela Proposição 2.6.6), então $H_0(G, \mathbb{Z}G) \simeq \mathbb{Z}$. Como $\mathbb{Z}$ é $\mathbb{Z}G$-trivial, então $H_0(G, \mathbb{Z}) \simeq \mathbb{Z}$ (pelo Teorema 5.1.8). Como $L_0 T\phi : H_0(G, \mathbb{Z}G) \to H_0(G, \mathbb{Z})$ é um homomorfismo sobrejetivo,

$H_0(G,\mathbb{Z}G) \simeq \mathbb{Z}$ e $H_0(G,\mathbb{Z}) \simeq \mathbb{Z}$, então $ker(L_0T\phi) = 0$. Logo, pela exatidão da sequência, segue que $L_0Ti = 0$, logo ∂_1 é sobrejetivo. Como $\mathbb{Z}G$ é livre, então $\mathbb{Z}G$ é plano (pelo Teorema 3.2.5 e pela Proposição 3.4.5), logo $H_1(G,\mathbb{Z}G) := Tor_1^{\mathbb{Z}G}(\mathbb{Z},\mathbb{Z}G) = 0$ (pela Proposição 4.5.4). Assim, pela exatidão da sequência, segue que ∂_1 é injetivo. Como $\partial_1 : H_1(G,\mathbb{Z}) \to H_0(G,\mathfrak{g})$ é sobrejetivo e injetivo, então $H_1(G,\mathbb{Z}) \simeq H_0(G,\mathfrak{g})$. Pelo Teorema 5.1.8, $H_0(G,\mathfrak{g}) \simeq \mathfrak{g}/\mathfrak{g}^2$; logo, $H_1(G,\mathbb{Z}) \simeq \mathfrak{g}/\mathfrak{g}^2$.

Seja $\psi : G \to \mathfrak{g}/\mathfrak{g}^2$ dada por $g \mapsto g - 1 + \mathfrak{g}^2$. Pelo Lema 5.1.9, ψ está bem definida. Além disso, ψ é um homomorfismo, pois

$$(gh-1) - (g-1) - (h-1) = (g-1)(h-1) \in \mathfrak{g}^2 \ \forall\ g,h \in G.$$

Como $\psi : G \to \mathfrak{g}/\mathfrak{g}^2$ é homomorfismo e $\mathfrak{g}/\mathfrak{g}^2$ é abeliano, então $G' \subseteq ker(\psi)$. Assim, pelo Teorema 2.1.16, ψ induz um homomorfismo $\overline{\psi} : G/G' \to \mathfrak{g}/\mathfrak{g}^2$ dado por:

$$gG' \mapsto g - 1 + \mathfrak{g}^2.$$

Como $\mathfrak{g}$ é um grupo abeliano livre com base $G-1$ (pelo Lema 5.1.9), então, pela Proposição 2.4.4, existe um homomorfismo $\xi : \mathfrak{g} \to G/G'$ tal que $\xi(g-1) = gG'$ para todo $g \in G$. Sejam $u = \sum_{g\in G} u_g(g-1) \in \mathfrak{g}$ e $v = \sum_{g \in G} v_g(g-1) \in \mathfrak{g}$. Logo:

$$\begin{aligned} uv &= \sum_{(g,h)\in G\times G} u_g v_h (g-1)(h-1) \\ &= \sum_{(g,h)\in G\times G} u_g v_h [(gh-1) - (g-1) - (h-1)]. \end{aligned}$$

Como ξ é um homomorfismo, então:

$$\begin{aligned} \xi(uv) &= \prod_{(g,h)\in G\times G} [\xi(gh-1)(\xi(g-1))^{-1}(\xi(h-1))^{-1}]^{u_g v_g} \\ &= \prod_{(g,h)\in G\times G} [(gh)g^{-1}h^{-1}]^{u_g v_g} G'. \end{aligned}$$

Assim, $\xi(uv) = G'$, logo $uv \in ker(\xi)$. Como $\{uv : u, v \in \mathfrak{g}\}$ gera $\mathfrak{g}^2$ (como grupo abeliano), então $\mathfrak{g}^2 \subseteq ker(\xi)$. Assim, pelo Teorema 2.1.16, ξ induz um homomorfismo $\overline{\xi} : \mathfrak{g}/\mathfrak{g}^2 \to G/G'$ dado por:

$$g - 1 + \mathfrak{g}^2 \mapsto gG'.$$

Por definição, $\overline{\psi}$ e $\overline{\xi}$ são inversas entre si, logo $\mathfrak{g}/\mathfrak{g}^2 \simeq G/G'$. *QED.*

Definição 5.1.11. *Uma* ***derivação*** *de G em A é uma função $\langle\,\rangle : G \to A$ tal que $\langle xy \rangle = x\langle y \rangle + \langle x \rangle$ para todo $x, y \in G$. O conjunto das derivações de G em A é denotado por $Der(G, A)$.*

Lema 5.1.12. *$Der(G, A)$ é um grupo abeliano (munido da soma usual de funções).*

Demonstração. Segue da definição de $Der(G, A)$. *QED.*

Proposição 5.1.13. *Seja $\psi : Hom_{\mathbb{Z}GMod}(\mathfrak{g}, A) \to Der(G, A)$ tal que:*

$$\psi(f)(x) = f(x - 1)\ \forall\ f \in Hom_{\mathbb{Z}GMod}(\mathfrak{g}, A)\ \forall\ x \in G.$$

Então, ψ é um isomorfismo de grupos.

Demonstração. Como

$$f(xy - 1) = f(x(y - 1) + x - 1) = xf(y - 1) + f(x - 1)\ \forall\ f \in Hom_{\mathbb{Z}GMod}(\mathfrak{g}, A)\ \forall\ x, y \in G,$$

então $\psi(f) \in Der(G, A)$ para todo $f \in Hom_{\mathbb{Z}GMod}(\mathfrak{g}, A)$, logo ψ está bem definida e é um homomorfismo de grupos. Dado $\phi \in Der(G, A)$, seja $\phi_0 : G - 1 \to A \mid g - 1 \mapsto \phi(g)$. Como $\mathfrak{g}$ é grupo abeliano livre com base $G - 1$ (pelo Lema 5.1.9), então existe um único homomorfismo de grupos $\overline{\phi_0} : \mathfrak{g} \to A$ tal que $\overline{\phi_0}|_{G-1} = \phi_0$. Como para todo $\phi \in Der(G, A)$, segue que

$$\overline{\phi_0}(x(g - 1)) = \overline{\phi_0}((xg - 1) - (x - 1)) = \overline{\phi_0}(xg - 1) - \overline{\phi_0}(x - 1) =$$

$$\phi_0(xg - 1) - \phi_0(x - 1) = \phi(xg) - \phi(x) = x\phi(g)\ \forall\ x, g \in G,$$

então $\overline{\phi_0} \in Hom_{\mathbb{Z}GMod}(\mathfrak{g}, A)$ (pois $G-1$ é base de $\mathfrak{g}$). Defina:

$$\xi : Der(G, A) \to Hom_{\mathbb{Z}GMod}(\mathfrak{g}, A) \mid \phi \mapsto \overline{\phi_0}.$$

Como $G-1$ é base de $\mathfrak{g}$, então, por definição, ξ e ψ são inversas, logo ψ é um isomorfismo de grupos. *QED.*

Definição 5.1.14. *Define-se o* ***produto semidireto*** *de A por G, denotado por $A \rtimes G$, como o conjunto $A \times G$ munido da operação $+ : (A \times G) \times (A \times G) \to A \times G$ dada por:*

$$(a, g) + (a', g') := (a + ga', gg').$$

Lema 5.1.15. *$(A \rtimes G, +)$ é um grupo.*

Demonstração. A associatividade de $+$ segue da definição. Além disso:

$$(a, g) + (0, 1) = (0, 1) + (a, g) = (a, g) \ \forall \ (a, g) \in A \rtimes G,$$

$$(a, g) + (-g^{-1}a, g^{-1}) = (-g^{-1}a, g^{-1}) + (a, g) = (0, 1) \ \forall \ (a, g) \in A \rtimes G.$$

Portanto, $A \rtimes G$ é um grupo cujo elemento neutro é $(0, 1)$ e em que a inversão é dada por $(a, g)^{-1} = (-g^{-1}a, g^{-1})$ para todo $(a, g) \in A \rtimes G$. *QED.*

Teorema 5.1.16. *Suponha que G é um grupo livre com base X. Então, $\mathfrak{g}$ é um $\mathbb{Z}G$-módulo livre com base $X - 1$.*

Demonstração. Como $xy - 1 = (x - 1) + x(y - 1)$ e $x^{-1} - 1 = -x^{-1}(x - 1)$ para todo $x, y \in G$ e X é base de G, então $G - 1 \subseteq \langle X - 1 \rangle$. Como $G - 1 \subseteq \langle X - 1 \rangle$ e $\langle G - 1 \rangle = \mathfrak{g}$ (pelo Lema 5.1.9), então $\langle X - 1 \rangle = \mathfrak{g}$.

Seja B um $\mathbb{Z}$-módulo à esquerda e $\phi : X - 1 \to B$. Defina $\lambda : X \to B \rtimes G$ tal que $x \mapsto (\phi(x-1), x)$. Como G é um grupo livre com base X, então existe um homomorfismo $\overline{\lambda} : G \to B \rtimes G$ tal que $\overline{\lambda}|_X = \lambda$. Como X gera G, então existe uma função $\langle \ \rangle : G \to B$

tal que $\overline{\lambda}(g) = (\langle g \rangle, g)\ \forall\ g \in G$. Como $\overline{\lambda}$ é um homomorfismo, então:

$$(\langle gh \rangle, gh) = \overline{\lambda}(gh) = \overline{\lambda}(g) + \overline{\lambda}(h) = (\langle g \rangle, g) + (\langle h \rangle, h) = (\langle g \rangle + g\langle h \rangle, gh)\ \forall\ g, h \in G.$$

Assim, $\langle gh \rangle = \langle g \rangle + g\langle h \rangle$ para todo $g, h \in G$, logo $\langle\ \rangle \in Der(G, B)$. Seja $\psi : Hom_{\mathbb{Z}GMod}(\mathfrak{g}, B) \to Der(G, B)$ conforme definido na Proposição 5.1.13. Então, $\overline{\phi} := \psi^{-1}(\langle\ \rangle) : \mathfrak{g} \to B$ é um homomorfismo tal que $\overline{\phi}|_{X-1} = \phi$. Se $\gamma : \mathfrak{g} \to B$ é um homomorfismo tal que $\gamma|_{X-1} = \phi$, então, pela Proposição 2.1.11, $\gamma = \overline{\phi}$. Portanto, $\mathfrak{g}$ é um $\mathbb{Z}G$-módulo livre com base $X - 1$. *QED.*

Corolário 5.1.17. *Suponha que G é um grupo livre. Então, $H_n(G, A) = H^n(G, A) = 0$ para todo $n \in \mathbb{N}$ tal que $n \geq 2$.*

Demonstração. Como G é grupo livre, então $\mathfrak{g}$ é um $\mathbb{Z}G$-módulo livre (pelo Teorema 5.1.16), logo a sequência

$$0 \longrightarrow \mathfrak{g} \xrightarrow{\ i\ } \mathbb{Z}G \xrightarrow{\ \phi\ } \mathbb{Z} \longrightarrow 0\ ,$$

em que i é a inclusão, é uma $\mathbb{Z}G$-resolução livre de $\mathbb{Z}$; em particular, pelo Teorema 3.2.5 e pela Proposição 3.4.5, essa sequência é uma $\mathbb{Z}G$-resolução projetiva e plana de $\mathbb{Z}$. Assim, por definição, $H_n(G, A) = H^n(G, A) = 0$ para todo $n \in \mathbb{N}$ tal que $n \geq 2$. *QED.*

Proposição 5.1.18. *Seja P_n o grupo abeliano livre com base G^{n+1} para todo $n \in \mathbb{N}$. Considere P_n como $\mathbb{Z}G$-módulo via a ação*

$$\cdot : G \times G^{n+1} \to G^{n+1}\ \mid\ x \cdot (x_0, ..., x_n) = (xx_0, ..., xx_n).$$

Seja $\partial_0 = \phi : \mathbb{Z}G \to \mathbb{Z}$. Dado $n \in \mathbb{N}\backslash\{0\}$, seja $\partial_n : P_n \to P_{n-1}$ o homomorfismo de grupos abelianos dado por

$$(x_0, ..., x_n) \mapsto \sum_{i=0}^{n} (-1)^i (x_0, ..., \hat{x}_i, ..., x_n),$$

em que $(x_0, ..., \hat{x_i}, ..., x_n)$ *denota a* $(n-1)$*-upla* $(x_0, ..., x_{i-1}, x_{i+1}, ..., x_n)$. *Então,*

$$P : ... \longrightarrow P_2 \xrightarrow{\partial_2} P_1 \xrightarrow{\partial_1} P_0 \simeq \mathbb{Z}G \xrightarrow{\partial_0} \mathbb{Z} \longrightarrow 0$$

é uma $\mathbb{Z}G$*-resolução livre de* $\mathbb{Z}$.

Demonstração. Seja $\beta_n = \{(1, x_1, ..., x_n) : x_1, ..., x_n \in G\}$ para todo $n \in \mathbb{N}$. Por definição, β_n gera P_n como $\mathbb{Z}G$-módulo para todo $n \in \mathbb{N}$. Sejam $v_1, ..., v_k \in \beta_n$ ($v_i = (1, x_{i1}, ..., x_{in})$) elementos 2 a 2 distintos. Sejam $g_1, ..., g_\ell \in G$ elementos 2 a 2 distintos e $\lambda_{ij} \in \mathbb{Z}$ tais que

$$\sum_{i=1}^{k} \left(\sum_{j=1}^{\ell} \lambda_{ij} g_j \right) v_i = 0.$$

Logo:

$$\sum_{i=1}^{k} \sum_{j=1}^{\ell} \lambda_{ij} (g_j v_i) = 0.$$

Como $g_j v_i = (g_j, g_j x_{i1}, ..., g_j x_{in})$, $v_1, ..., v_k$ são 2 a 2 distintos e $g_1, ..., g_\ell$ são 2 a 2 distintos, então $g_j v_i = g_{j'} v_{i'}$ se, e somente se, $j = j'$ e $i = i'$. Assim, como P_n é um grupo abeliano livre com base G^{n+1}, então $\lambda_{ij} = 0$ para todo $i \in \{1, ..., k\}$ e para todo $j \in \{1, ..., \ell\}$, logo $\sum_{j=1}^{\ell} \lambda_{ij} g_j = 0$ para todo $i \in \{1, ..., k\}$. Portanto, P_n é um $\mathbb{Z}G$-módulo livre com base β_n.

Seja $(x_0, x_1) \in P_1$. Então:

$$\partial_0 \partial_1((x_0, x_1)) = \phi \partial_1((x_0, x_1)) = \phi(x_1 - x_0) = 0.$$

Como ∂_0 e ∂_1 são homomorfismos de $\mathbb{Z}$-módulos, então $\partial_0 \partial_1 = 0$. Sejam $n \in \mathbb{N} \backslash \{0\}$ e $(x_0, ..., x_{n+1}) \in P_{n+1}$. Então:

$$\partial_n \partial_{n+1}((x_0, ..., x_{n+1})) = \partial_n \left(\sum_{i=0}^{n} (-1)^i (x_0, ..., \hat{x_i}, ..., x_{n+1}) \right) =$$

$$\sum_{i=0}^{n} (-1)^i \left(\sum_{j=0}^{i-1} (-1)^j (x_0, ..., \hat{x_j}, ..., \hat{x_i}, ..., x_{n+1}) + \sum_{j=i+1}^{n+1} (-1)^{j-1} (x_0, ..., \hat{x_i}, ..., \hat{x_j}, ..., x_{n+1}) \right) =$$

$$\sum_{i=0}^{n}(-1)^i\left(\sum_{j=0}^{i-1}(-1)^j(x_0,...,\hat{x_j},...,\hat{x_i},...,x_{n+1})-\sum_{j=i+1}^{n+1}(-1)^j(x_0,...,\hat{x_i},...,\hat{x_j},...,x_{n+1})\right)=$$

$$\sum_{i=0}^{n}\sum_{j=0}^{i-1}(-1)^{i+j}(x_0,...,\hat{x_j},...,\hat{x_i},...,x_{n+1})-\sum_{i=0}^{n}\sum_{j=i+1}^{n+1}(-1)^{i+j}(x_0,...,\hat{x_i},...,\hat{x_j},...,x_{n+1})=0.$$

Como ∂_k é homomorfismo de $\mathbb{Z}G$-módulos para todo $k \in \mathbb{N}$, então $\partial_n\partial_{n+1}=0$ para todo $n \in \mathbb{N}\backslash\{0\}$. Assim, $\partial_n\partial_{n+1}=0$ para todo $n \in \mathbb{N}$, logo P é um complexo de $\mathbb{Z}G$-módulos.

Seja $s_{-1}:\mathbb{Z}\to P_0$ o homomorfismo de $\mathbb{Z}$-módulos tal que $1_\mathbb{Z}\mapsto 1_G$. Dado $n\in\mathbb{N}$, seja $s_n:P_n\to P_{n+1}$ o homomorfismo de $\mathbb{Z}$-módulos tal que $(x_0,...,x_n)\mapsto(1,x_0,...,x_n)$. Então:

$$\phi s_{-1}(1_\mathbb{Z})=\phi(1_G)=1_\mathbb{Z}.$$

Como ϕ e s_{-1} são homomorfismos de $\mathbb{Z}$-módulos, então $\phi s_{-1}=1_\mathbb{Z}$. Sejam $n\in\mathbb{N}$ e $(x_0,...,x_n)\in P_n$. Então:

$$(\partial_{n+1}s_n+s_{n-1}\partial_n)((x_0,...,x_n))=\partial_{n+1}((1,x_0,...,x_n))+s_{n-1}\left(\sum_{i=0}^{n}(-1)^i(x_0,...,\hat{x_i},...,x_n)\right)=$$

$$(x_0,...,x_n)+\sum_{j=0}^{n}(-1)^{j+1}(1,x_0,...,\hat{x_j},...,x_n)+\sum_{i=0}^{n}(-1)^i(1,x_0,...,\hat{x_i},...,x_n)=(x_0,...,x_n).$$

Como $\partial_{n+1}s_n+s_{n-1}\partial_n$ é um homomorfismo de $\mathbb{Z}$-módulos para todo $n\in\mathbb{N}$, então:

$$\partial_{n+1}s_n+s_{n-1}\partial_n=1_{P_n}\ \forall\ n\in\mathbb{N}.$$

Assim, $s=(s_n)_{n\in\mathbb{Z}}$ (em que $s_n=0$ se $n\le -2$) é uma homotopia entre $1_P:P\to P$ e $0_P:P\to P$. Pelo Corolário 4.2.4, P é uma sequência exata de $\mathbb{Z}$-módulos, logo P é uma sequência exata de $\mathbb{Z}G$-módulos. Portanto, P é uma $\mathbb{Z}G$-resolução livre de $\mathbb{Z}$. *QED.*

Proposição 5.1.19. *Seja Q_0 o $\mathbb{Z}G$-módulo livre cuja base é o conjunto unitário $\{[\,]\}$. Seja Q_n o $\mathbb{Z}G$-módulo livre com base G^n para todo $n\in\mathbb{N}\backslash\{0\}$ (em que $(x_1,...,x_n)\in G^n$ é denotado por $[x_1,...,x_n]$). Seja $d_0=\phi:\mathbb{Z}G\to\mathbb{Z}$. Dado $n\in\mathbb{N}\backslash\{0\}$, seja $d_n:Q_n\to Q_{n-1}$*

o homomorfismo de $\mathbb{Z}G$-módulos dado por:

$$[x_1, ..., x_n] \mapsto x_1[x_2, ..., x_n] + (-1)^n[x_1, ..., x_{n-1}] + \sum_{i=1}^{n-1}(-1)^i[x_1, ..., x_i x_{i+1}, ..., x_n].$$

Então,

$$Q : ... \longrightarrow Q_2 \xrightarrow{d_2} Q_1 \xrightarrow{d_1} Q_0 \simeq \mathbb{Z}G \xrightarrow{d_0} \mathbb{Z} \longrightarrow 0$$

é uma $\mathbb{Z}G$-resolução livre de $\mathbb{Z}$ (denominada ***$\mathbb{Z}G$-resolução padrão de $\mathbb{Z}$****).*

Demonstração. Seja P a $\mathbb{Z}G$-resolução de $\mathbb{Z}$ definida na Proposição 5.1.18. Por definição, Q_n é um grupo abeliano livre com base $\alpha_n := \{x_0[x_1, ..., x_n] : x_0, ..., x_n \in G\}$ para todo $n \in \mathbb{N}$. Como Q_n e P_n são grupos abelianos livres com bases α_n e G^{n+1}, respectivamente, então, para todo $n \in \mathbb{N}$, existem homomorfismos de grupos abelianos dados por:

$$\tau_n : P_n \to Q_n \;\mid\; (x_0, ..., x_n) \mapsto x_0[x_0^{-1}x_1, x_1^{-1}x_2, ..., x_{n-1}^{-1}x_n],$$

$$\sigma_n : Q_n \to P_n \;\mid\; x_0[x_1, ..., x_n] \mapsto x_0(1, x_1, x_1x_2, ..., x_1...x_n).$$

Por definição, $\tau_n = \sigma_n^{-1}$ para todo $n \in \mathbb{N}$ e $d_n = \tau_{n-1}\partial_n\sigma_n$ para todo $n \in \mathbb{N}\backslash\{0\}$. Como $d_n = \tau_{n-1}\partial_n\sigma_n$ para todo $n \in \mathbb{N}\backslash\{0\}$ e $\partial_n\partial_{n-1} = 0$ para todo $n \in \mathbb{N}\backslash\{0\}$, então $d_nd_{n-1} = 0$ para todo $n \in \mathbb{N}\backslash\{0\}$, logo Q é um complexo de $\mathbb{Z}$-módulos.

