UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Álgebra homológica e cohomologia de grupos

Alexandre Carissimi

Dissertação de Mestrado do Programa de Pós-Graduação em Matemática (PPG-Mat)

ICMC USP SÃO CARLOS

Alexandre Carissimi

Álgebra homológica e cohomologia de grupos

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Matemática. *VERSÃO REVISADA*

Área de Concentração: Matemática

Orientador: Prof. Dr. Victor Hugo Jorge Pérez

USP – São Carlos
Maio de 2020

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

C277Á

Carissimi, Alexandre
Álgebra homológica e cohomologia de grupos / Alexandre Carissimi; orientador Victor Hugo Jorge Pérez. -- São Carlos, 2020.
97 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Matemática) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2020.

1. Funtores Ext e Tor. 2. Extensões de grupo. 3. Módulos projetivos e injetivos. I. Jorge Pérez, Victor Hugo, orient. II. Título.

Bibliotecários responsáveis pela estrutura de catalogação da publicação de acordo com a AACR2:
Gláucia Maria Saia Cristianini - CRB - 8/4938
Juliana de Souza Moraes - CRB - 8/6176

Alexandre Carissimi

Homological algebra and group cohomology

Master dissertation submitted to the Institute of Mathematics and Computer Sciences – ICMC-USP, in partial fulfillment of the requirements for the degree of the Master Program in Mathematics. *FINAL VERSION*

Concentration Area: Mathematics

Advisor: Prof. Dr. Victor Hugo Jorge Pérez

USP – São Carlos
May 2020

Dedico este trabalho à minha futura esposa, Bruna Secco Pasini, pelo amor, carinho e paciência dedicados durante este período.

AGRADECIMENTOS

Os agradecimentos principais são direcionados ao Professor Doutor Victor Hugo Jorge Pérez, orientador desse trabalho, e à Coordenação de aperfeiçoamento de pessoal de nível superior, a CAPES, pelo apoio financeiro prestado, sem os quais este trabalho não teria sido desenvolvido.

Agradecimentos especiais são direcionados à minha família, meus pais e irmã, que me apoiaram e me deram o suporte necessário para buscar meus sonhos e objetivos.

"Tudo o que temos de decidir é o que fazer com o tempo que nos é dado."

Gandalf, em O Senhor dos Anéis, TOLKIEN, J. R. R.

RESUMO

CARISSIMI, A. **Álgebra homológica e cohomologia de grupos**. 2020. 99 p. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2020.

Neste trabalho abordamos conceitos básicos de teoria de categorias e aplicamos tais ideias à categoria de módulos sobre um anel. Também desenvolvemos as ferramentas necessárias para se estudar álgebra homológica, como complexos de cadeia, resoluções projetivas e injetivas, para então tratar dos funtores Ext e Tor. Em