Seja $\tau := (\tau_n)_{n\in\mathbb{Z}}$ (em que $\tau_n := 0$ se $n < 0$). Como P e Q são complexos de $\mathbb{Z}$-módulos, $H_n(P) = 0$ para todo $n \in \mathbb{Z}$ (pela Proposição 5.1.18) e $\tau : P \to Q$ é um isomorfismo de complexos (pelo Lema 4.1.4), então, pela Proposição 4.1.7 e pela Proposição 2.2.6, $H_n(Q) = H_n(P) = 0$ para todo $n \in \mathbb{Z}$. Assim, Q é uma sequência exata de $\mathbb{Z}$-módulos, logo Q é uma $\mathbb{Z}G$-resolução livre de $\mathbb{Z}$. *QED.*

O teorema a seguir é baseado no Teorema 6.5.8 do livro *An Introduction to Homological Algebra* (referência [6]), de Charles Weibel.

Teorema 5.1.20. *Suponha que G é um grupo finito de ordem m. Então:*

$$mH_n(G,A) = mH^n(G,A) = 0 \ \forall\ n \in \mathbb{N}\backslash\{0\}.$$

Demonstração. Seja Q a $\mathbb{Z}G$-resolução de $\mathbb{Z}$ definida na Proposição 5.1.19. Seja $N = \sum_{g\in G} g$. Defina os seguintes homomorfismos de $\mathbb{Z}G$-módulos:

$$\xi_n : Q_n \to Q_n \ \mid\ x \mapsto mx \ \forall\ n \in \mathbb{N},$$

$$s_{-1} : \mathbb{Z} \to Q_0 \ \mid\ x \mapsto xN[\,],$$

$$s_n : Q_n \to Q_{n+1} \ \left|\ [x_1, ..., x_n] \mapsto (-1)^{n+1} \sum_{x_{n+1}\in G} [x_1, ..., x_{n+1}] \ \forall\ n \in \mathbb{N}.\right.$$

Por definição:

$$(d_1 s_0 + s_{-1} d_0)([\,]) = -\sum_{x_1\in G} (x_1[\,] - [\,]) + N[\,] = m[\,] = \xi_0([\,]).\ (1)$$

Sejam $n \in \mathbb{N}\backslash\{0\}$ e $[x_1, ..., x_n] \in Q_n$. Então:

$$d_{n+1}s_n([x_1, ..., x_n]) =$$

$$(-1)^{n+1} \sum_{x_{n+1}\in G} \Bigg(x_1[x_2, ..., x_{n+1}] + (-1)^{n+1}[x_1, ..., x_n] +$$

$$\sum_{i=1}^{n} (-1)^i [x_1, ..., x_i x_{i+1}, ..., x_{n+1}] \Bigg) =$$

$$-(-1)^n \sum_{x_{n+1}\in G} \Bigg(x_1[x_2, ..., x_{n+1}] + \sum_{i=1}^{n} (-1)^i [x_1, ..., x_i x_{i+1}, ..., x_{n+1}] \Bigg) +$$

$$m[x_1, ..., x_n].\ (2)$$

Além disso:

$$s_{n-1}d_n([x_1, ..., x_n]) =$$

$$(-1)^n \sum_{x_{n+1}\in G}\Bigg(x_1[x_2,...,x_{n+1}] + (-1)^n[x_1,...,x_{n-1},x_{n+1}] +$$

$$\sum_{i=1}^{n-1}(-1)^i[x_1,...,x_ix_{i+1},...,x_{n+1}]\Bigg). \ (3)$$

Por (2) e (3), segue que:

$$(d_{n+1}s_n + s_{n-1}d_n)([x_1,...,x_n]) =$$

$$m[x_1,...,x_n] - \sum_{x_{n+1}\in G}[x_1,...,x_{n-1},x_nx_{n+1}] + \sum_{x_{n+1}\in G}[x_1,...,x_{n-1},x_{n+1}] = \xi_n([x_1,...,x_n]). \ (4)$$

Como s_{-1}, s_n e ξ_n são homomorfismos de $\mathbb{Z}G$-módulos para todo $n \in \mathbb{N}$, então, por (1) e (4), segue que:

$$d_{n+1}s_n + s_{n-1}d_n = \xi_n \ \forall \ n \in \mathbb{N}. \ (5)$$

Seja F um funtor aditivo na categoria de $\mathbb{Z}G$-módulos. Logo:

$$Fd_{n+1}Fs_n + Fs_{n-1}Fd_n = F\xi_n \ \forall \ n \in \mathbb{N}. \ (6)$$

Como F é um funtor aditivo, então $F\xi_n : FQ_n \to FQ_n$ é dada por $x \mapsto mx$ para todo $n \in \mathbb{N}$. Assim, por (6), segue que:

$$(Fd_{n+1}Fs_n)(x) = mx \ \forall \ n \in \mathbb{N} \ \forall \ x \in ker(Fd_n);$$

$$m \cdot ker(Fd_n) \subseteq im(Fd_{n+1}) \ \forall \ n \in \mathbb{N};$$

$$m \cdot ker(Fd_n)/im(Fd_{n+1}) = 0 \ \forall \ n \in \mathbb{N}. \ (7)$$

Em particular, tomando $F = \otimes_{\mathbb{Z}G}A$ e $F = Hom_{\mathbb{Z}G}(-,A)$, respectivamente, obtém-se que:

$$mH_n(G,A) = mH^n(G,A) = 0 \ \forall \ n \in \mathbb{N}\backslash\{0\}.$$

QED.

Lema 5.1.21. *Suponha que G é um grupo finito e que A é um $\mathbb{Z}G$-módulo finitamente gerado. Então, $H_n(G, A)$ é um grupo abeliano finitamente gerado para todo $n \in \mathbb{N}$.*

Demonstração. Pelo Teorema 5.1.8, $H_0(G, A) \simeq \mathbb{Z} \otimes_{\mathbb{Z}G} A$, logo $H_0(G, A)$ é um grupo abeliano finitamente gerado (pela Proposição 2.6.14). Assim, seja $n \in \mathbb{N}$ tal que $n \geq 1$. Seja Q a $\mathbb{Z}G$-resolução padrão de $\mathbb{Z}$. Por definição, segue que:

$$H_n(G, A) \simeq ker(d_n \otimes 1_A)/im(d_{n+1} \otimes 1_A).$$

Como $ker(d_n \otimes 1_A)$ é um subgrupo de $Q_n \otimes_{\mathbb{Z}G} A$ e $Q_n \otimes_{\mathbb{Z}G} A$ é um grupo abeliano finitamente gerado (pela Proposição 2.6.14), então $ker(d_n \otimes 1_A)$ é um grupo abeliano finitamente gerado (pela Proposição 2.4.7), logo $H_n(G, A)$ é um grupo abeliano finitamente gerado. *QED.*

Teorema 5.1.22. *Suponha que G é um grupo finito e que A é um $\mathbb{Z}G$-módulo finitamente gerado. Então, $H_n(G, A)$ é um grupo abeliano finito para todo $n \in \mathbb{N}\backslash\{0\}$.*

Demonstração. Segue do Teorema 5.1.20 e do Lema 5.1.21. *QED.*

5.2 O multiplicador de Schur e a Fórmula de Hopf

Nesta seção, será definido o multiplicador de Schur de um grupo e será demonstrada a Fórmula de Hopf.

Pelo restante da seção, salvo menção do contrário, todos os módulos considerados serão à esquerda (resultados análogos são válidos para módulos à direita).

Por toda a seção, suponha que $G \simeq F/R$, em que F é um grupo livre com base X e R é um subgrupo normal de F. Pelo Teorema de Nielsen-Schreier (Teorema 8.9 da referência [4]), que afirma que todo subgrupo de um grupo livre é livre, segue que R é um grupo livre (Y denotará uma base de R). Sejam $\pi : F \to G$ a projeção canônica e $\overline{\pi} : \mathbb{Z}F \to \mathbb{Z}G$ o homomorfismo de grupos tal que $\overline{\pi}|_F = \pi$. Além disso, definem-se $\mathfrak{f}$ como o ideal aumentado de F e $r := ker(\overline{\pi})$.

Proposição 5.2.1. *$r \subseteq \mathfrak{f}$, $\mathbb{Z}G \simeq \mathbb{Z}F/r$, $\mathfrak{g} \simeq \mathfrak{f}/r$.*

Demonstração. Seja $x = \sum_{f \in F} z_f f \in \mathfrak{r}$. Logo:

$$0 = \overline{\pi}\left(\sum_{f \in F} z_f f\right) = \sum_{f \in F} z_f \overline{\pi}(f) = \sum_{f \in F} z_f \pi(f) \in \mathbb{Z}G.$$

Como $\pi(F) = G$ e $\mathbb{Z}G$ é um grupo abeliano livre com base G, então $\sum_{f \in F} z_f = 0$, logo $x \in \mathfrak{f}$. Portanto, $\mathfrak{r} \subseteq \mathfrak{f}$. Como $\overline{\pi} : \mathbb{Z}F \to \mathbb{Z}G$ é um homomorfismo sobrejetivo de grupos e $\mathfrak{r} = ker(\overline{\pi})$, então $\mathbb{Z}G \simeq \mathbb{Z}F/\mathfrak{r}$ (pelo Teorema 2.1.16). Em particular, como $\overline{\pi}(\mathfrak{f}) = \mathfrak{g}$ e $\mathfrak{r} \subseteq \mathfrak{f}$, então $\mathfrak{g} \simeq \mathfrak{f}/\mathfrak{r}$. *QED.*

Lema 5.2.2. *$\mathfrak{r}$ é um $\mathbb{Z}F$-módulo livre com base $Y - 1$.*

Demonstração. Seja $(f_j)_{j \in J}$ uma família de elementos de F tal que $\cup_{j \in J} f_j R = F$ e $f_i R \cap f_j R = \emptyset$ se $i \neq j$. Seja $u \in \mathfrak{r}$. Como $u \in \mathbb{Z}F$ e $\cup_{j \in J} f_j R = F$, existem um subconjunto finito J' de J, $r_1, ..., r_n \in R$ e uma família $(z_{ji})_{j \in J', 1 \leq i \leq n}$ de elementos de $\mathbb{Z}$ tais que

$$u = \sum_{j \in J'} \sum_{i=1}^{n} z_{ji} f_j r_i.$$

Como $u \in \mathfrak{r} = ker(\overline{\pi})$ e $R = ker(\pi)$, então:

$$\sum_{j \in J'} \left(\sum_{i=1}^{n} z_{ji}\right) \pi(f_j) = \sum_{j \in J'} \sum_{i=1}^{n} z_{ji} \pi(f_j) \pi(r_i) = \overline{\pi}(u) = 0.$$

Como $\pi(f_i) \neq \pi(f_j)$ se $i \neq j$ (por definição de $(f_j)_{j \in J}$) e $\mathbb{Z}F$ é um grupo abeliano livre com base F, então:

$$\sum_{i=1}^{n} z_{ji} = 0 \ \forall \ j \in J'.$$

Portanto:

$$u = \sum_{j \in J'} \sum_{i=1}^{n} z_{ji} f_j r_i - \sum_{j \in J'} \left(\sum_{i=1}^{n} z_{ji}\right) f_j = \sum_{i=1}^{n} \left(\sum_{j \in J'} z_{ji} f_j (r_i - 1)\right) \in \langle R - 1 \rangle.$$

Como $xy - 1 = (x - 1) + x(y - 1)$ e $x^{-1} - 1 = -x^{-1}(x - 1)$ para todo $x, y \in F$ e Y é base de R, então $R - 1 \subseteq \langle Y - 1 \rangle$. Logo, $u \in \langle Y - 1 \rangle$. Assim, $\mathfrak{r} \subseteq \langle Y - 1 \rangle$, logo $\mathfrak{r} = \langle Y - 1 \rangle$

(pois, por definição, $Y - 1 \subseteq r$).

Sejam $\alpha_1, ..., \alpha_n \in \mathbb{Z}F$ e $y_1, ..., y_n \in Y$ tais que $\sum_{k=1}^{n} \alpha_k(y_k - 1) = 0$. Como $\cup_{j\in J} f_j R = F$, então existe um subconjunto finito J'' de J tal que, para cada $k \in \{1, ..., n\}$, existem $\beta_{jk} \in \mathbb{Z}R$ tais que $\alpha_k = \sum_{j\in J''} \beta_{jk} f_j$. Logo:

$$\sum_{k=1}^{n} \left(\sum_{j\in J''} \beta_{jk} f_j \right) (y_k - 1) = 0;$$

$$\sum_{j\in J''} \left(\sum_{k=1}^{n} \beta_{jk}(y_k - 1) \right) f_j = 0.$$

Seja $\gamma_j = \sum_{k=1}^{n} \beta_{jk}(y_k - 1) \ \forall\ j \in J''$. Logo:

$$\sum_{j\in J''} \gamma_j f_j = 0.$$

Por definição, $\gamma_j \in \mathbb{Z}R$ para todo $j \in J''$. Assim, existem $r_1, ..., r_m \in R$ ($r_i \neq r_j$ se $i \neq j$) e uma família $(z_{ji})_{j\in J', 1\leq i\leq n}$ de elementos de $\mathbb{Z}$ tais que $\gamma_j = \sum_{i=1}^{m} z_{ji} r_i$. Portanto:

$$\sum_{j\in J''} \sum_{i=1}^{m} z_{ji} r_i f_j = 0.$$

Como $r_i \neq r_j$ se $i \neq j$, $f_i R \cap f_j R = \emptyset$ se $i \neq j$ e $\mathbb{Z}F$ é um grupo abeliano livre com base F, então $z_{ji} = 0$ para todo $j \in J''$ e para todo $i \in \{1, ..., m\}$. Assim, $\gamma_j = 0$ para todo $j \in J''$, logo:

$$\sum_{k=1}^{n} \beta_{jk}(y_k - 1) = 0 \ \forall\ j \in J''.$$

Como R é um grupo livre com base Y, então $\beta_{jk} = 0$ para todo $j \in J''$ e para todo $k \in \{1, ..., n\}$ (pelo Teorema 5.1.9), logo $\alpha_k = 0$ para todo $k \in \{1, ..., n\}$. Portanto, r é um $\mathbb{Z}F$-módulo livre com base $Y - 1$. *QED.*

Lema 5.2.3. *Seja M um $\mathbb{Z}F$-módulo à esquerda. Então, M/rM é um $\mathbb{Z}G$-módulo à* *esquerda se munido da operação* $\cdot : \mathbb{Z}G \times (M/rM) \to M/rM$ *dada por:*

$$\left(\sum_{f\in F} z_f \pi(f), m + rM\right) \mapsto \sum_{f\in F} z_f f m + rM.$$

Demonstração. Seja $\cdot : \mathbb{Z}G \times (M/rM) \to M/rM$ conforme definida no enunciado. Se $f, f' \in F$ são tais que $\pi(f) = \pi(f')$, então $f - f' \in ker(\overline{\pi}) = r$, logo:

$$(f - f')m \in rM \ \forall \ m \in M.$$

Portanto, $\cdot$ está bem definida e M/rM é um $\mathbb{Z}G$-módulo se munido da operação $\cdot$. *QED.*

Lema 5.2.4. *Seja* M *um* $\mathbb{Z}F$*-módulo à esquerda livre com base* W*. Então,* M/rM *é um* $\mathbb{Z}G$*-módulo livre com base* $\{w + rM : w \in W\}$*. Além disso,* $M/\mathfrak{f}M$ *é um grupo abeliano livre com base* $\{w + \mathfrak{f}M : w \in W\}$*.*

Demonstração. Como M é um $\mathbb{Z}F$-módulo livre com base W, então $M = \coprod_{w\in W}(\mathbb{Z}F)w$, logo $rM = \coprod_{w\in W} rw$, portanto:

$$\frac{M}{rM} = \frac{\coprod_{w\in W}(\mathbb{Z}F)w}{\coprod_{w\in W} rw} \simeq \coprod_{w\in W} \frac{\mathbb{Z}Fw}{rw} \simeq \coprod_{w\in W} (\mathbb{Z}F/r)(w + rM).$$

Como $\mathbb{Z}F/r \simeq \mathbb{Z}G$ (pela Proposição 5.2.1), então M/rM é um $\mathbb{Z}G$-módulo livre com base $\{w + rM : w \in W\}$. Em particular, se $G = 1$, então $\mathbb{Z}G \simeq \mathbb{Z}$ e $r = \mathfrak{f}$, logo $M/\mathfrak{f}M$ é um $\mathbb{Z}$-módulo livre (ou seja, grupo abeliano livre) com base $\{w + \mathfrak{f}M : w \in W\}$. *QED.*

Proposição 5.2.5. *Seja* M *um* $\mathbb{Z}F$*-módulo à esquerda. Então:*

1. $\mathfrak{g}(M/rM) = \mathfrak{f}M/rM$;

2. *Existe um isomorfismo* $\psi : \mathbb{Z} \otimes_{\mathbb{Z}G} (M/rM) \to M/\mathfrak{f}M$ *tal que:*

$$\psi(x \otimes (m + rM)) = xm + \mathfrak{f}M \ \forall \ (x, m) \in X \times M.$$

Em particular, $\mathbb{Z} \otimes_{\mathbb{Z}G} (M/rM) \simeq M/\mathfrak{f}M$*.*

Demonstração.

1. Pelo Lema 5.2.3, M/rM é um $\mathbb{Z}G$-módulo se munido da operação $\cdot$. Se $f \in F, g \in G$ são tais que $\pi(f) = g$, então $g(m + rM) := f(m + rM)$ para todo $m \in M$. Logo:

$$\mathfrak{g}(M/rM) = \mathfrak{f}(M/rM) = \mathfrak{f}M/rM.$$

2. Como $\mathfrak{g}(M/rM) = \mathfrak{f}M/rM$, então, pela Proposição 5.1.7, existe um isomorfismo $\alpha : \mathbb{Z} \otimes_{\mathbb{Z}G} (M/rM) \to (M/rM)/(\mathfrak{f}M/rM)$ tal que:

$$\alpha(x \otimes (m + rM)) = x(m + rM) + (\mathfrak{f}M/rM) \ \forall \ (x, m) \in \mathbb{Z} \times M.$$

Pelo Teorema 2.1.17, existe um isomorfismo $\beta : (M/rM)/(\mathfrak{f}M/rM) \to M/\mathfrak{f}M$ dado por:

$$(m + rM) + (\mathfrak{f}M/rM) \mapsto m + \mathfrak{f}M.$$

Portanto, $\psi := \beta\alpha : \mathbb{Z} \otimes_{\mathbb{Z}G} (M/rM) \to M/\mathfrak{f}M$ é um isomorfismo tal que:

$$\psi(x \otimes (m + rM)) = xm + \mathfrak{f}M \ \forall \ (x, m) \in X \times M.$$

QED.

Proposição 5.2.6. *$r/r\mathfrak{f} \simeq R/R'$, $(r\mathfrak{f} + \mathfrak{f}r)/r\mathfrak{f} \simeq [F, R]/R'$, $r/(r\mathfrak{f} + \mathfrak{f}r) \simeq R/[F, R]$.*

Demonstração. Como $r/r\mathfrak{f}$ é um grupo abeliano livre com base $\{y - 1 + r\mathfrak{f} : y \in Y\}$ (pelo Lema 5.2.4), R/R' é um grupo abeliano livre com base $\{yR' : y \in Y\}$ e

$$|\{y - 1 + r/r\mathfrak{f} : y \in Y\}| = |\{yR' : y \in Y\}| = |Y|,$$

então existe isomorfismo de grupos $\phi : r/r\mathfrak{f} \to R/R'$ tal que $\phi(y - 1 + r\mathfrak{f}) = yR'$ para todo $y \in Y$. Em particular, $r/r\mathfrak{f} \simeq R/R'$. Como

$$xy - 1 = (x - 1)(y - 1) + (x - 1) + (y - 1) \ \forall \ x, y \in R,$$

$$x^{-1} - 1 = -(x-1) - (x-1)(x^{-1}-1) \ \forall \ x, y \in R$$

e Y é base de R, então:

$$\phi(r - 1 + r\mathfrak{f}) = rR' \ \forall \ r \in R.$$

Como $[F, R] \subseteq R$ (pelo Lema 1.1.7, pois $R \lhd F$) e

$$(f-1)(r-1) = ([f,r]-1) + ([f,r]-1)(rf-1) + (r-1)(f-1) \ \forall \ f \in F \ \forall \ r \in R,$$

então $(f-1)(r-1) + r\mathfrak{f} = ([f,r]-1) + r\mathfrak{f} \ \forall \ f \in F \ \forall \ r \in R$, logo:

$$\phi((f-1)(r-1) + r\mathfrak{f}) = [f,r]R' \ \forall \ f \in F \ \forall \ r \in R.$$

Assim, $\phi((r\mathfrak{f} + \mathfrak{f}r)/r\mathfrak{f}) = [F,R]/R'$, portanto:

$$(r\mathfrak{f} + \mathfrak{f}r)/r\mathfrak{f} \simeq [F,R]/R'.$$

Como $\phi : r/r\mathfrak{f} \to R/R'$ é um isomorfismo tal que $\phi(r - 1 + r\mathfrak{f}) = rR'$ para todo $r \in R$ e $\phi((r\mathfrak{f} + \mathfrak{f}r)/r\mathfrak{f}) = [F,R]/R'$, então, pelo Teorema 2.1.17, existe um isomorfismo $\overline{\phi} : r/(r\mathfrak{f} + \mathfrak{f}) \to R/[F,R]$ tal que $\overline{\phi}(r - 1 + (r\mathfrak{f} + \mathfrak{f}r)) = r[F,R]$ para todo $r \in R$. Em particular:

$$r/(r\mathfrak{f} + \mathfrak{f}r) \simeq R/[F,R].$$

QED.

Lema 5.2.7. *Sejam $\mathfrak{a}, \mathfrak{b}$ ideais bilaterais livres de $\mathbb{Z}F$ com respectivas bases A e B. Então, $\mathfrak{ab}$ é um $\mathbb{Z}F$-módulo livre com base $AB := \{ab : a \in A, b \in B\}$.*

Demonstração. Por definição, tem-se que:

$$\mathfrak{ab} = \langle AB \rangle.$$

Sejam $a_1, ..., a_n \in A$ (2 a 2 distintos), $b_1, ..., b_m \in B$ (2 a 2 distintos) e $x_{ij} \in \mathbb{Z}F$ para todo $i \in \{1, ..., n\}$ e para todo $j \in \{1, ..., m\}$ tais que $\sum_{j=1}^{m} \sum_{i=1}^{n} x_{ij} a_i b_j = 0$. Como

$\sum_{j=1}^{m}\left(\sum_{i=1}^{n} x_{ij}a_i\right) b_j = \sum_{j=1}^{m}\sum_{i=1}^{n} x_{ij}a_ib_j = 0$ e $\mathfrak{b}$ é um $\mathbb{Z}F$-módulo livre com base B, então $\sum_{i=1}^{n} x_{ij}a_i = 0$ para todo $j \in \{1,...,m\}$, logo $x_{ij} = 0$ para todo $i \in \{1,...,n\}$ e para todo $j \in \{1,...,m\}$ (pois $\mathfrak{a}$ é um $\mathbb{Z}F$-módulo livre com base A). Portanto, $\mathfrak{ab}$ é um $\mathbb{Z}F$-módulo livre com base AB. *QED.*

Teorema 5.2.8. *Para todo $n \in \mathbb{N}\backslash\{0\}$, defina:*

$$r^0 := \mathbb{Z}F \ , \ G_0 := r^0/r^1 \ , \ G_{2n} := r^n/r^{n+1} \ , \ G_{2n-1} := r^{n-1}\mathfrak{f}/r^n\mathfrak{f},$$

$$d_{2n} : G_{2n} \to G_{2n-1} \ | \ x + r^{n+1} \mapsto x + r^n\mathfrak{f},$$

$$d_{2n-1} : G_{2n-1} \to G_{2n-2} \ | \ x + r^n\mathfrak{f} \mapsto x + r^n.$$

Então,

$$G : ... \longrightarrow G_2 \xrightarrow{d_2} G_1 \xrightarrow{d_1} G_0 \simeq \mathbb{Z}G \xrightarrow{\phi} \mathbb{Z} \longrightarrow 0$$

*é uma $\mathbb{Z}G$-resolução livre de $\mathbb{Z}$ (denominada $\mathbb{Z}G$**-resolução de Gruenberg de** $\mathbb{Z}$).*

Demonstração. Como F e R são grupos livres com respectivas bases F e R, então $\mathfrak{f}$ e r são $\mathbb{Z}G$-módulos livres com respectivas bases $X-1$ e $Y-1$ (pelo Teorema 5.1.16 e pelo Lema 5.2.2). Assim, pelos Lemas 5.2.4 e 5.2.7, G_n é um $\mathbb{Z}G$-módulo livre para todo $n \in \mathbb{N}$. Por definição dos mapas d_n, tem-se que (para todo $n \in \mathbb{N}$):

$$ker(d_{2n}) = r^n\mathfrak{f}/r^{n+1} \ , \ im(d_{2n}) = r^n/r^n\mathfrak{f},$$

$$ker(d_{2n+1}) = r^{n+1}/r^{n+1}\mathfrak{f} \ , \ im(d_{2n+1}) = r^n\mathfrak{f}/r^{n+1}.$$

Portanto, $im(d_{2n+1}) = ker(d_{2n})$ e $im(d_{2n+2}) = ker(d_{2n-1})$ para todo $n \in \mathbb{N}$. Além disso, como $im(\phi) = \mathbb{Z}$, $G_0 = r^0/r^1 = \mathbb{Z}F/r \simeq \mathbb{Z}G$ e $im(d_1) = r^0\mathfrak{f}/r^1 = \mathfrak{f}/r \simeq \mathfrak{g} = ker(\phi)$ (pela Proposição 5.2.1), então a sequência

$$... \longrightarrow G_2 \xrightarrow{d_2} G_1 \xrightarrow{d_1} G_0 \simeq \mathbb{Z}G \xrightarrow{\phi} \mathbb{Z} \longrightarrow 0$$

é exata e, em particular, é uma $\mathbb{Z}G$-resolução livre de $\mathbb{Z}$. *QED.*

Definição 5.2.9. *Define-se o* ***multiplicador de Schur*** *de G como $M(G) := H_2(G,\mathbb{Z})$.*

Teorema 5.2.10. ***(Fórmula de Hopf)***

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

Demonstração. Pelo Teorema 5.2.8, existe uma $\mathbb{Z}G$-resolução livre de $\mathbb{Z}$ (em particular, pelo Teorema 3.2.5 e pela Proposição 3.4.5, uma resolução plana) dada por:

$$\ldots \longrightarrow \mathfrak{r}\mathfrak{f}/\mathfrak{r}^2\mathfrak{f} \xrightarrow{d_3} \mathfrak{r}/\mathfrak{r}^2 \xrightarrow{d_2} \mathfrak{f}/\mathfrak{r}\mathfrak{f} \longrightarrow \mathbb{Z}G \longrightarrow \mathbb{Z} \longrightarrow 0 \ ,$$

em que:

$$d_3 : \mathfrak{r}\mathfrak{f}/\mathfrak{r}^2\mathfrak{f} \to \mathfrak{r}/\mathfrak{r}^2 \ \mid \ x + \mathfrak{r}^2\mathfrak{f} \mapsto x + \mathfrak{r}^2,$$

$$d_2 : \mathfrak{r}/\mathfrak{r}^2 \to \mathfrak{f}/\mathfrak{r}\mathfrak{f} \ \mid \ x + \mathfrak{r}^2 \mapsto x + \mathfrak{r}\mathfrak{f}.$$

Aplicando o funtor $\mathbb{Z}\otimes_{\mathbb{Z}G}$ à sequência anterior, obtém-se a sequência

$$\ldots \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}G} (\mathfrak{r}\mathfrak{f}/\mathfrak{r}^2\mathfrak{f}) \xrightarrow{1\otimes d_3} \mathbb{Z} \otimes_{\mathbb{Z}G} (\mathfrak{r}/\mathfrak{r}^2) \xrightarrow{1\otimes d_2} \mathbb{Z} \otimes_{\mathbb{Z}G} (\mathfrak{f}/\mathfrak{r}\mathfrak{f}) \longrightarrow \ldots \ .$$

Pelo isomorfismo estabelecido na Proposição 5.2.5, esta sequência é isomorfa (pelo Lema 4.1.4) à sequência

$$\ldots \longrightarrow \mathfrak{r}\mathfrak{f}/\mathfrak{f}\mathfrak{r}\mathfrak{f} \xrightarrow{\Delta_3} \mathfrak{r}/\mathfrak{f}\mathfrak{r} \xrightarrow{\Delta_2} \mathfrak{f}/\mathfrak{f}^2 \longrightarrow \ldots \ ,$$

em que:

$$\Delta_3 : \mathfrak{r}\mathfrak{f}/\mathfrak{f}\mathfrak{r}\mathfrak{f} \to \mathfrak{r}/\mathfrak{f}\mathfrak{r} \ \mid \ x + \mathfrak{f}\mathfrak{r}\mathfrak{f} \mapsto x + \mathfrak{f}\mathfrak{r},$$

$$\Delta_2 : \mathfrak{r}/\mathfrak{f}\mathfrak{r} \to \mathfrak{f}/\mathfrak{f}^2 \ \mid \ x + \mathfrak{f}\mathfrak{r} \mapsto x + \mathfrak{f}^2.$$

Assim, por definição de $H_2(G,\mathbb{Z})$ e pela Proposição 5.1.3, segue que:

$$M(G) := H_2(G,\mathbb{Z}) \simeq \frac{ker(\Delta_2)}{im(\Delta_3)}.$$

Por definição, $ker(\Delta_2) = (r \cap \mathfrak{f}^2)/\mathfrak{f}r$ e $im(\Delta_3) = (r\mathfrak{f} + \mathfrak{f}r)/\mathfrak{f}r$. Seja $\theta : r/(r\mathfrak{f} + \mathfrak{f}r) \to \mathfrak{f}^2$ dada por $x + (r\mathfrak{f} + \mathfrak{f}r) \mapsto x + \mathfrak{f}^2$. Por definição, $ker(\theta) = (r \cap \mathfrak{f}^2)/(r\mathfrak{f} + \mathfrak{f}r)$. Assim, pelo Teorema 2.1.17, tem-se que:

$$M(G) \simeq \frac{ker(\Delta_2)}{im(\Delta_3)} = \frac{(r \cap \mathfrak{f}^2)/\mathfrak{f}r}{(r\mathfrak{f} + \mathfrak{f}r)/\mathfrak{f}r} \simeq \frac{r \cap \mathfrak{f}^2}{(r\mathfrak{f} + \mathfrak{f}r)} = ker(\theta).$$

Seja $\eta : R/[F, R] \to F/F'$ dada por $r[F, R] \mapsto rF'$. Por definição, $ker(\eta) = (F' \cap R)/[F, R]$. Sejam $\overline{\psi}$ e $\overline{\phi}$ os respectivos isomorfismos estabelecidos no Teorema 5.1.10 e na Proposição 5.2.6. Por definição dos mapas, o seguinte diagrama comuta:

$$\begin{tikzcd} r/(r\mathfrak{f} + \mathfrak{f}r) \arrow[r, "\theta"] \arrow[d, "\overline{\phi}"] & \mathfrak{f}/\mathfrak{f}^2 \arrow[d, "\overline{\psi}"] \\ R/[F, R] \arrow[r, "\eta"] & F/F' \end{tikzcd}$$

Logo, $ker(\theta) \simeq ker(\eta)$. Portanto:

$$M(G) \simeq ker(\theta) \simeq ker(\eta) = (F' \cap R)/[F, R].$$

QED.

5.3 Extensões centrais e extensões stem

Nesta seção, serão estudadas as extensões centrais e extensões stem de um grupo e a sua conexão com o multiplicador de Schur.

Definição 5.3.1. *Uma* ***extensão central*** *de G é um par $(\overline{G}, Z)$, em que $\overline{G}$ é um grupo e $Z \lhd \overline{G}$, tal que $G \simeq \overline{G}/Z$ e $Z \subseteq Z(\overline{G})$.*

Definição 5.3.2. *Uma* ***extensão stem*** *de G é um par $(\overline{G}, Z)$, em que $\overline{G}$ é um grupo e $Z \lhd \overline{G}$, tal que $G \simeq \overline{G}/Z$ e $Z \subseteq Z(\overline{G}) \cap \overline{G}'$; se $Z \simeq M(G)$, então $(\overline{G}, Z)$ é dito um* ***recobrimento stem*** *de G.*

Os dois teoremas a seguir são essenciais para diversas demonstrações a respeito de $\mathscr{X}(G)$ e $\nu(G)$ nos dois capítulos seguintes.

Teorema 5.3.3. *Existe um recobrimento stem de G.*

Demonstração. Sejam F um grupo livre e $R \lhd F$ tais que $G \simeq F/R$. Como $\phi : R/(F' \cap R) \to F/F' \ \mid \ r(F' \cap R) \mapsto rF'$ é um homomorfismo injetivo de grupos e F/F' é um grupo abeliano livre (pois F é livre), então, pelo Teorema 2.4.8, $R/(F' \cap R)$ é um grupo abeliano livre. Como $R/[F,R]$ é um grupo abeliano (pois $R' \subseteq [F,R]$), $R/(F' \cap R)$ é um grupo abeliano livre e $\psi : R/[F,R] \to R/(F' \cap R) \ \mid \ r + [F,R] \mapsto r + (F' \cap R)$ é um homomorfismo sobrejetivo tal que $ker(\psi) = (F' \cap R)/[F,R]$, então, pela Proposição 2.4.5, existe um subgrupo S de R ($[F,R] \subseteq S$) tal que:

$$\frac{R}{[F,R]} = \frac{F' \cap R}{[F,R]} \oplus \frac{S}{[F,R]}.$$

Pelo Lema 2.3.9, segue que $R = (F' \cap R)S$ e $(F' \cap R) \cap S = [F,R]$. Assim, pelo Teorema 5.2.10, segue que:

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

Como $[F,R] \subseteq S$, então $[F/S, R/S] = 1$, logo $R/S \subseteq Z(F/S)$. Como $R = (F' \cap R)S$, então $R/S \subseteq (F'S)/S = (F/S)'$. Portanto, $R/S \subseteq Z(F/S) \cap (F/S)'$. Como $R/S \subseteq Z(F/S) \cap (F/S)'$, $(F/S)/(R/S) \simeq F/R \simeq G$ e $R/S \simeq M(G)$, então $(F/S, R/S)$ é um recobrimento stem de G. *QED.*

Teorema 5.3.4. *Seja $(\overline{G}, Z)$ uma extensão central de G. Então, existe um homomorfismo sobrejetivo $\phi : M(G) \to \overline{G}' \cap Z$. Em particular, se $(\overline{G}, Z)$ é uma extensão stem de G, então existe um homomorfismo sobrejetivo $\phi : M(G) \to Z$.*

Demonstração. Sejam F um grupo livre e $S \lhd F$ tais que $\overline{G} \simeq F/S$. Como $Z \lhd \overline{G} \simeq F/S$, então existe $R \lhd F$ tal que $S \subseteq R$ e $Z \simeq R/S$. Como $(\overline{G}, Z)$ é uma extensão central de G, $Z \simeq R/S$ e $\overline{G} \simeq F/S$, então $G \simeq (F/S)/(R/S) \simeq F/R$ e $R/S \subseteq Z(F/S)$. Como $R/S \subseteq Z(F/S)$, então $[F/S, R/S] = 1$, logo $[F,R]S/S = 1$, portanto:

$$[F,R] \subseteq S.$$

Assim, o homomorfismo $\xi : (F' \cap R)/[F,R] \to R/S \mid x[F,R] \mapsto xS$ está bem definido. Por definição, $im(\xi) = (F' \cap R)S/S = (F'S \cap RS)/S$. Como $S \subseteq R$, então $F'S \cap RS = F'S \cap R$. Logo, $im(\xi) = (F'S \cap R)/S = (F'S/S) \cap (R/S)$. Como $Z \simeq R/S$ e $\overline{G}' \simeq (F/S)' = F'S/S$, então $im(\xi) \simeq \overline{G}' \cap Z$. Como $im(\xi) \simeq \overline{G}' \cap Z$ e $M(G) \simeq (F' \cap R)/[F,R]$ (pelo Teorema 5.2.10), então existe um homomorfismo sobrejetivo $\phi : M(G) \to \overline{G}' \cap Z$. *QED.*

5.4 O multiplicador de Schur de grupos finitos

Nesta seção, serão apresentadas propriedades do multiplicador de Schur de grupos finitos. As demonstrações serão omitidas.

Proposição 5.4.1. *Seja H um grupo finito. Então, $M(H)$ é finito e $|H| \cdot M(H) = 0$.*

Demonstração. Segue do Teorema 5.1.20 e do Teorema 5.1.22. *QED.*

Proposição 5.4.2. *Sejam X, Y grupos finitos tais que $MDC(|X|, |Y|) = 1$. Então:*

$$M(X \times Y) \simeq M(X) \times M(Y).$$

Demonstração. Teorema 2.1 da referência [7]. *QED.*

Definição 5.4.3. *Seja H um grupo (multiplicativo). Defina:*

$$E := \{n \in \mathbb{N} \backslash \{0\} : h^n = 1_H \ \forall \ h \in H\}.$$

Se $E \neq \emptyset$, define-se o ***expoente*** *do grupo H, denotado por $exp(H)$, como o elemento mínimo do conjunto E; caso contrário, denota-se $exp(H) = \infty$.*

Proposição 5.4.4. *Sejam $p \in \mathbb{N}$ primo e $a_1, ..., a_n \in \mathbb{N}$ tais que $a_1 \geq a_2 \geq ... \geq a_n \geq 1$. Seja*

$$H = \prod_{i=1}^{n} \mathbb{Z}/p^{a_i}\mathbb{Z}.$$

Então:

$$M(H) = \prod_{i=2}^{n} (\mathbb{Z}/p^{a_i}\mathbb{Z})^{i-1}.$$

Em particular, $exp(M(H)) = p^{a_2}$ *e* $|M(H)| = p^u$*, em que* $u = \sum_{i=2}^{n}(i-1)a_i$.

Demonstração. Teorema 1.2 da referência [8]. *QED.*

6 A construção $\mathscr{X}(G)$

Neste capítulo, será estudada a construção $\mathscr{X}(G)$, definida no artigo *On weak permutability between groups* (referência [1]) de S. Sidki.

Por todo o capítulo, G denotará um grupo (multiplicativo) arbitrário com elemento neutro 1, e $\psi : G \to G^{\psi}$ denotará um isomorfismo tal que G e G^{ψ} são disjuntos. Além disso, será utilizada a seguinte notação:

$$g^{\psi} := \psi(g) \ \forall \ g \in G, \ g^{-\psi} := \psi(g^{-1}) \ \forall \ g \in G, \ Y^{\psi} := \psi(Y) \ \forall \ Y \subseteq G.$$

Definição 6.0.1. *O grupo $\mathscr{X}(G)$ é definido como:*

$$\mathscr{X}(G) := \frac{G * G^{\psi}}{\langle [g, g^{\psi}] : g \in G \rangle^{G * G^{\psi}}}.$$

Pelo restante do capítulo, as imagens de G e G^{ψ} pela projeção canônica $p : G * G^{\psi} \to \mathscr{X}(G)$ serão denotadas por G e G^{ψ}, respectivamente.

Definição 6.0.2. *Definem-se os seguintes subgrupos de $\mathscr{X}(G)$:*

$$D(G) := [G, G^{\psi}], \ L(G) := \langle \{g^{-1}g^{\psi} : g \in G\} \rangle,$$

$$L_1(G) := [L(G), G], \ L_2(G) := [L(G), G^{\psi}],$$

$$W(G) := D(G) \cap L(G), \ R(G) := [L_1(G), G^{\psi}].$$

Lema 6.0.3. *Sejam H um grupo e $u : G \to H$, $v : G^{\psi} \to H$ homomorfismos tais que $(u * v)([g, g^{\psi}]) = 1_H$ para todo $g \in G$. Então, existe um único homomorfismo $\phi : \mathscr{X}(G) \to H$ tal que $\phi(g) = u(g)$ e $\phi(g^{\psi}) = v(g^{\psi})$ para todo $g \in G$.*

Demonstração. Segue das definições de produto livre e de $\mathscr{X}(G)$. *QED.*

Em particular, existe um isomorfismo $\psi : \mathscr{X}(G) \to \mathscr{X}(G)$ tal que $g \mapsto g^{\psi}$ e $g^{\psi} \mapsto g$ para todo $g \in G$.

6.1 A construção $T(\overline{G}, Z)$

Nesta seção, será apresentada a construção $T(\overline{G}, Z)$ e a sua relação com a construção $\mathscr{X}(G)$.

Por toda a seção, $(\overline{G}, Z)$ denotará uma extensão stem de G.

Definição 6.1.1. *Definem-se:*

$$\overline{T} := \overline{G} \times \overline{G} \times \overline{G},$$

$$\overline{\psi} : \overline{T} \to \overline{T} \ \mid \ (x, y, z) \mapsto (z, y, x),$$

$$\overline{G}_1 := \{(g, g, 1) : g \in \overline{G}\}, \ \overline{G}_2 := \{(1, g, g) : g \in \overline{G}\} = \overline{\psi}(\overline{G}_1),$$

$$Z_1 := \{(z, z, 1) : z \in Z\}, \ Z_2 := \{(1, z, z) : z \in Z\} = \overline{\psi}(Z_1),$$

$$T(\overline{G}, Z) := \frac{\langle \overline{G}_1, \overline{G}_2 \rangle}{Z_1 Z_2}, \ G_1 := \frac{\overline{G}_1 Z_2}{Z_1 Z_2}, \ G_2 := \frac{\overline{G}_2 Z_1}{Z_1 Z_2}.$$

Proposição 6.1.2. *Valem as seguintes propriedades:*

1. $G_1 = \{(g, g, 1)Z_1Z_2 : g \in \overline{G}\}$ *e* $G_2 = \{(1, g, g)Z_1Z_2 : g \in \overline{G}\}$*;*

2. $T(\overline{G}, Z) = \langle G_1, G_2 \rangle$ *e* $G_1 \cap G_2 = 1$*;*

3. $G_1 \simeq G_2 \simeq G$*;*

4. *Existe um homomorfismo* $\psi : T(\overline{G}, Z) \to T(\overline{G}, Z)$ *dado por:*

$$(x, y, z)Z_1Z_2 \mapsto (z, y, x)Z_1Z_2.$$

   Além disso, $\psi^2 = id$ *e* $G_1^{\psi} = G_2$*;*

5. $[g_1, g_1^{\psi}] = 1$ *para todo* $g_1 \in G_1$.

Demonstração.

1. Segue da definição anterior.

2. Segue da definição anterior e do item 1.

3. Seja $\phi : \overline{G} \to \overline{G}_1$ dada por $g \mapsto (g, g, 1)$. Por definição, $\phi : \overline{G} \to \overline{G}_1$ e $\phi|_Z : Z \to Z_1$ são isomorfismos, logo ϕ induz um isomorfismo $\phi' : \overline{G}/Z \to \overline{G}_1/Z_1$. Portanto:

$$G_1 := \frac{\overline{G}_1 Z_2}{Z_1 Z_2} \simeq \frac{\overline{G}_1}{Z_1} \simeq \frac{\overline{G}}{Z} := G.$$

Analogamente, $G_2 \simeq G$.

4. Como $Z \lhd \overline{G}$, então $Z_1 \lhd \overline{T}$ e $Z_2 \lhd \overline{T}$, logo $Z_1 Z_2 = Z_2 Z_1$ e $Z_1 Z_2 \lhd \overline{T}$. Como $Z_1 Z_2 = Z_2 Z_1 \lhd \overline{T}$, $\overline{\psi}(Z_1) = Z_2$ e $\overline{\psi}^2 = \overline{\psi}$, então $\overline{\psi}$ induz um homomorfismo $\psi : T(\overline{G}, Z) \to T(\overline{G}, Z)$ dado por $(x, y, z)Z_1 Z_2 \mapsto (z, y, x)Z_1 Z_2$.

5. Como $G_1 = \{(g, g, 1)Z_1 Z_2 : g \in \overline{G}\}$ e

$$(g, g, 1)(1, g, g)Z_1 Z_2 = (g, g^2, g)Z_1 Z_2 = (1, g, g)(g, g, 1)Z_1 Z_2 \ \forall\ g \in \overline{G},$$

então $[g_1, g_1^{\psi}] = 1$ para todo $g_1 \in G_1$.

QED.

Definição 6.1.3. *Definem-se os seguintes subgrupos de $T(\overline{G}, Z)$:*

$$D := [G_1, G_1^{\psi}],\ \ L := \langle \{g_1^{-1} g_1^{\psi} : g_1 \in G_1\} \rangle,$$

$$W := D \cap L,\ \ R := [[G_1, L], G_1^{\psi}].$$

Proposição 6.1.4. *Valem as seguintes propriedades:*

1. $D = \{(1, g, 1)Z_1 Z_2 : g \in \overline{G}'\}$;

2. $L = \langle \{(g^{-1}, 1, g)Z_1 Z_2 : g \in \overline{G}\} \rangle$;

3. $R = 1$.

Demonstração.

1. Pela Proposição 6.1.2, $G_1 = \{(g,g,1)Z_1Z_2 : g \in \overline{G}\}$. Logo:

$$D := [G_1, G_1^{\psi}] = \langle \{[(g,g,1),(1,h,h)]Z_1Z_2 : g,h \in \overline{G}\}\rangle =$$

$$\langle \{(1,[g,h],1)Z_1Z_2 : g,h \in \overline{G}\}\rangle = \{(1,g,1)Z_1Z_2 : g \in \overline{G}'\}.$$

2. Como $G_1 = \{(g,g,1)Z_1Z_2 : g \in \overline{G}\}$, então:

$$L := \langle \{g_1^{-1}g_1^{\psi} : g_1 \in G_1\}\rangle = \langle \{(g,g,1)^{-1}(1,g,g)Z_1Z_2 : g \in T(\overline{G},Z)\}\rangle =$$

$$\langle \{(g^{-1},g^{-1},1)(1,g,g)Z_1Z_2 : g \in T(\overline{G},Z)\}\rangle = \langle \{(g^{-1},1,g)Z_1Z_2 : g \in \overline{G}\}\rangle.$$

3. Pelo item 2, $L \subseteq \{(g_1,1,g_2))Z_1Z_2 : g_1,g_2 \in \overline{G}\}$. Logo:

$$\begin{aligned}[G_1,L] &= \langle \{[(g,g,1)(g_1,1,g_2)]Z_1Z_2 : g,g_1,g_2 \in \overline{G}\}\rangle \\ &= \langle \{([g,g_1],1,1)Z_1Z_2 : g,g_1 \in \overline{G}\}\rangle.\end{aligned}$$

Portanto, $[G_1,L] \subseteq \{(g,1,1)Z_1Z_2 : g \in \overline{G}\}$. Logo:

$$R := [[G_1,L],G_1^{\psi}] = \langle \{[(g,1,1),(1,h,h)]Z_1Z_2 : g,h \in \overline{G}\}\rangle = 1.$$

QED.

Lema 6.1.5. *$L \lhd T(\overline{G},Z)$ e $T(\overline{G},Z) = LG_1 = LG_1^{\psi}$.*

Demonstração. Primeiramente:

$$yx^{-1}x^{\psi}y^{-1} = yx^{-1}x^{\psi}y^{-\psi}y^{\psi}y^{-1} \ \forall\ x,y \in G_1;$$

$$yx^{-1}x^{\psi}y^{-1} = ((xy^{-1})^{-1}(xy^{-1})^{\psi})(yy^{-\psi})^{-1} \in L \ \forall\ x,y \in G_1. \ (1)$$

Além disso:

$$y^{\psi}x^{-1}x^{\psi}y^{-\psi} = y^{\psi}y^{-1}yx^{-1}x^{\psi}y^{-\psi} \ \forall\ x,y \in G_1;$$

$$y^{\psi}x^{-1}x^{\psi}y^{-\psi} = (yy^{-\psi})^{-1}((xy^{-1})^{-1}(xy^{-1})^{\psi}) \in L \ \forall \ x, y \in G_1. \ (2)$$

Como $T(\overline{G}, Z) = \langle G_1, G_1^{\psi} \rangle$ e $L := \langle \{g_1^{-1}g_1^{\psi} : g_1 \in G_1\} \rangle$, então, por (1) e (2), segue que:

$$L \lhd T(\overline{G}, Z).$$

Como $G_1 \leq T(\overline{G}, Z)$ e $L \lhd T(\overline{G}, Z)$, então $LG_1 \leq T(\overline{G}, Z)$. Como $g^{\psi} = (gg^{-\psi})^{-1}g$ para todo $g \in G_1$, então $G_1 \cup G_1^{\psi} \subseteq LG_1$. Como $G_1 \cup G_1^{\psi} \subseteq LG_1$, $T(\overline{G}, Z)$ é gerado por $G_1 \cup G_1^{\psi}$ e $L \lhd T(\overline{G}, Z)$, então $T(\overline{G}, Z) = LG_1$. Como $g = (gg^{-\psi})g^{\psi}$ para todo $g \in G_1$ e $T(\overline{G}, Z) = LG_1$, então $T(\overline{G}, Z) = LG_1^{\psi}$. *QED.*

Lema 6.1.6. *$L(G) \lhd \mathscr{X}(G)$ e $\mathscr{X}(G) = L(G)G = L(G)G^{\psi}$.*

Demonstração. A demonstração é análoga à do Lema 6.1.5. *QED.*

Proposição 6.1.7. *Sejam $\alpha : T(\overline{G}, Z) \to G \times G$ dada por $(g_1, g_2, g_3)Z_1Z_2 \mapsto (g_1Z, g_3Z)$ e $\beta : T(\overline{G}, Z) \to G$ dada por $(g_1, g_2, g_3)Z_1Z_2 \mapsto g_2Z$. Então:*

1. *α e β estão bem definidas;*
2. *α e β são homomorfismos sobrejetivos;*
3. *$ker(\alpha) = D$;*
4. *$ker(\beta) = L$.*

Em particular, D, L e W são subgrupos normais de $T(\overline{G}, Z)$.

Demonstração.

1. Suponha que $(g_1, g_2, g_3)Z_1Z_2 = (g_1', g_2', g_3')Z_1Z_2$. Como $Z_1Z_2 \subseteq Z \times Z \times Z$, então $g_iZ = g_i'Z$ para todo $i \in \{1, 2, 3\}$, logo α e β estão bem definidas.
2. Por definição, α e β são homomorfismos. Como $G \simeq \overline{G}/Z$ e $(g, g, 1)Z_1Z_2 \in T(\overline{G}, Z)$, $(1, g, g)Z_1Z_2 \in T(\overline{G}, Z)$ para todo $g \in \overline{G}$, então α e β são sobrejetivas.

3. Pelo item 1 da Proposição 6.1.4, segue que $D \subseteq ker(\alpha)$. Seja $v \in ker(\alpha)$. Pelos itens 1 e 2 da Proposição 6.1.2, existem $n \in \mathbb{N}$ e $g_1, ..., g_n, h_1, ..., h_n \in \overline{G}$ tais que:

$$v = \prod_{i=1}^{n}(g_i, g_i, 1)(1, h_i, h_i)Z_1Z_2 = \left(\prod_{i=1}^{n} g_i, \prod_{i=1}^{n} g_ih_i, \prod_{i=1}^{n} h_i\right) Z_1Z_2.$$

   Como $v \in ker(\alpha)$, então $\prod_{i=1}^{n} g_i \in Z$ e $\prod_{i=1}^{n} h_i \in Z$, logo

$$\prod_{i=1}^{n}(g_i, g_i, 1)\prod_{i=1}^{n}(1, h_i, h_i)Z_1Z_2 = Z_1Z_2.$$

   Pelo Lema 1.1.8, existe $c \in D = [G_1, G_1^{\psi}]$ tal que

$$v = c\left(\prod_{i=1}^{n}(g_i, g_i, 1)\prod_{i=1}^{n}(1, h_i, h_i)Z_1Z_2\right) = c.$$

   Assim, $ker(\alpha) \subseteq D$, logo $ker(\alpha) = D$.

4. Pelo item 2 da Proposição 6.1.4, segue que $L \subseteq ker(\beta)$. Seja $v \in ker(\beta)$. Pelo Lema 6.1.5, existem $\ell \in L$ e $g \in G_1$ tais que $v = \ell g$. Como $L \subseteq ker(\beta)$, $\ell \in L$, $v = \ell g$ e $v \in \ker(\beta)$, então $\beta(g) = \beta(v) = 1_G$. Como $\beta(g) = 1_G$ e $g \in G_1$, então $g = 1_{T(\overline{G},Z)}$, logo $v = \ell \in L$. Assim, $ker(\beta) \subseteq L$, logo $ker(\beta) = L$.

QED.

Proposição 6.1.8. $W = \{(1, z, 1)Z_1Z_2 : z \in Z\} \simeq Z$.

Demonstração. Seja $w \in W = D \cap L$. Pela Proposição 6.1.4, existem $g \in \overline{G}'$ e $u, v \in \overline{G}$ tais que $w = (1, g, 1)Z_1Z_2 = (u, 1, v)Z_1Z_2$. Assim, existem $z_1, z_2 \in Z$ tais que:

$$(1, g, 1) = (u, 1, v)(z_1, z_1, 1)(1, z_2, z_2) = (uz_1, z_1z_2, vz_2).$$

Em particular, $g = z_1z_2 \in Z$. Como $w = (1, g, 1)Z_1Z_2$ e $g \in Z$, então:

$$w \in \{(1, z, 1)Z_1Z_2 : z \in Z\}.$$

Portanto:

$$W \subseteq \{(1, z, 1)Z_1Z_2 : z \in Z\}.$$

Sejam α e β conforme definidas na Proposição 6.1.7. Por definição:

$$\{(1, z, 1)Z_1Z_2 : z \in Z\} \subseteq ker(\alpha) = D, \ \{(1, z, 1)Z_1Z_2 : z \in Z\} \subseteq ker(\beta) = L.$$

Logo, $\{(1, z, 1)Z_1Z_2 : z \in Z\} \subseteq D \cap L = W$. Portanto:

$$W = \{(1, z, 1)Z_1Z_2 : z \in Z\}.$$

Seja $\phi : Z \to \{(1, z, 1)Z_1Z_2 : z \in Z\}$ dada por:

$$z \mapsto (1, z, 1)Z_1Z_2.$$

Por definição, ϕ é um homomorfismo sobrejetivo. Seja $z \in ker(\phi)$. Assim, $(1, z, 1) \in Z_1Z_2$, logo existem $z_1, z_2 \in Z$ tais que $(1, z, 1) = (z_1, z_1, 1)(1, z_2, z_2) = (z_1, z_1z_2, z_2)$, o que implica que $z_1 = z_2 = 1$ e $z = z_1z_2 = 1$. Portanto, $ker(\phi) = 1$. Como ϕ é um homomorfismo sobrejetivo e $ker(\phi) = 1$, então ϕ é um isomorfismo, logo:

$$W = \{(1, z, 1)Z_1Z_2 : z \in Z\} \simeq Z.$$

QED.

Teorema 6.1.9. *Existe um homomorfismo sobrejetivo* $\lambda : \mathscr{X}(G) \to T(\overline{G}, Z)$ *que satisfaz as seguintes propriedades:*

1. $\lambda(G) = G_1$ *e* $\lambda(G^{\psi}) = G_1^{\psi}$;

2. $R(G) \subseteq ker(\lambda) \subseteq W(G)$;

3. $\lambda(W(G)) = \{(1, z, 1)Z_1Z_2 : z \in Z\} \simeq Z$.

Em particular, se $\overline{G} = G$, *então* $ker(\lambda) = W(G)$.

Demonstração. Pela Proposição 6.1.2, existem isomorfismos $\phi_1 : G \to G_1$ e $\phi_2 : G^\psi \to G_1^\psi$. Como $[g_1, g_1^\psi] = 1$ para todo $g_1 \in G_1$, então, pelo Lema 6.0.3, existe um homomorfismo $\lambda : \mathscr{X}(G) \to T(\overline{G}, Z)$ tal que $\lambda|_G = \phi_1$ e $\lambda|_{G^\psi} = \phi_2$. Como ϕ_1, ϕ_2 são isomorfismos e $T(\overline{G}, Z) = \langle G_1, G_1^\psi \rangle$, então λ é sobrejetivo. Além disso:

$$\lambda(D(G)) = D,\ \lambda(L(G)) = L,\ \lambda(W(G)) = W\ \ \lambda(R(G)) = R.$$

Sejam α, β conforme definidos na Proposição 6.1.7. Sejam $\alpha' := \alpha\lambda$ e $\beta' := \beta\lambda$. Por definição, $\alpha' : \mathscr{X}(G) \to G \times G$ e $\beta' : \mathscr{X}(G) \to G$ são tais que:

$$\alpha'(g) = (g, 1)\ ,\ \alpha'(g^\psi) = (1, g)\ \forall\ g \in G,$$

$$\beta'(g) = g\ ,\ \beta'(g^\psi) = g\ \forall\ g \in G.$$

Analogamente à Proposição 6.1.7 (usando o Lema 6.1.6), demonstra-se que:

$$ker(\alpha') = D(G),\ ker(\beta') = L(G).$$

Portanto:

$$ker(\lambda) \subseteq ker(\alpha\lambda) \cap ker(\beta\lambda) = ker(\alpha') \cap ker(\beta') = D(G) \cap L(G) = W(G).$$

Como $\lambda(R(G)) = R$ e $R = 1$ (pela Proposição 6.1.4), então $R(G) \subseteq ker(\lambda)$. Além disso, como $\lambda(W(G)) = W$ e $W = \{(1, z, 1)Z_1Z_2 : z \in Z\} \simeq Z$ (pela Proposição 6.1.8), então $\lambda(W(G)) = \{(1, z, 1)Z_1Z_2 : z \in Z\} \simeq Z$. Em particular, se $\overline{G} = G$, então $Z = 1$, logo $\lambda(W(G)) = 1$; como $ker(\lambda) \subseteq W(G)$, então $ker(\lambda) = W(G)$. *QED.*

6.2 A estrutura interna de $\mathscr{X}(G)$

Nesta seção, será estudada a estrutura do grupo $\mathscr{X}(G)$.

Proposição 6.2.1. *Valem as seguintes afirmações:*

1. *Existe um homomorfismo sobrejetivo* $\alpha' : \mathscr{X}(G) \to G \times G$ *tal que* $ker(\alpha') = D(G)$ *e* $\alpha'(g) = (g, 1)$ *e* $\alpha'(g^{\psi}) = (1, g)$ *para todo* $g \in G$*;*

2. *Existe um homomorfismo sobrejetivo* $\beta' : \mathscr{X}(G) \to G$ *tal que* $ker(\beta') = L(G)$ *e* $\beta'(g) = g$ *e* $\beta'(g^{\psi}) = g$ *para todo* $g \in G$*;*

3. *Existe um homomorfismo* $\rho : \mathscr{X}(G) \to G \times G \times G$ *tal que* $ker(\rho) = W(G)$*.*

Em particular, $D(G)$*,* $L(G)$ *e* $W(G)$ *são subgrupos normais de* $\mathscr{X}(G)$*.*

Demonstração.

1. Segue da demonstração do Teorema 6.1.9.

2. Segue da demonstração do Teorema 6.1.9.

3. Defina $\rho : \mathscr{X}(G) \to G \times G \times G$ dada por $x \mapsto (\alpha'(x), \beta'(x))$. Portanto:

$$ker(\rho) = ker(\alpha') \cap ker(\beta') = D(G) \cap L(G) = W(G).$$

QED.

Proposição 6.2.2. *Valem as seguintes propriedades:*

1. $\mathscr{X}(G) = L(G)G = L(G)G^{\psi}$*;*

2. $L_1(G) \lhd \mathscr{X}(G)$ *e* $L_2(G) \lhd \mathscr{X}(G)$*;*

3. $L_1(G) \subseteq L(G)$ *e* $L_2(G) \subseteq L(G)$*;*

4. $\mathscr{X}(G) = L(G) \rtimes G = L(G) \rtimes G^{\psi}$*;*

5. $D(G)/W(G) \simeq G'$*.*

Demonstração.

1. Segue do Lema 6.1.6.

2. Pelo item 1, segue que $\mathscr{X}(G) = \langle L(G) \cup G \rangle = \langle L(G) \cup G^{\psi} \rangle$, logo $L_1(G) := [L(G), G]$ e $L_2(G) := [L(G), G^{\psi}]$ são subgrupos normais de $\mathscr{X}(G)$ (pelo Lema 1.1.7).

3. Como $L(G) \lhd \mathscr{X}(G)$, então:

$$[\ell, x] = \ell^{-1}(x^{-1}\ell x) \in L(G) \ \forall\ \ell \in L(G) \ \forall\ x \in \mathscr{X}(G).$$

   Em particular, $L_1(G) \subseteq L(G)$ e $L_2(G) \subseteq L(G)$.

4. Como $L(G) \lhd \mathscr{X}(G)$, $L(G) \cap G = 1$ e $L(G) \cap G^{\psi} = 1$, então, pelo item 1, segue que $\mathscr{X}(G) = L(G) \rtimes G = L(G) \rtimes G^{\psi}$.

5. Seja $\lambda : \mathscr{X}(G) \to T(G, 1)$ conforme definido no Teorema 6.1.9. Como $ker(\lambda) = W(G) \subseteq D(G)$ e $\lambda(D(G)) = D = 1 \times G' \times 1 \simeq G'$ (pela Proposição 6.1.4, pois $Z = 1$), então $D(G)/W(G) \simeq G'$.

QED.

Lema 6.2.3. *Sejam $g_1, g_2, g_3 \in G$. Valem as seguintes relações em $\mathscr{X}(G)$:*

1. $[g_1^{\psi}, g_2] = [g_1, g_2^{\psi}]$;

2. $[g_1, g_3^{\psi}]^{g_2} = [g_1, g_3^{\psi}]^{g_2^{\psi}}$ *e* $[g_1, g_3^{\psi}]^{g_2 g_2^{-\psi}} = [g_1, g_3^{\psi}]$;

3. $[g_1, g_2^{\psi}] = [g_2^{-\psi} g_2, g_1][g_1, g_2]$.

Demonstração.

1. Pelos itens 8 e 9 do Lema 1.1.2, segue que:

$$[g_1 g_2, (g_1 g_2)^{\psi}] = [g_1, (g_1 g_2)^{\psi}]^{g_2}[g_2, (g_1 g_2)^{\psi}] =$$

$$([g_1, g_2^{\psi}][g_1, g_1^{\psi}]^{g_2^{\psi}})^{g_2}([g_2, g_2^{\psi}][g_2, g_1^{\psi}]^{g_2^{\psi}}).$$

   Como $[g, g^{\psi}] = 1$ para todo $g \in G$, então:

$$1 = [g_1, g_2^{\psi}]^{g_2}[g_2, g_1^{\psi}]^{g_2^{\psi}}.$$

Conjugando ambos os lados por $g_2^{-1}g_2^{-\psi} = g_2^{-\psi}g_2^{-1}$, segue que:

$$\begin{aligned}
1 &= [g_1, g_2^{\psi}]^{g_2 \cdot g_2^{-1} g_2^{-\psi}} [g_2, g_1^{\psi}]^{g_2^{\psi} \cdot g_2^{-\psi} g_2^{-1}} \\
&= [g_1, g_2^{\psi}]^{g_2^{-\psi}} [g_2, g_1^{\psi}]^{g_2^{-1}} \\
&= g_2^{\psi}(g_1^{-1} g_2^{-\psi} g_1 g_2^{\psi}) g_2^{-\psi} \cdot g_2 (g_2^{-1} g_1^{-\psi} g_2 g_1^{\psi}) g_2^{-1} \\
&= g_2^{\psi} g_1^{-1} g_2^{-\psi} g_1 \cdot g_1^{-\psi} g_2 g_1^{\psi} g_2^{-1} \\
&= (g_2^{\psi} g_1^{-1} g_2^{-\psi} g_1)(g_2 g_1^{-\psi} g_2^{-1} g_1^{\psi})^{-1} \\
&= [g_2^{-\psi}, g_1][g_2^{-1}, g_1^{\psi}]^{-1}.
\end{aligned}$$

Portanto:

$$[g_2^{-1}, g_1^{\psi}] = [g_2^{-\psi}, g_1].$$

2. Pelo item 8 do Lema 1.1.2 e pelo item 1, segue que:

$$[g_1 g_2, g_3^{\psi}] = [g_1, g_3^{\psi}]^{g_2}[g_2, g_3^{\psi}] = [g_1, g_3^{\psi}]^{g_2}[g_2^{\psi}, g_3], \quad (1)$$

$$[g_1 g_2, g_3^{\psi}] = [(g_1 g_2)^{\psi}, g_3] = [g_1^{\psi}, g_3]^{g_2^{\psi}}[g_2^{\psi}, g_3]. \quad (2)$$

Por (1) e (2), segue que:

$$[g_1, g_3^{\psi}]^{g_2}[g_2^{\psi}, g_3] = [g_1^{\psi}, g_3]^{g_2^{\psi}}[g_2^{\psi}, g_3];$$

$$[g_1, g_3^{\psi}]^{g_2} = [g_1^{\psi}, g_3]^{g_2^{\psi}}.$$

Conjugando ambos os lados da igualdade anterior por $g_2^{-\psi}$, segue que:

$$[g_1, g_3^{\psi}]^{g_2 g_2^{-\psi}} = [g_1^{\psi}, g_3].$$

3. Pelo item 9 do Lema 1.1.2, segue que:

$$[g_1, g_2^{\psi}] = [g_1, g_2(g_2^{-1} g_2^{\psi})] = [g_1, g_2^{-1} g_2^{\psi}][g_1, g_2]^{g_2^{-1} g_2^{\psi}}.$$

Conjugando ambos os lados por $g_2^{-\psi}g_2$, segue que:

$$[g_1, g_2^{\psi}]^{g_2^{-\psi}g_2} = [g_1, g_2^{-1}g_2^{\psi}]^{g_2^{-\psi}g_2}[g_1, g_2].$$

Pelo item 2, segue que $[g_1, g_2^{\psi}]^{g_2^{-\psi}g_2} = [g_1, g_2^{\psi}]$. Logo:

$$[g_1, g_2^{\psi}] = [g_1, g_2^{-1}g_2^{\psi}]^{g_2^{-\psi}g_2}[g_1, g_2].$$

Pelo item 7 do Lema 1.1.2, $[g_1, g_2^{-1}g_2^{\psi}]^{g_2^{-\psi}g_2} = [g_2^{-\psi}g_2, g_1]$. Logo:

$$[g_1, g_2^{\psi}] = [g_2^{-\psi}g_2, g_1][g_1, g_2].$$

QED.

Proposição 6.2.4. *$[D(G), L(G)] = 1$, $W(G) \subseteq Z(D(G))$ e $W(G)$ é abeliano.*

Demonstração. Pelo item 2 do Lema 6.2.3, segue que $[D(G), L(G)] = 1$. Como $[D(G), L(G)] = 1$ e $W(G) = D(G) \cap L(G)$, então $[W(G), D(G)] = 1$, logo $W(G) \subseteq Z(D(G))$. Em particular, $W(G)$ é abeliano. *QED.*

A seguir, será demonstrado o principal resultado deste texto.

Teorema 6.2.5. *Para toda extensão stem $(\overline{G}, Z)$ de G, existe um homomorfismo sobrejetivo $\phi : W(G)/R(G) \to Z$. Em particular, existe um homomorfismo sobrejetivo $\phi : W(G)/R(G) \to M(G)$.*

Demonstração. Pelo Teorema 6.1.9, existe um homomorfismo $\lambda : \mathscr{X}(G) \to T(\overline{G}, Z)$ tal que $R(G) \subseteq ker(\lambda) \subseteq W(G)$ e $\lambda(W(G)) \simeq Z$. Em particular, existe um isomorfismo $\psi : W(G)/ker(\lambda) \to Z$. Como $R(G) \subseteq W(G)$ e $W(G)$ é abeliano (pela Proposição 6.2.4), então $R(G) \lhd W(G)$. Seja $\pi : W(G)/R(G) \to W(G)/ker(\lambda)$ dado por:

$$w \cdot R(G) \mapsto w \cdot ker(\lambda).$$

Como $R(G) \subseteq ker(\lambda)$, então π está bem definida e é um homomorfismo sobrejetivo. Portanto, $\phi = \psi\pi : W(G)/R(G) \to Z$ é um homomorfismo sobrejetivo. Em particular, pelo Teorema 5.3.3, existe um homomorfismo sobrejetivo $\phi : W(G)/R(G) \to M(G)$. *QED.*

Lema 6.2.6. *Valem as seguintes propriedades:*

1. $D(G)^\psi = D(G)$;
2. $L(G)^\psi = L(G)$;
3. $W(G)^\psi = W(G)$;
4. $L_1(G)^\psi = L_2(G)$;
5. $R(G)^\psi = [L_2(G), G] = R(G)$.

Demonstração.

1. Pelo Lema 1.1.6 e pelo item 5 do Lema 1.1.2, segue que:

$$D(G)^\psi = [G, G^\psi]^\psi = [G^\psi, (G^\psi)^\psi] = [G^\psi, G] = [G, G^\psi] = D(G).$$

2.
$$L(G)^\psi = \langle\{g^{-1}g^\psi : g \in G\}\rangle^\psi = \langle\{(g^{-1}g^\psi)^\psi : g \in G\}\rangle =$$
$$\langle\{g^{-\psi}g : g \in G\}\rangle = \langle\{(g^{-1}g^\psi)^{-1} : g \in G\}\rangle = L(G).$$

3. Segue dos itens 1 e 2.

4. Pelo Lema 1.1.6 e pelo item 2, segue que:

$$L_1(G)^\psi = [L(G), G]^\psi = [L(G)^\psi, G^\psi] = [L(G), G^\psi] = L_2(G).$$

5. Pelo Lema 1.1.6 e pelo item 4, segue que:

$$R(G)^\psi = [L_1(G), G^\psi]^\psi = [L_1(G)^\psi, (G^\psi)^\psi] = [L_1(G)^\psi, G] = [L_2(G), G].$$

Como $R(G)^{\psi} = [L_1(G)^{\psi}, G]$, então, pelo item 1 do Lema 6.2.3, segue que:

$$R(G)^{\psi} = [L_1(G)^{\psi}, G] = [L_1(G), G^{\psi}] = R(G).$$

QED.

Proposição 6.2.7. *Valem as seguintes propriedades:*

1. $D(G) \subseteq L_1(G)G'$, $L_1(G) = L(G) \cap (D(G)G')$;

2. $W(G) \subseteq L_1(G)$, $[W(G), G] \subseteq R(G)$;

3. $D(G)L_1(G) = D(G)G'$;

4. $[[G^{\psi}, G'], G'] \subseteq [D(G), G'] \subseteq D(G)'$;

5. $$\frac{[G', G^{\psi}]L_1(G)}{L_1(G)} = \frac{[G', G]L_1(G)}{L_1(G)}, \ \frac{[G', G^{\psi}]L(G)}{L(G)} = \frac{[G', G]L(G)}{L(G)}.$$

Demonstração.

1. Pelo item 3 do Lema 6.2.3, segue que:

$$D(G) \subseteq L_1(G)G', \ \ L_1(G) \subseteq D(G)G'.$$

Como $L_1(G) \subseteq D(G)G'$ e $L_1(G) \subseteq L(G)$ (pelo item 4 da Proposição 6.2.2), então $L_1(G) \subseteq L(G) \cap (D(G)G')$. Seja $x \in L(G) \cap (D(G)G')$. Logo, existem $d \in D(G)$, $g_1 \in G'$ tais que $x = dg_1$. Além disso, como $D(G) \subseteq L_1(G)G'$, existem $\ell \in L_1(G)$, $g_2 \in G'$ tais que $d = \ell g_2$. Portanto, $x = \ell(g_1g_2)$. Como $x \in L(G)$, $\ell \in L_1(G) \subseteq L(G)$, $g_1g_2 \in G'$ e $L(G) \cap G' = 1$, então $x = \ell \in L_1(G)$. Assim, $L(G) \cap (D(G)G') \subseteq L_1(G)$. Logo:

$$L_1(G) = L(G) \cap (D(G)G').$$

2. Como $W(G) = D(G) \cap L(G)$ e $L_1(G) = L(G) \cap (D(G)G')$ (pelo item 1), então:

$$W(G) \subseteq L_1(G).$$

Como $W(G) \subseteq L_1(G)$ e $R(G) = [L_1(G), G^{\psi}]$, então:

$$[W(G), G^{\psi}] \subseteq R(G).$$

Pelo item 1 do Lema 6.2.3 pelo item 3 do Lema 6.2.6, segue que:

$$[W(G), G^{\psi}] = [W(G)^{\psi}, G] = [W(G), G].$$

Portanto:

$$[W(G), G] = [W(G), G^{\psi}] \subseteq R(G).$$

3. Pelo item 3 do Lema 6.2.3, segue que $G' \subseteq L_1(G)D(G)$. Como $G' \subseteq L_1(G)D(G)$ e $L_1(G) \subseteq L(G) \lhd \mathscr{X}(G)$ (pela Proposição 6.2.2), então

$$G' \subseteq L(G)D(G) = D(G)L(G),$$

logo $D(G)G' \subseteq D(G)L(G)$. Como $D(G)L_1(G) = (D(G)L(G)) \cap (D(G)G')$ (pelo item 1) e $D(G)G' \subseteq D(G)L(G)$, então:

$$D(G)L_1(G) = D(G)G'.$$

4. Como $G' \subseteq D(G)L(G)$ e $[D(G), L(G)] = 1$ (pela Proposição 6.2.4), então $[D(G), G'] \subseteq D(G)'$. Como $[G^{\psi}, G'] \subseteq [G^{\psi}, G] = D(G)$, então:

$$[[G^{\psi}, G'], G'] \subseteq [D(G), G'] \subseteq D(G)'.$$

5. Pelo item 3 do Lema 6.2.3, segue que:

$$[h, g^{\psi}] = [g^{-\psi}g, h][h, g] \ \forall \ g \in G \ \forall \ h \in G'.$$

Como $L_1(G) := [L(G), G]$, então $[G', G^{\psi}] \subseteq L_1(G)[G', G]$ e $[G', G] \subseteq L_1(G)[G', G^{\psi}]$. Como $L_1(G) \lhd \mathscr{X}(G)$ (pela Proposição 6.2.2), então:

$$\frac{[G', G^{\psi}]L_1(G)}{L_1(G)} = \frac{[G', G]L_1(G)}{L_1(G)}.$$

Como $L_1(G) \subseteq L(G) \lhd \mathscr{X}(G)$ (pela Proposição 6.2.2), então:

$$\frac{[G', G^{\psi}]L(G)}{L(G)} = \frac{[G', G]L(G)}{L(G)}.$$

QED.

Proposição 6.2.8. *Valem as seguintes propriedades:*

1. $R(G) \lhd \mathscr{X}(G)$;

2. $[g_1^{g_3}, [(g_2^{g_3})^{\psi}, g_3^{-\psi}g_3]] = [g_1, g_2^{\psi}]^{g_3}[g_1^{g_3}, (g_2^{g_3})^{\psi}]^{-1} \ \forall \ g_1, g_2, g_3 \in G$;

3. $[g_1, g_2^{\psi}]^{g_3}R(G) = [g_1^{g_3}, (g_2^{g_3})^{\psi}]R(G) = [g_1, g_2^{\psi}]^{g_3^{\psi}}R(G) \ \forall \ g_1, g_2, g_3 \in G$;

4. $R(G) = \langle [g_1, g_2^{\psi}]^{g_3}[g_1^{g_3}, (g_2^{g_3})^{\psi}]^{-1} : g_1, g_2, g_3 \in G\rangle^{\mathscr{X}(G)}$.

Demonstração.

1. Como $L_1(G) \lhd \mathscr{X}(G)$ e $L_2(G) \lhd \mathscr{X}(G)$ (pela Proposição 6.2.2), então, pelo item 6 do Lema 1.1.2, segue que:

$$[L_1(G), G^{\psi}]^{G^{\psi}} = [L_1(G)^{G^{\psi}}, (G^{\psi})^{G^{\psi}}] = [L_1(G), G^{\psi}], \ (1)$$

$$[G, L_2(G)]^{G} = [G^{G}, L_2(G)^{G}] = [G, L_2(G)]. \ (2)$$

Como $(G^{\psi})^{G} \subseteq D(G)G^{\psi}$ (pelo item 4 do Lema 1.1.2), $L_1(G) \lhd \mathscr{X}(G)$ e $[L_1(G), D(G)] = 1$ (pela Proposição 6.2.2 e pela Proposição 6.2.4), então, pelos itens

6 e 9 do Lema 1.1.2, segue que:

$$[L_1(G), G^{\psi}]^G \subseteq [L_1(G)^G, (G^{\psi})^G] \subseteq [L_1(G), D(G)G^{\psi}] \subseteq$$

$$[L_1(G), G^{\psi}][L_1(G), D(G)]^{G^{\psi}} = [L_1(G), G^{\psi}]. \ (3)$$

Como $G^{G^{\psi}} \subseteq D(G)G$ (pelo item 4 do Lema 1.1.2), $L_2(G) \lhd \mathscr{X}(G)$ e $[L_2(G), D(G)] = 1$ (pela Proposição 6.2.2 e pela Proposição 6.2.4), então, pelos itens 6 e 8 do Lema 1.1.2, segue que:

$$[G, L_2(G)]^{G^{\psi}} \subseteq [G^{G^{\psi}}, L_2(G)^{G^{\psi}}] \subseteq [D(G)G, L_2(G)] \subseteq$$

$$[D(G), L_2(G)]^G[G, L_2(G)] = [G, L_2(G)]. \ (4)$$

Como $\mathscr{X}(G) = \langle G, G^{\psi} \rangle$, então, por (1), (2), (3), (4), segue que:

$$[L_1(G), G^{\psi}] \lhd \mathscr{X}(G) \ , \ [G, L_2(G)] \lhd \mathscr{X}(G).$$

Como $[G, L_2(G)] = [L_2(G), G]$ (pelo item 5 do Lema 1.1.2) e $R(G) = [L_1(G), G] = [L_2(G), G]$ (pelo item 5 do Lema 6.2.6), então:

$$R(G) \lhd \mathscr{X}(G).$$

2. Sejam $g_1, g_2, g_3 \in G$. Pelo item 6 do Lema 1.1.2, segue que:

$$\begin{aligned}
[g_1, g_2^{\psi}]^{g_3} &= [g_1^{g_3}, (g_2^{\psi})^{g_3}] \\
&= [g_1^{g_3}, (g_2^{\psi})^{g_3^{\psi}(g_3^{-\psi} g_3)}] \\
&= [g_1^{g_3}, ((g_2^{\psi})^{g_3^{\psi}})^{g_3^{-\psi} g_3}] \\
&= [g_1^{g_3}, (g_2^{\psi})^{g_3^{\psi}}[(g_2^{\psi})^{g_3^{\psi}}, g_3^{-\psi} g_3]].
\end{aligned}$$

Pelo item 9 do Lema 1.1.2, segue que:

$$[g_1, g_2^{\psi}]^{g_3} = [g_1^{g_3}, [(g_2^{\psi})^{g_3^{\psi}}, g_3^{-\psi} g_3]][g_1^{g_3}, (g_2^{\psi})^{g_3^{\psi}}]^{[(g_2^{\psi})^{g_3^{\psi}}, g_3^{-\psi} g_3]}.$$

Como $[D(G), L(G)] = 1$ (pela Proposição 6.2.4), $[g_1^{g_3}, (g_2^{\psi})^{g_3^{\psi}}] \in D(G)$ e $[(g_2^{\psi})^{g_3^{\psi}}, g_3^{-\psi} g_3] \in L_2(G) \subseteq L(G)$ (pela Proposição 6.2.2), então $[g_1^{g_3}, (g_2^{\psi})^{g_3^{\psi}}]^{[(g_2^{\psi})^{g_3^{\psi}}, g_3^{-\psi} g_3]} = [g_1^{g_3}, (g_2^{\psi})^{g_3^{\psi}}]$. Logo:

$$[g_1, g_2^{\psi}]^{g_3} = [g_1^{g_3}, [(g_2^{\psi})^{g_3^{\psi}}, g_3^{-\psi} g_3]][g_1^{g_3}, (g_2^{\psi})^{g_3^{\psi}}];$$

$$[g_1^{g_3}, [(g_2^{\psi})^{g_3^{\psi}}, g_3^{-\psi} g_3]] = [g_1, g_2^{\psi}]^{g_3}[g_1^{g_3}, (g_2^{\psi})^{g_3^{\psi}}]^{-1}.$$

Como $(g_2^{\psi})^{g_3^{\psi}} = (g_2^{g_3})^{\psi}$, então:

$$[g_1^{g_3}, [(g_2^{g_3})^{\psi}, g_3^{-\psi} g_3]] = [g_1, g_2^{\psi}]^{g_3}[g_1^{g_3}, (g_2^{g_3})^{\psi}]^{-1}.$$

3. Sejam $g_1, g_2, g_3 \in G$. Como $[g_1^{g_3}, [(g_2^{\psi})^{g_3^{\psi}}, g_3^{-\psi} g_3]] \in [G, L_2(G)] = R(G)$ (pelo item 1) e $[g_1^{g_3}, [(g_2^{g_3})^{\psi}, g_3^{-\psi} g_3]] = [g_1, g_2^{\psi}]^{g_3}[g_1^{g_3}, (g_2^{g_3})^{\psi}]^{-1}$ (pelo item 2), então:

$$[g_1, g_2^{\psi}]^{g_3} R(G) = [g_1^{g_3}, (g_2^{g_3})^{\psi}] R(G).$$

Como $[g_1, g_2^{\psi}]^{g_3} = [g_1, g_2^{\psi}]^{g_3^{\psi}}$ (pelo item 2 do Lema 6.2.3), segue que:

$$[g_1, g_2^{\psi}]^{g_3} R(G) = [g_1^{g_3}, (g_2^{g_3})^{\psi}] R(G) = [g_1, g_2^{\psi}]^{g_3^{\psi}} R(G).$$

4. Como $R(G) = [G, L_2(G)] = [G, [G^{\psi}, L(G)]] \lhd \mathscr{X}(G)$ (pelo item 1) e $L(G) := \langle g^{-\psi} g : g \in G \rangle$, então, aplicando repetidamente os itens 8 e 9 do Lema 1.1.2, segue que:

$$R(G) = \langle [x_1, [x_2^{\psi}, x_3^{-\psi} x_3]] : x_1, x_2, x_3 \in G \rangle^{\mathscr{X}(G)}.$$

Como o mapa $c_y : G \to G$ dado por $x \mapsto x^y$ é uma bijeção para todo $y \in G$, então:

$$R(G) = \langle [g_1^{g_3}, [(g_2^{g_3})^{\psi}, g_3^{-\psi} g_3]] : g_1, g_2, g_3 \in G \rangle^{\mathscr{X}(G)}.$$

Pelo item 2, segue que:

$$R(G) = \langle [g_1, g_2^{\psi}]^{g_3} [g_1^{g_3}, (g_2^{g_3})^{\psi}]^{-1} : g_1, g_2, g_3 \in G \rangle^{\mathscr{X}(G)}.$$

QED.

Lema 6.2.9. *Sejam $x, y \in G$ tais que $[x, y] = 1$. Então, $[x, y^{\psi}] \in W(G)$ e, para todo $n \in \mathbb{N}$, $[x^n, y^{\psi}] = [x, y^{\psi}]^n$. Além disso, se $|x|, |y| < \infty$, então $|[x, y^{\psi}]| \mid MDC(|x|, |y|)$. Em particular, se $MDC(|x|, |y|) = 1$, então $[x, y^{\psi}] = 1$.*

Demonstração. Como $[x, y] = 1$, então, pelo item 3 do Lema 6.2.3, segue que:

$$[x, y^{\psi}] = [y^{-\psi} y, x] \subseteq [L(G), G] = L_1(G).$$

Como $L_1(G) \subseteq L(G)$ (pela Proposição 6.2.2), então $[x, y^{\psi}] \in L(G)$. Como $[x, y^{\psi}] \in L(G)$ e $[x, y^{\psi}] \in D(G)$, então:

$$[x, y^{\psi}] \in W(G).$$

Como $[x, y] = 1$ e $[g, g^{\psi}] = 1 \ \forall \ g \in G$, então $x^{-\psi} x^{-1} y^{-\psi} = x^{-1} y^{-\psi} x^{-\psi}$ e $x y^{\psi} x^{\psi} = x^{\psi} x y^{\psi}$. Logo:

$$[x, y^{\psi}]^{x^{\psi}} = x^{-\psi} x^{-1} y^{-\psi} x y^{\psi} x^{\psi} = x^{-1} y^{-\psi} x^{-\psi} x^{\psi} x y^{\psi} = x^{-1} y^{-\psi} x y^{\psi} = [x, y^{\psi}]. \ (*)$$

Suponha, por hipótese indutiva, que $[x^n, y^{\psi}] = [x, y^{\psi}]^n$ para algum $n \in \mathbb{N}$. Pelo item 8 do Lema 1.1.2, segue que $[x^n x, y^{\psi}] = [x^n, y^{\psi}]^x [x, y^{\psi}]$, e, pelo item 2 do Lema 6.2.3, segue que

$[x^n, y^\psi]^x = [x^n, y^\psi]^{x^\psi}$. Logo, pelo item 8 do Lema 1.1.2, segue que:

$$\begin{aligned}
[x^{n+1}, y^\psi] &= [x^n x, y^\psi] \\
&= [x^n, y^\psi]^x [x, y^\psi] \\
&= [x^n, y^\psi]^{x^\psi} [x, y^\psi] \\
&= ([x, y^\psi]^n)^{x^\psi} [x, y^\psi] \\
&= ([x, y^\psi]^{x^\psi})^n [x, y^\psi] \\
&= ([x, y^\psi])^n [x, y^\psi] \ (por\ (*)) \\
&= ([x, y^\psi])^{n+1}.
\end{aligned}$$

Como $[x^0, y^\psi] = [x, y^\psi]^0 = 1$, então, por indução, segue que $[x^n, y^\psi] = [x, y^\psi]^n$ para todo $n \in \mathbb{N}$. Pelo item 1 do Lema 6.2.3 e pelo item 5 do Lema 1.1.2, segue que:

$$[x, (y^n)^\psi] = [x^\psi, y^n] = [y^n, x^\psi]^{-1} = [y, x^\psi]^{-n} \ \forall \ n \in \mathbb{N}.$$

Suponha que $|x|, |y| < \infty$. Como $[x^n, y^\psi] = [x, y^\psi]^n$ e $[x, (y^n)^\psi] = [y, x^\psi]^{-n}$ para todo $n \in \mathbb{N}$, então $[x, y^\psi]^{|x|} = [x, y^\psi]^{|y|} = 1$, logo $|[x, y^\psi]| \mid MDC(|x|, |y|)$. *QED.*

Proposição 6.2.10. *Sejam $H, K \lhd G$ tais que $G \simeq H \times K$. Então:*

1. $[H, K^\psi] \lhd \mathscr{X}(G)$, $[H, K^\psi] \subseteq W(G)$;
2. $\mathscr{X}(G) = [H, K^\psi]\langle H, H^\psi\rangle\langle K, K^\psi\rangle$;
3. $\mathscr{X}(G)/[H, K^\psi] \simeq \mathscr{X}(H) \times \mathscr{X}(K)$, $\mathscr{X}(H) \simeq \langle H, H^\psi\rangle$, $\mathscr{X}(K) \simeq \langle K, K^\psi\rangle$, $W(G) \simeq [H, K^\psi] \times W(H) \times W(K)$;
4. *Se* $MDC(|H|, |K|) = 1$, *então* $[H, K^\psi] = 1$, $\mathscr{X}(G) \simeq \mathscr{X}(H) \times \mathscr{X}(K)$, $W(G) \simeq W(H) \times W(K)$.

Demonstração.

1. Pelo Lema 1.1.2, segue que:

$$[h_1h_2, k^\psi] = [h_1, k^\psi]^{h_2}[h_2, k^\psi] \ \forall \ h_1, h_2 \in H \ \forall \ k \in K;$$

$$[h_1, k^\psi]^{h_2} = [h_1h_2, k^\psi][h_2, k^\psi]^{-1} \in [H, K^\psi] \ \forall \ h_1, h_2 \in H \ \forall \ k \in K.$$

Portanto, $[H, K^\psi]^H = [H, K^\psi]$. Além disso:

$$[h, k_1^\psi k_2^\psi] = [h, k_2^\psi][h, k_1^\psi]^{k_2^\psi} \ \forall \ h \in H \ \forall \ k_1, k_2 \in K;$$

$$[h, k_1^\psi]^{k_2^\psi} = [h, k_2^\psi]^{-1}[h, k_1^\psi k_2^\psi] \in [H, K^\psi] \ \forall \ h \in H \ \forall \ k_1, k_2 \in K.$$

Portanto, $[H, K^\psi]^{K^\psi} = [H, K^\psi]$. Pelo Lema 6.2.3, segue que:

$$[H, K^\psi]^H = [H, K^\psi]^{H^\psi}, \ [H, K^\psi]^K = [H, K^\psi]^{K^\psi}.$$

Como $\mathscr{X}(G) = \langle H \cup H^\psi \cup K \cup K^\psi \rangle$ e $[H, K^\psi]^X = [H, K^\psi]$ para todo $X \in \{H, H^\psi, K, K^\psi\}$, então $[H, K^\psi] \lhd \mathscr{X}(G)$. Além disso, como $[H, K] = 1$ (pois $G \simeq H \times K$), então $[H, K^\psi] \subseteq W(G)$ (pelo Lema 6.2.9).

2. Seja $g \in \mathscr{X}(G)$. Como $H, K \lhd G$ e $G \simeq H \times K$, então existem $h_1, ..., h_n \in H$, $k_1, ..., k_n \in K$, $x_1, ..., x_n \in H^\psi$, $y_1, ..., y_n \in K^\psi$ tais que $g = h_1k_1x_1y_1...h_nk_nx_ny_n$. Pelo Lema 1.1.8, existe $u \in [H \cup H^\psi, K \cup K^\psi]$ tal que $g = uh_1x_1...h_nx_nk_1y_1...k_ny_n$. Portanto:

$$\mathscr{X}(G) = [H \cup H^\psi, K \cup K^\psi]\langle H, H^\psi \rangle \langle K, K^\psi \rangle.$$

Pelo Lema 1.1.2, cada elemento de $[H \cup H^\psi, K \cup K^\psi]$ é da forma $g_1^{z_1}...g_m^{z_m}$, em que $z_1, ..., z_m \in \mathscr{X}(G)$ e $g_1, ..., g_m$ são elementos da forma $[h, k], [h, k^\psi], [h^\psi, k], [h^\psi, k^\psi]$, em que $h \in H, k \in K$. Como $[h, k^\psi] = [h^\psi, k]$ (pelo Lema 6.2.3) e $[H, K] = [H^\psi, K^\psi] = 1$ (pois $H, K \lhd G$ e $G \simeq H \times K$), então $g_1, ..., g_m \in [H, K^\psi]$. Como $[H, K^\psi] \lhd \mathscr{X}(G)$, então $g_1^{z_1}...g_m^{z_m} \in [H, K^\psi]$. Assim:

$$[H \cup H^\psi, K \cup K^\psi] = [H, K^\psi].$$

Logo:

$$\mathscr{X}(G) = [H, K^{\psi}]\langle H, H^{\psi}\rangle\langle K, K^{\psi}\rangle.$$

3. Pelo Lema 6.0.3, existe um homomorfismo sobrejetivo $\phi : \mathscr{X}(G) \to \mathscr{X}(H) \times \mathscr{X}(K)$ tal que:

$$\phi(h) = (h, 1), \phi(h^{\psi}) = (h^{\psi}, 1), \phi(k) = (1, k), \phi(k^{\psi}) = (1, k^{\psi}) \ \forall \ h \in H \ \forall \ k \in K.$$

Como $\phi(g) = (g, 1)$ para todo $g \in \langle H, H^{\psi}\rangle$, $\phi(g) = (1, g)$ para todo $g \in \langle K, K^{\psi}\rangle$ e $\phi([h, k^{\psi}]) = 1$ para todo $h \in H$ e para todo $k \in K$, então, pelo item 2,
$ker(\phi) = [H, K^{\psi}]$. Como ϕ é sobrejetivo, então:

$$\mathscr{X}(G)/[H, K^{\psi}] \simeq \mathscr{X}(H) \times \mathscr{X}(K).$$

Além disso, como $ker(\phi) \cap \langle H, H^{\psi}\rangle = ker(\phi) \cap \langle K, K^{\psi}\rangle = 1$, então:

$$\mathscr{X}(H) \simeq \langle H, H^{\psi}\rangle \ , \ \mathscr{X}(K) \simeq \langle K, K^{\psi}\rangle.$$

Como $[H, K^{\psi}]$, $\langle H, H^{\psi}\rangle \cap W(G)$ e $\langle K, K^{\psi}\rangle \cap W(G)$ são subgrupos 2 a 2 disjuntos de $W(G)$ (pois $G \simeq H \times K$), $\mathscr{X}(G) = [H, K^{\psi}]\langle H, H^{\psi}\rangle\langle K, K^{\psi}\rangle$,
$\langle H, H^{\psi}\rangle \cap W(G) \simeq W(H)$ e $\langle K, K^{\psi}\rangle \cap W(G) \simeq W(K)$ (via ϕ) e $W(G)$ é abeliano (pela Proposição 6.2.4), então:

$$W(G) \simeq [H, K^{\psi}] \times W(H) \times W(K).$$

4. Suponha que $MDC(|H|, |K|) = 1$. Pelo Lema 6.2.9, segue que $[H, K^{\psi}] = 1$. Assim, pelo item 3, segue que:

$$\mathscr{X}(G) \simeq \mathscr{X}(H) \times \mathscr{X}(K) \ , \ W(G) \simeq W(H) \times W(K).$$

QED.

Proposição 6.2.11. *Seja K um subgrupo de G. Então:*

1. $[K^{\psi}, G] = [K, G^{\psi}] \lhd \mathscr{X}(G)$;

2. $\langle K, K^{\psi}\rangle \cap D(G) = [K^{\psi}, G]$;

3. *Se* $K \lhd G$, *então* $\langle K, K^{\psi}\rangle^{\mathscr{X}(G)} = \langle K, K^{\psi}\rangle[K^{\psi}, G]$;

4. *Se* $K \lhd G$, *então* $\langle K, K^{\psi}\rangle^{\mathscr{X}(G)} \cap D(G) = [K^{\psi}, G]$.

Em particular, $\langle G', (G')^{\psi}\rangle^{\mathscr{X}(G)} \cap D(G) = [G', G^{\psi}]$.

Demonstração.

1. Pelo item 1 do Lema 6.2.3, $[K^{\psi}, G] = [K, G^{\psi}]$. Pelo Lema 1.1.7, $[K^{\psi}, G] \lhd \langle K^{\psi}, G\rangle$ e $[K, G^{\psi}] \lhd \langle K, G^{\psi}\rangle$. Portanto, $[K^{\psi}, G]^{G} = [K^{\psi}, G]$ e $[K^{\psi}, G]^{G^{\psi}} = [K^{\psi}, G]$. Como $\mathscr{X}(G) = \langle G, G^{\psi}\rangle$, então $[K^{\psi}, G] \lhd \mathscr{X}(G)$.

2. Seja $\alpha' : \mathscr{X}(G) \to G \times G$ o homomorfismo sobrejetivo definido na Proposição 6.2.1. Como $\alpha'(g) = (g, 1)$ e $\alpha'(g^{\psi}) = (1, g)$ para todo $g \in G$, e $ker(\alpha') = D(G)$, então α' induz um homomorfismo sobrejetivo $\pi : \langle K, K^{\psi}\rangle/(\langle K, K^{\psi}\rangle \cap D(G)) \to K \times K$ tal que $\pi(k(\langle K, K^{\psi}\rangle \cap D(G))) = (k, 1)$ e $\pi(k^{\psi}(\langle K, K^{\psi}\rangle \cap D(G))) = (1, k)$ para todo $k \in K$. Além disso, seja $\phi : K \times K \to \langle K, K^{\psi}\rangle/[K, K^{\psi}]$ o homomorfismo sobrejetivo tal que $\phi(k_1, k_2) = k_1 k_2^{\psi}[K, K^{\psi}]$ para todo $k_1, k_2 \in K$. Assim, $\phi\pi : \langle K, K^{\psi}\rangle/(\langle K, K^{\psi}\rangle \cap D(G)) \to \langle K, K^{\psi}\rangle/[K, K^{\psi}]$ é um homomorfismo sobrejetivo tal que $(\phi\pi)(k(\langle K, K^{\psi}\rangle \cap D(G))) = k[K, K^{\psi}]$ para todo $k \in K$. Portanto, $\langle K, K^{\psi}\rangle \cap D(G) \subseteq [K, K^{\psi}]$. Como $[K, K^{\psi}] \subseteq \langle K, K^{\psi}\rangle \cap D(G)$ (por definição), então:

$$\langle K, K^{\psi}\rangle \cap D(G) = [K^{\psi}, G].$$

3. Suponha que $K \lhd G$. Logo, $\langle K, K^{\psi}\rangle^{G} = \langle K, (K^{\psi})^{G}\rangle$. Como

$$g^{-1}k^{\psi}g = [g, k^{-\psi}]k^{\psi} \ \forall\ g \in G\ \forall\ k \in K,$$

então $(K^\psi)^G = \langle [K^\psi, G], K^\psi \rangle$, logo $\langle K, (K^\psi)^G \rangle = \langle K, [K^\psi, G], K^\psi \rangle$. Pelo item 1, $[K^\psi, G] \lhd \mathscr{X}(G)$, logo $\langle K, [K^\psi, G], K^\psi \rangle = \langle K, K^\psi \rangle [K^\psi, G]$. Portanto, $\langle K, K^\psi \rangle^G = \langle K, K^\psi \rangle [K^\psi, G]$. Analogamente, $\langle K, K^\psi \rangle^{G^\psi} = \langle K, K^\psi \rangle [K, G^\psi]$. Pelo Lema 6.2.3, $[K, G^\psi] = [K^\psi, G]$, logo:

$$\langle K, K^\psi \rangle^{G^\psi} = \langle K, K^\psi \rangle^G = \langle K, K^\psi \rangle [K^\psi, G].$$

Como $\mathscr{X}(G) = \langle G, G^\psi \rangle$ e $[K^\psi, G] \lhd \mathscr{X}(G)$, então $\langle K, K^\psi \rangle^{\mathscr{X}(G)} = \langle K, K^\psi \rangle [K^\psi, G]$.

4. Segue dos itens 2 e 3.

QED.

Proposição 6.2.12. *Seja $\phi : G \to K$ um homomorfismo sobrejetivo. Então, existe um homomorfismo sobrejetivo $\overline{\phi} : \mathscr{X}(G) \to \mathscr{X}(K)$ tal que:*

1. $\overline{\phi}(g) = \phi(g)\ \forall\ g \in G$, $\overline{\phi}(g^\psi) = (\phi(g))^\psi\ \forall\ g \in G$, $\overline{\phi}(D(G)) = D(K)$;
2. $ker(\overline{\phi}) = \langle ker(\phi), ker(\phi)^\psi \rangle^{\mathscr{X}(G)}$;
3. $ker(\overline{\phi}) \cap D(G) = [ker(\phi), G^\psi]$.

Demonstração.

1. Como ϕ é um homomorfismo sobrejetivo, então existe um homomorfismo sobrejetivo $\overline{\phi} : \mathscr{X}(G) \to \mathscr{X}(K)$ tal que $\overline{\phi}(g) = \phi(g)$ e $\overline{\phi}(g^\psi) = (\phi(g))^\psi$ para todo $g \in G$ (pelo Lema 6.0.3). Logo:
$$\overline{\phi}(D(G)) = D(K).$$

2. Seja $N := \langle ker(\phi), ker(\phi)^\psi \rangle^{\mathscr{X}(G)}$. Por definição, $\langle ker(\phi), ker(\phi)^\psi \rangle \subseteq ker(\overline{\phi})$, logo $N \subseteq ker(\overline{\phi})$ (pelo Lema 1.1.4). Assim, existe um homomorfismo sobrejetivo $\pi : \mathscr{X}(G)/N \to \mathscr{X}(K)$ tal que $\pi(gN) = \overline{\phi}(g)$ e $\pi(g^\psi N) = (\overline{\phi}(g))^\psi$ para todo $g \in G$. Pela Proposição 6.2.11, $N = \langle ker(\phi), ker(\phi)^\psi \rangle [ker(\phi)^\psi, G]$. Assim, existe um homomorfismo sobrejetivo $\xi : \mathscr{X}(K) \to \mathscr{X}(G)/N$ tal que $\xi(k) = \overline{\phi}^{-1}(k)N$ e $\xi(k^\psi) = \overline{\phi}^{-1}(k^\psi)N$ para todo $k \in K$ (pelo Lema 6.0.3). Como $\xi\pi = 1_{\mathscr{X}(K)}$ e

π é sobrejetivo, então π é um isomorfismo. Como $\overline{\phi} : \mathscr{X}(G) \to \mathscr{X}(K)$ é um homomorfismo sobrejetivo, $N \subseteq ker(\overline{\phi})$ e $\pi : \mathscr{X}(G)/N \to \mathscr{X}(K)$ é um isomorfismo, então:

$$ker(\overline{\phi}) = N.$$

3. Como $[ker(\phi), G^{\psi}] \subseteq D(G) \cap ker(\overline{\phi})$ e $ker(\overline{\phi}) = N$, então:

$$D(G) \cap ker(\overline{\phi}) = (D(G) \cap \langle ker(\phi), ker(\phi)^{\psi} \rangle)[ker(\phi), G^{\psi}].$$

Como $D(G) \cap \langle ker(\phi), ker(\phi)^{\psi} \rangle = [ker(\phi)^{\psi}, G]$ (pela Proposição 6.2.11) e $[ker(\phi), G^{\psi}] = [ker(\phi)^{\psi}, G]$ (pelo Lema 6.2.3), então:

$$ker(\overline{\phi}) \cap D(G) = [ker(\phi), G^{\psi}].$$

QED.

Corolário 6.2.13.

$$D(G/G') \simeq \frac{D(G)\langle G', (G')^{\psi} \rangle^{\mathscr{X}(G)}}{\langle G', (G')^{\psi} \rangle^{\mathscr{X}(G)}}$$

Demonstração. Seja $\phi : G \to G/G'$ dada por $g \mapsto gG'$. Pela Proposição 6.2.12, $\overline{\phi}(D(G)) = D(G/G')$ e $ker(\overline{\phi}) \cap D(G) = [G', G^{\psi}]$. Portanto:

$$D(G/G') \simeq \frac{D(G)}{[G', G^{\psi}]}.$$

Pela Proposição 6.2.11, $\langle G', (G')^{\psi} \rangle^{\mathscr{X}(G)} \cap D(G) = [(G')^{\psi}, G]$. Portanto:

$$D(G/G') \simeq \frac{D(G)}{\langle G', (G')^{\psi} \rangle^{\mathscr{X}(G)} \cap D(G)} \simeq \frac{D(G)\langle G', (G')^{\psi} \rangle^{\mathscr{X}(G)}}{\langle G', (G')^{\psi} \rangle^{\mathscr{X}(G)}}.$$

QED.

6.3 Grupos abelianos

Nesta seção, serão estudadas propriedades de $\mathscr{X}(G)$ no caso em que G é um grupo abeliano.

Proposição 6.3.1. *Suponha que G é abeliano. Então:*

1. $D(G) = W(G) = [L(G), G]$, $D(G) \subseteq Z(L(G))$;

2. $R(G) = [D(G), G] = [D(G), G^{\psi}]$;

3. $L(G)' \subseteq D(G)$, $[L(G)', L(G)] = 1$.

Demonstração.

1. Sejam $g, h \in G$. Como G é abeliano, então:

$$\begin{aligned} [g, h^{\psi}] &= g^{-1}h^{-\psi}gh^{\psi} \\ &= g^{-1}h^{-\psi}ghh^{-1}h^{\psi} \\ &= g^{-1}(h^{-\psi}h)g(h^{-1}h^{\psi}) \\ &= (h^{-\psi}h)^{g}(h^{-1}h^{\psi}) \\ &= [g, h^{-1}h^{\psi}]. \end{aligned}$$

   Portanto, $D(G) = [G, L(G)] = [L(G), G]$. Como $L(G) \lhd \mathscr{X}(G)$, então $[g, h^{\psi}] \in L(G)$. Assim, $D(G) \subseteq L(G)$, logo $D(G) = D(G) \cap L(G) = W(G)$. Como $D(G) \subseteq L(G)$ e $[D(G), L(G)] = 1$ (pela Proposição 6.2.4), então $D(G) \subseteq Z(L(G))$.

2. Como $R(G) := [[G, L(G)], G^{\psi}]$ e $D(G) = [G, L(G)]$, então $R(G) = [D(G), G^{\psi}]$. Como $[D(G), G^{\psi}] = [D(G), G]$ (pelo item 2 do Lema 6.2.3), então $R(G) = [D(G), G]$.

3. Sejam $g, h \in G$. Pelos itens 8 e 9 do Lema 1.1.2, segue que:

$$[g^{-1}g^{\psi}, h^{-1}h^{\psi}] = [g^{-1}, h^{-1}h^{\psi}]^{g^{\psi}}[g^{\psi}, h^{-1}h^{\psi}] =$$

$$([g^{-1}, h^{\psi}][g^{-1}, h^{-1}]^{h^{\psi}})^{g^{\psi}}[g^{\psi}, h^{\psi}][g^{\psi}, h^{-1}]^{h^{\psi}}.$$

Como G é abeliano, então $[g^{-1}, h^{-1}] = [g^{\psi}, h^{\psi}] = 1$. Logo:

$$[g^{-1}g^{\psi}, h^{-1}h^{\psi}] = [g^{-1}, h^{\psi}]^{g^{\psi}}[g^{\psi}, h^{-1}]^{h^{\psi}}.$$

Como $D(G) \lhd \mathscr{X}(G)$, então $[g^{-1}g^{\psi}, h^{-1}h^{\psi}] \in D(G)$. Assim, $L(G)' \subseteq D(G)$. Como $[D(G), L(G)] = 1$ (pela Proposição 6.2.4), então $[L(G)', L(G)] \subseteq [D(G), L(G)] = 1$.

QED.

Lema 6.3.2. *Seja $g \in G$. Então, $(g^{-1}g^{\psi})^n = g^{-n}(g^{\psi})^n$ para todo $n \in \mathbb{N}$.*

Demonstração. Como $[g, g^{\psi}] = 1$, então:

$$g^{-1}g^{\psi} = g^{-1}g^{\psi}gg^{-1} = g^{-1}gg^{\psi}g^{-1} = g^{\psi}g^{-1}.$$

Por indução, segue que $(g^{-1}g^{\psi})^n = g^{-n}(g^{\psi})^n$ para todo $n \in \mathbb{N}$. *QED.*

Lema 6.3.3. *Suponha que G é abeliano. Sejam $m, n \in \mathbb{N}$ e $g, h \in G$. Então:*

$$[g^m, (h^{\psi})^n] = [g, h^{\psi}]^{mn}.$$

Demonstração. Como G é abeliano, então $D(G) \subseteq Z(L(G))$ (pela Proposição 6.3.1). Logo:

$$g^{-\psi}g[g, h^{\psi}] = [g, h^{\psi}]g^{-\psi}g;$$

$$g^{\psi}gg^{-1}h^{-\psi}gh^{\psi} = g^{-1}h^{-\psi}gh^{\psi}g^{-\psi}g;$$

$$g^{\psi}h^{-\psi}gh^{\psi} = g^{-1}(h^{-\psi}gh^{\psi}g^{-\psi})g;$$

$$[g, h^{\psi}] = [g, h^{\psi}]^g.$$

Pelo item 2 do Lema 6.2.3, $[g, h^{\psi}]^g = [g, h^{\psi}]^{g^{\psi}}$. Logo:

$$[g, h^{\psi}] = [g, h^{\psi}]^g = [g, h^{\psi}]^{g^{\psi}}. \ (1)$$

Analogamente:

$$[g, h^{\psi}] = [g, h^{\psi}]^{h} = [g, h^{\psi}]^{h^{\psi}}. \ (2)$$

Pelos itens 8 e 9 do Lema 1.1.2 e por (1) e (2), segue que:

$$[g^{m}, (h^{\psi})^{n}] = [g, h^{\psi}]^{mn}.$$

QED.

Teorema 6.3.4. *Sejam $p \in \mathbb{N}$ primo e $a_1, ..., a_n \in \mathbb{N}$ tais que $a_1 \geq a_2 \geq ... \geq a_n \geq 1$. Suponha que*

$$G = \prod_{i=1}^{n} \mathbb{Z}/p^{a_i}\mathbb{Z}.$$

Seja $u = \sum_{i=2}^{n}(i-1)a_i$. Então:

1. *$\mathscr{X}(G)$ é um p-grupo finito;*

2. *$W(G)/R(G) \simeq M(G)$, $|W(G)/R(G)| = p^{u}$, $exp(W(G)) = exp(M(G)) = p^{a_2}$.*

Demonstração.

1. Seja $v(g) := g^{-1}g^{\psi}$ para todo $g \in G$. Como G é um p-grupo abeliano, então, pelo Lema 6.3.2, $|v(g)|$ é uma potência de p para todo $g \in G$. Além disso, como G é abeliano, então $[L(G)', L(G)] = 1$ (pelo item 3 da Proposição 6.3.1). Logo:

$$1 = (v(g)^{v(h)})^{|v(g)|} = (v(g)[v(g), v(h)])^{|v(g)|} =$$

$$v(g)^{|v(g)|}[v(g), v(h)]^{|v(g)|} = [v(g), v(h)]^{|v(g)|} \ \forall \ g, h \in G.$$

   Portanto, $|[v(g), v(h)]|$ é finita para todo $g, h \in G$. Como $[L(G)', L(G)] = 1$ e $L(G) := \langle v(g) : g \in G \rangle$, então:

$$L(G) = \left\{ \prod_{g,h \in G} [v(g), v(h)]^{k_{gh}} \prod_{u \in G} v(u)^{e_u} : k_{gh}, e_u \in \mathbb{Z} \right\}.$$

Como $|[v(g), v(h)]|$, $|v(g)|$ são finitas para todo $g, h \in G$, então $L(G)$ é finito. Como $L(G) := \langle v(g) : g \in G \rangle$, $L(G)$ é finito e $|v(g)|$ é uma potência de p para todo $g \in G$, então $L(G)$ é um p-grupo finito. Como $L(G)$ e G são p-grupos finitos e $\mathscr{X}(G) = L(G) \rtimes G$ (pela Proposição 6.2.2), então $\mathscr{X}(G)$ é um p-grupo finito.

2. Como $D(G)$ é abeliano e $R(G) = [D(G), G]$ (pela Proposição 6.3.1), então, pelos itens 8 e 9 do Lema 1.1.2, pelo Lema 1.1.8 e pelos itens 1 e 2 do Lema 6.2.3, segue que:

$$D(G) = R(G)\langle \{[g_i, g_j^{\psi}] : g_i \in \mathbb{Z}/p^{a_i}\mathbb{Z}, g_j \in \mathbb{Z}/p^{a_j}\mathbb{Z}, 1 \leq i < j \leq n\}\rangle. \ (1)$$

Pelo Lema 6.3.3, segue que:

$$|[g_i, g_j^{\psi}]| \mid p^{a_j} \ \forall \ i, j \in \{1, ..., n\}, \ i < j. \ (2)$$

Assim, $D(G)^{p^u|R(G)|} = 1$. Como $D(G)$ é finito (pelo item 1), então $|D(G)| \mid p^u|R(G)|$, logo $|W(G)/R(G)| \mid p^u$. Como $|M(G)| = p^u$ (pela Proposição 5.4.4), então:

$$|W(G)/R(G)| \mid |M(G)|.$$

Pelo Teorema 6.2.5, existe um homomorfismo sobrejetivo $\phi : W(G)/R(G) \to M(G)$. Logo:

$$M(G) \simeq W(G)/R(G), \ |W(G)/R(G)| = |M(G)| = p^u. \ (3)$$

Como $exp(M(G)) = p^{a_2}$ (pela Proposição 5.4.4) e $D(G) = W(G)$ (pela Proposição 6.3.1), então, por (1), (2) e (3), segue que:

$$exp(W(G)) = exp(D(G)) = exp(M(G)) = p^{a_2}.$$

QED.

Corolário 6.3.5. *Suponha que G é um grupo abeliano finito. Então:*

1. $\mathscr{X}(G)$ *é um grupo finito;*

2. $exp(W(G)) = exp(M(G))$*;*

3. O conjunto dos primos que dividem a ordem de $\mathscr{X}(G)$ *é igual ao conjunto dos primos que dividem a ordem de* G*.*

Demonstração. Segue da Proposição 5.4.2, do item 4 da Proposição 6.2.10 e do Teorema 6.3.4. *QED.*

6.4 O expoente de $\mathscr{X}(G)$

Nesta seção, será estabelecida uma cota superior para o expoente de $\mathscr{X}(G)$ no caso em que G é um grupo finito.

Lema 6.4.1. *Suponha que* G *possui expoente finito. Então,* $\mathscr{X}(G)^{exp(G)} \subseteq D(G)$*.*

Demonstração. Seja $x \in \mathscr{X}(G)$. Logo, existem $g_1, ..., g_n \in G$ e $h_1, ..., h_n \in G^{\psi}$ tais que $x = g_1h_1...g_nh_n$. Pelo Lema 1.1.8, existe $d \in D(G)$ tal que:

$$x^{exp(G)} = d(g_1...g_n)^{exp(G)}(h_1...h_n)^{exp(G)} = d.$$

Portanto, $\mathscr{X}(G)^{exp(G)} \subseteq D(G)$. *QED.*

Teorema 6.4.2. *Suponha que* G *é um grupo finito. Então:*

$$exp(D(G)) \mid exp(M(G/G'))exp(M(G'))exp(G').$$

Demonstração. Pelo Lema 1.1.8, para todo $h \in G', g \in G$, existe $d \in [[G^{\psi}, G'], G']$ tal que $[h, g^{\psi}]^{exp(G')} = d[h^{exp(G')}, g^{\psi}] = d$. Logo, $[G^{\psi}, G']^{exp(G')} \subseteq [[G^{\psi}, G'], G']$. Como $[[G^{\psi}, G'], G'] \subseteq D(G)'$ (pelo item 4 da Proposição 6.2.7), então:

$$[G', G^{\psi}]^{exp(G')} \subseteq D(G)'. \ (1)$$

Pelo item 5 da Proposição 6.2.7, $[G', G^{\psi}]L(G)/L(G) = [G', G]L(G)/L(G)$. Assim, $([G', G^{\psi}]L(G)/L(G))^{exp([G',G])} \subseteq ([G', G]L(G)/L(G))^{exp([G',G])} = 1$, logo $[G', G^{\psi}]^{exp([G',G])} \subseteq L(G)$. Como $[G', G^{\psi}] \subseteq [G, G^{\psi}] = D(G)$, então:

$$[G', G^{\psi}]^{exp([G',G])} \subseteq D(G) \cap L(G) = W(G). \ (2)$$

Como $exp([G', G]) \mid exp(G')$ (pois $[G', G] \subseteq [G, G] = G'$), então, por (1) e (2), segue que:

$$[G', G^{\psi}]^{exp(G')} \subseteq D(G)' \cap W(G). \ (3)$$

Pelo Corolário 6.2.13 e pela Proposição 6.3.1, segue que:

$$D(G/G') \simeq \frac{D(G)\langle G', (G')^{\psi}\rangle^{\mathscr{X}(G)}}{\langle G', (G')^{\psi}\rangle^{\mathscr{X}(G)}}, \ (4)$$

$$D(G/G') = W(G/G'). \ (5)$$

Por (4) e (5), segue que:

$$(D(G)\langle G', (G')^{\psi}\rangle^{\mathscr{X}(G)})^{exp(W(G/G'))} \subseteq \langle G', (G')^{\psi}\rangle^{\mathscr{X}(G)}. \ (6)$$

Pela Proposição 6.2.11, segue que:

$$\langle G', (G')^{\psi}\rangle^{\mathscr{X}(G)} \cap D(G) = [G', G^{\psi}]. \ (7)$$

Por (6) e (7), segue que:

$$D(G)^{exp(W(G/G'))} \subseteq [G', G^{\psi}]. \ (8)$$

Por (3) e (8), segue que:

$$D(G)^{exp(W(G/G'))exp(G')} \subseteq D(G)' \cap W(G). \ (9)$$

Como $(D(G), W(G))$ é uma extensão central de $D(G)/W(G)$, então, pelo Teorema 5.3.4, $D(G)' \cap W(G) \simeq M(D(G)/W(G))$. Como $D(G)/W(G) \simeq G'$ (pela Proposição 6.2.2), então $D(G)' \cap W(G) \simeq M(G')$. Logo:

$$exp(D(G)) \mid exp(W(G/G'))exp(M(G'))exp(G'). \ (10)$$

Pelo item 2 do Corolário 6.3.5, $exp(W(G/G')) = exp(M(G/G'))$. Logo:

$$exp(D(G)) \mid exp(M(G/G'))exp(M(G'))exp(G'). \ (11)$$

QED.

Corolário 6.4.3. *Suponha que G é um grupo finito. Então:*

$$exp(M(G)) \mid exp(M(G/G'))exp(M(G'))exp(G').$$

Demonstração. Como $W(G) \subseteq D(G)$ e existe um homomorfismo sobrejetivo $\phi : W(G)/R(G) \to M(G)$ (pelo Teorema 6.2.5), então $exp(M(G)) \mid exp(D(G))$. Pelo Teorema 6.4.2, segue que:

$$exp(M(G)) \mid exp(M(G/G'))exp(M(G'))exp(G').$$

QED.

Teorema 6.4.4. *Suponha que G é um grupo finito. Então:*

$$exp(\mathscr{X}(G)) \mid exp(M(G/G'))exp(M(G'))exp(G')exp(G).$$

Em particular, se G é finito, então $exp(\mathscr{X}(G))$ é finito.

Demonstração. Segue da Proposição 5.4.1, do Lema 6.4.1 e do Teorema 6.4.2. *QED.*

6.5 Propriedades de $\mathscr{X}(G)$

Nesta seção, serão apresentadas algumas propriedades do grupo G que são preservadas pelo grupo $\mathscr{X}(G)$.

Teorema 6.5.1. *Suponha que G é finito. Então, $\mathscr{X}(G)$ é finito.*

Demonstração. Seja $p : G * G^{\psi} \to \mathscr{X}(G)$ a projeção canônica. Dado $u \in G * G^{\psi}$, existem únicos $s \in \mathbb{N}\backslash\{0\}$ e $g_1, ..., g_s \in G$ tais que $u = g_1 g_2^{\psi} ... g_{2i-1} g_{2i}^{\psi} ... g_s$ e $g_i \neq 1$ se $i \notin \{1, s\}$. Sob essas condições, define-se o comprimento de u como $\ell(u) := |\{i \in \{1, ..., s\} : g_i \neq 1\}|$, e define-se o termo final de u como g_s se $g_s \neq 1$ e como g_{s-1} se $g_s = 1$; além disso, u pode ser classificado como pertencente a uma de 4 classes possíveis, correspondentes aos seguintes casos:

$$g_1 = 1 \ e \ g_s = 1; g_1 = 1 \ e \ g_s \neq 1; g_1 \neq 1 \ e \ g_s = 1; g_1 \neq 1 \ e \ g_s \neq 1.$$

Considere a seguinte relação de equivalência em $G * G^{\psi}$:

$$u \sim v \iff p(u) = p(v).$$

Dado $u \in G * G^{\psi}$, u é dito *minimal* se $u \sim u'$ implica $\ell(u) \leq \ell(u')$. Como

$$g_1 g_2^{\psi} g_3 \sim (g_1 g_2^{-1}) g_2^{\psi} (g_2 g_3) \ \forall \ g_1, g_2, g_3 \in G,$$

$$g_1^{\psi} g_2 g_3^{\psi} \sim (g_1 g_2^{-1})^{\psi} g_2 (g_2 g_3)^{\psi} \ \forall \ g_1, g_2, g_3 \in G,$$

então todo elemento minimal de $G * G^{\psi}$ de comprimento 3 é equivalente a (pelo menos) 2 elementos minimais com mesmo comprimento e classe mas com termos finais distintos. Suponha, por hipótese indutiva, que, para algum $s \in \mathbb{N}$ $(s > 3)$, todo elemento minimal de $G * G^{\psi}$ de comprimento n $(1 < n < s)$ é equivalente a (pelo menos) $n - 1$ elementos minimais de $G * G^{\psi}$ com mesmo comprimento e classe mas com termos finais distintos. Seja $u \in G * G^{\psi}$ um elemento minimal de comprimento s, e suponha que $u = g_1 g_2^{\psi} ... g_{2i-1} g_{2i}^{\psi} ... g_s^{\psi}$, em que $g_1, ..., g_s \in G\backslash\{1\}$ (os demais casos são análogos). Logo,

$u_0 := g_1 g_2^{\psi} ... g_{2i-1} g_{2i}^{\psi} ... g_{s-2}^{\psi}$ é um elemento minimal de comprimento $s-2$. Por hipótese indutiva, para todo $k \in \{1, ..., s-3\}$, existem $g_1^{(k)}, ..., g_{s-2}^{(k)} \in G$ tais que $u_k \sim u_0$ (em que $u_k := g_1^{(k)} g_2^{(k)\psi} ... g_{2i-1}^{(k)} g_{2i}^{(k)\psi} ... g_{s-2}^{(k)\psi}$) e $g_{s-2}^{(m)} \neq g_{s-2}^{(n)}$ se $m \neq n$. Defina:

$$u^{(k)} := u_k g_{s-1} g_s^{\psi} \ \forall \ k \in \{1, ..., s-3\},$$

$$v^{(k)} := g_1^{(k)} g_2^{(k)\psi} ... g_{2i-1}^{(k)} g_{2i}^{(k)\psi} ... g_{s-4}^{(k)\psi} (g_{s-3}^{(k)} g_{s-2}^{(k)}) g_{s-2}^{(k)\psi} (g_{s-2}^{-(k)} g_{s-1}) g_s^{\psi} \ \forall \ k \in \{1, ..., s-3\}.$$

Como $u_k \sim u_0$ para todo $k \in \{1, ..., s-3\}$, então $u^{(k)} \sim u$ para todo $k \in \{1, ..., s-3\}$. Como $g_{s-3}^{(k)} g_{s-2}^{(k)\psi} g_{s-1} \sim (g_{s-3}^{(k)} g_{s-2}^{(k)}) g_{s-2}^{(k)\psi} (g_{s-2}^{-(k)} g_{s-1})$ para todo $k \in \{1, ..., s-3\}$, então $u^{(k)} \sim v^{(k)}$ para todo $k \in \{1, ..., s-3\}$. Portanto, $v^{(k)} \sim u$ para todo $k \in \{1, ..., s-3\}$. Defina:

$$w := g_1 g_2^{\psi} ... g_{2i-1} g_{2i}^{\psi} ... g_{s-3} (g_{s-2} g_{s-1}^{-1})^{\psi} g_{s-1} (g_{s-1} g_s)^{\psi},$$

$$w^{(k)} := g_1^{(k)} g_2^{(k)\psi} ... g_{2i-1}^{(k)} g_{2i}^{(k)\psi} ... g_{s-4}^{(k)\psi} (g_{s-3}^{(k)} g_{s-2}^{(k)})$$

$$(g_{s-2}^{(k)} (g_{s-2}^{-(k)} g_{s-1})^{-1})^{\psi} (g_{s-2}^{-(k)} g_{s-1}) ((g_{s-2}^{-(k)} g_{s-1}) g_s)^{\psi} \ \forall \ k \in \{1, ..., s-3\}.$$

Como $g_{s-2}^{\psi} g_{s-1} g_s^{\psi} \sim (g_{s-2} g_{s-1}^{-1})^{\psi} g_{s-1} (g_{s-1} g_s)^{\psi}$, então $w \sim u$. Como $g_{s-2}^{(k)\psi} (g_{s-2}^{-(k)} g_{s-1}) g_s^{\psi} \sim (g_{s-2}^{(k)} (g_{s-2}^{-(k)} g_{s-1})^{-1})^{\psi} (g_{s-2}^{-(k)} g_{s-1}) ((g_{s-2}^{-(k)} g_{s-1}) g_s)^{\psi}$, então $w^{(k)} \sim v^{(k)}$ para todo $k \in \{1, ..., s-3\}$, logo $w^{(k)} \sim u$ para todo $k \in \{1, ..., s-3\}$. Portanto, $W := \{u, w\} \cup \{w^{(k)} : k \in \{1, ..., s-3\}\}$ é um conjunto de cardinalidade $s-1$ cujos elementos são minimais, equivalentes entre si e cujos termos finais são distintos. Por indução, segue que, para todo $s \in \mathbb{N}$ ($s \geq 2$), todo elemento minimal de $G * G^{\psi}$ de comprimento s é equivalente a (pelo menos) $s-1$ elementos minimais de $G * G^{\psi}$ com mesmo comprimento e classe mas com termos finais distintos. Logo, como G é finito, não existem elementos minimais de $G * G^{\psi}$ com comprimento $\ell > |G| + 1$, e existe um número finito de elementos minimais de $G * G^{\psi}$ com comprimento $\ell \leq |G| + 1$. Assim, como todo elemento de $G * G^{\psi}$ é equivalente a algum elemento minimal, então $\mathscr{X}(G)$ é finito. *QED.*

Definição 6.5.2. *Um grupo H é dito* ***solúvel*** *se existe $n \in \mathbb{N}$ tal que $H^{(n)} = 1$. Se H é solúvel, então o* ***comprimento derivado*** *de H é definido como $min\{n \in \mathbb{N} : H^{(n)} = 1\}$.*

Definição 6.5.3. *Um grupo H é dito* **perfeito** *se $H = H'$.*

Teorema 6.5.4. *A construção $\mathscr{X}(G)$ satisfaz as seguintes propriedades:*

1. *G é um grupo solúvel $\implies$ $\mathscr{X}(G)$ é um grupo solúvel;*

2. *G é um grupo perfeito $\implies$ $\mathscr{X}(G)$ é um grupo perfeito;*

3. *G é um grupo finito $\implies$ $\mathscr{X}(G)$ é um grupo finito;*

4. *G é um p-grupo finito (p primo) $\implies$ $\mathscr{X}(G)$ é um p-grupo finito.*

Demonstração.

1. Suponha que G é solúvel com comprimento derivado n. Seja $\rho : \mathscr{X}(G) \to G \times G \times G$ conforme definido na Proposição 6.2.1. Como ρ é um homomorfismo de grupos e $G^{(n)} = 1$, então:

$$\rho(\mathscr{X}(G)^{(n)}) = \rho(\mathscr{X}(G))^{(n)} \subseteq (G \times G \times G)^{(n)} = G^{(n)} \times G^{(n)} \times G^{(n)} = 1.$$

   Assim, $\mathscr{X}(G)^{(n)} \subseteq ker(\rho) = W(G)$. Como $W(G)$ é abeliano (pela Proposição 6.2.4) e $\mathscr{X}(G)^{(n)} \subseteq W(G)$, então $\mathscr{X}(G)^{(n+1)} = 1$, logo $\mathscr{X}(G)$ é solúvel com comprimento derivado no máximo $n + 1$.

2. Suponha que G é perfeito. Como G, G^{ψ} são isomorfos e $G = G'$, então $G^{\psi} = (G^{\psi})'$. Como $G = G'$, $G^{\psi} = (G^{\psi})'$ e $G' \cup (G^{\psi})' \subseteq \mathscr{X}(G)'$, então $G \cup G^{\psi} \subseteq \mathscr{X}(G)'$. Como $G \cup G^{\psi} \subseteq \mathscr{X}(G)'$, $\mathscr{X}(G)' \leq \mathscr{X}(G)$ e $\mathscr{X}(G) = \langle G \cup G^{\psi} \rangle$, então $\mathscr{X}(G)' = \mathscr{X}(G)$, ou seja, $\mathscr{X}(G)$ é perfeito.

3. Segue do Teorema 6.5.1.

4. Segue da Proposição 5.4.1, do Teorema 6.4.4 e do Teorema 6.5.1.

QED.

7 A construção $\nu(G)$

Neste capítulo, será brevemente introduzida a construção $\nu(G)$, definida no artigo *On a Construction Related to the Non-abelian Tensor Square of a Group* (referência [2]), de N. Rocco, e será construído um isomorfismo não trivial entre quocientes de $\mathscr{X}(G)$ e $\nu(G)$.

Por todo o capítulo, G denotará um grupo (multiplicativo) arbitrário com elemento neutro 1, e $\psi : G \to G^\psi$ denotará um isomorfismo tal que G e G^ψ são disjuntos. Além disso, será utilizada a seguinte notação:

$$g^\psi := \psi(g)\ \forall\ g \in G,\ g^{-\psi} := \psi(g^{-1})\ \forall\ g \in G,\ Y^\psi := \psi(Y)\ \forall\ Y \subseteq G.$$

Definição 7.0.1.

$$\nu(G) := \frac{G * G^\psi}{\langle [g_1, g_2^\psi]^{g_3}[g_1^{g_3}, (g_2^{g_3})^\psi]^{-1}, [g_1, g_2^\psi]^{g_3^\psi}[g_1^{g_3}, (g_2^{g_3})^\psi]^{-1} : g_1, g_2, g_3 \in G\rangle^{G*G^\psi}}.$$

Em particular, vale a seguinte relação em $\nu(G)$:

$$[g_1, g_2^\psi]^{g_3} = [g_1^{g_3}, (g_2^{g_3})^\psi] = [g_1, g_2^\psi]^{g_3^\psi}\ \forall\ g_1, g_2, g_3 \in G.\ (*)$$

Pelo restante do capítulo, esta relação será denotada por $(*)$. Além disso, as imagens de G e G^ψ pela projeção canônica $p : G * G^\psi \to \nu(G)$ serão denotadas por G e G^ψ, respectivamente.

Definição 7.0.2. *Define-se o seguinte subgrupo de $\nu(G)$:*

$$\Delta(G) := \langle \{[g, g^\psi] : g \in G\}\rangle.$$

Lema 7.0.3. *Sejam $g_1, g_2, g_3, g_4 \in G$. Valem as seguintes relações em $\nu(G)$:*

1. $[g_1, g_2^\psi]^{[g_3, g_4^\psi]} = [g_1, g_2^\psi]^{[g_3, g_4]}$;

2. $[[g_1, g_2], g_3^\psi] = [[g_1, g_2^\psi], g_3]$;

3. $[[g_1, g_1^\psi], g_2] = [[g_1, g_1^\psi], g_2^\psi] = 1.$

Demonstração.

1. Aplicando a relação $(*)$, segue que:

$$[g_1, g_2^\psi]^{[g_3, g_4^\psi]} = [g_1, g_2^\psi]^{g_3^{-1} g_4^{-\psi} g_3 g_4^\psi} = [g_1^{g_3^{-1} g_4^{-1} g_3 g_4}, (g_2^{g_3^{-1} g_4^{-1} g_3 g_4})^\psi] =$$

$$[g_1, g_2^\psi]^{g_3^{-1} g_4^{-1} g_3 g_4} = [g_1, g_2^\psi]^{[g_3, g_4]}.$$

2. Pelos itens 4 e 8 do Lema 1.1.2, segue que:

$$[[g_1, g_2], g_3^\psi] = [g_1^{-1} g_1^{g_2}, g_3^\psi] =$$

$$[g_1^{-1}, g_3^\psi]^{g_1^{g_2}} [g_1^{g_2}, g_3^\psi] = [g_1^{-1}, g_3^\psi]^{g_2^{-1} g_1 g_2} [g_1^{g_2}, g_3^\psi].$$

Pela relação $(*)$, $[g_1^{g_2}, g_3^\psi] = [g_1^{g_2}, (g_3^{g_2^{-1} g_2})^\psi] = [g_1, (g_3^{g_2^{-1}})^\psi]^{g_2}$. Logo:

$$[[g_1, g_2], g_3^\psi] = [g_1^{-1}, g_3^\psi]^{g_2^{-1} g_1 g_2} [g_1, (g_3^{g_2^{-1}})^\psi]^{g_2}.$$

Pelos itens 5 e 7 do Lema 1.1.2, $[g_1^{-1}, g_3^\psi] = [g_3^\psi, g_1]^{g_1^{-1}} = [g_1, g_3^\psi]^{-g_1^{-1}}$. Logo:

$$[[g_1, g_2], g_3^\psi] = [g_1, g_3^\psi]^{-g_1^{-1} g_2^{-1} g_1 g_2} [g_1, (g_3^{g_2^{-1}})^\psi]^{g_2} =$$

$$[g_1, g_3^\psi]^{-[g_1, g_2]} [g_1, (g_2 g_3 g_2^{-1})^\psi]^{g_2}.$$

Pelo item 9 do Lema 1.1.2 e pela relação $(*)$, tem-se que
$[g_1, (g_2 g_3 g_2^{-1})^\psi]^{g_2} = [g_1, (g_2^{-1})^\psi]^{g_2} [g_1, (g_2 g_3)^\psi] = [g_1, (g_2^{-1})^\psi]^{g_2} [g_1, g_3^\psi][g_1, g_2^\psi]^{g_3}$. Logo:

$$[[g_1, g_2], g_3^\psi] = [g_1, g_3^\psi]^{-[g_1, g_2]} [g_1, (g_2^{-1})^\psi]^{g_2} [g_1, g_3^\psi][g_1, g_2^\psi]^{g_3}.$$

Por $(*)$ e pelos itens 5 e 7 do Lema 1.1.2, $[g_1, (g_2^{-1})^\psi]^{g_2} = [g_2^\psi, g_1] = [g_1, g_2^\psi]^{-1}$. Logo:

$$[[g_1, g_2], g_3^\psi] = [g_1, g_3^\psi]^{-[g_1, g_2]} [g_1, g_2^\psi]^{-1} [g_1, g_3^\psi][g_1, g_2^\psi]^{g_3}.$$

Pelo item 1, $[g_1, g_3^{\psi}]^{-[g_1,g_2]} = [g_1, g_3^{\psi}]^{-[g_1,g_2^{\psi}]}$. Logo:

$$[[g_1, g_2], g_3^{\psi}] = [g_1, g_3^{\psi}]^{-[g_1,g_2^{\psi}]}[g_1, g_2^{\psi}]^{-1}[g_1, g_3^{\psi}][g_1, g_2^{\psi}]^{g_3} =$$

$$([g_1, g_2^{\psi}]^{-1}[g_1, g_3^{\psi}]^{-1}[g_1, g_2^{\psi}])[g_1, g_2^{\psi}]^{-1}[g_1, g_3^{\psi}][g_1, g_2^{\psi}]^{g_3} = [g_1, g_2^{\psi}]^{-1}[g_1, g_2^{\psi}]^{g_3}.$$

Pelo item 4 do Lema 1.1.2, $[g_1, g_2^{\psi}]^{-1}[g_1, g_2^{\psi}]^{g_3} = [[g_1, g_2^{\psi}], g_3]$. Portanto:

$$[[g_1, g_2], g_3^{\psi}] = [[g_1, g_2^{\psi}], g_3].$$

3. Pelo item 2, segue que

$$[[g_1, g_1^{\psi}], g_2] = [[g_1, g_1], g_2^{\psi}] = [1, g_2^{\psi}] = 1.$$

Além disso, por $(*)$ e pelo item 4 do Lema 1.1.2, segue que:

$$[[g_1, g_1^{\psi}], g_2^{\psi}] = [g_1, g_1^{\psi}]^{-1}[g_1, g_1^{\psi}]^{g_2^{\psi}} = [g_1, g_1^{\psi}]^{-1}[g_1, g_1^{\psi}]^{g_2} = [[g_1, g_1^{\psi}], g_2].$$

Portanto:

$$[[g_1, g_1^{\psi}], g_2] = [[g_1, g_1^{\psi}], g_2^{\psi}] = 1.$$

QED.

Proposição 7.0.4. *$\Delta(G) \subseteq Z(\nu(G)) \cap \nu(G)'$ e $\Delta(G) \lhd \nu(G)$.*

Demonstração. Como $[\Delta(G), G] = [\Delta(G), G^{\psi}] = 1$ (pelo item 3 do Lema 1.1.2) e $\nu(G) = \langle G, G^{\psi} \rangle$, então $\Delta(G) \subseteq Z(\nu(G))$. Como $\Delta := \langle [g, g^{\psi}] : g \in G \rangle$, então $\Delta(G) \subseteq \nu(G)'$. Logo:

$$\Delta(G) \subseteq Z(\nu(G)) \cap \nu(G)'.$$

Em particular, $\Delta(G) \lhd \nu(G)$. *QED.*

Teorema 7.0.5. *Existe um isomorfismo* $\eta : \nu(G)/\Delta(G) \to \mathscr{X}(G)/R(G)$ *tal que:*

$$g\Delta(G) \mapsto gR(G) \ \forall \ g \in G, \ \ g^{\psi}\Delta(G) \mapsto g^{\psi}R(G) \ \forall \ g \in G.$$

Além disso, existe um homomorfismo sobrejetivo $\phi : M(\mathscr{X}(G)/R(G)) \to \Delta(G)$.

Demonstração. Pela Proposição 7.0.4, segue que:

$$\Delta(G) \subseteq Z(\nu(G)) \cap \nu(G)', \ \ \Delta(G) \lhd \nu(G).$$

Pelos itens 3 e 4 da Proposição 6.2.8 e pelas definições de $\mathscr{X}(G)$, $\nu(G)$ e $\Delta(G)$, existe um isomorfismo $\eta : \nu(G)/\Delta(G) \to \mathscr{X}(G)/R(G)$ tal que:

$$g\Delta(G) \mapsto gR(G) \ \forall \ g \in G, \ \ g^{\psi}\Delta(G) \mapsto g^{\psi}R(G) \ \forall \ g \in G.$$

Além disso, como $\Delta(G) \subseteq Z(\nu(G)) \cap \nu(G)'$ e $\nu(G)/\Delta(G) \simeq \mathscr{X}(G)/R(G)$, então, pelo Teorema 5.3.4, existe um homomorfismo sobrejetivo $\phi : M(\mathscr{X}(G)/R(G)) \to \Delta(G)$. *QED.*

Teorema 7.0.6. *A construção* $\nu(G)$ *satisfaz as seguintes propriedades:*

1. *G é um grupo solúvel* $\Longrightarrow$ $\nu(G)$ *é um grupo solúvel;*

2. *G é um grupo perfeito* $\Longrightarrow$ $\nu(G)$ *é um grupo perfeito;*

3. *G é um grupo finito* $\Longrightarrow \nu(G)$ *é um grupo finito;*

4. *G é um p-grupo finito (p primo)* $\Longrightarrow$ $\nu(G)$ *é um p-grupo finito.*

Demonstração. Segue da Proposição 5.4.1, do Teorema 6.5.4 e do Teorema 7.0.5. *QED.*

RERERÊNCIAS BIBLIOGRÁFICAS

[1] S. Sidki. *On weak permutability between groups.* J. Algebra 63 (1980), no. 1, 186–225.

[2] N. R. Rocco. *On a Construction Related to the Non-abelian Tensor Square of a Group.* Bol. Soc. Brasil. Mat. (N.S.) 22 (1991), no. 1, 63–79.

[3] Joseph J. Rotman. *An Introduction to Homological Algebra.* Pure and Applied Mathematics, 85. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], New York-London, 1979.

[4] Daniel E. Cohen. *Combinatorial group theory: a topological approach.* London Mathematical Society Student Texts, 14. Cambridge University Press, Cambridge, 1989.

[5] Serge Lang. *Algebra.* Springer, 2002. ISBN: 038795385X.

[6] Charles A. Weibel. *An Introduction to Homological Algebra.* Cambridge University Press, 1994.

[7] S. Hatui; V. Kakkar; M. K. Yadav. *The Schur multipliers of p-groups of order* p^5. arXiv: 1804.11308v2, 2018.

[8] B. Mashayekhy; F. Mohammadzadeh; A. Hokmabadi. *On the Order of Schur Multipliers of Finite Abelian p-Groups.* Int. J. Contemp. Math. Sci., Vol. 2, 2007, no. 10, 479 - 485.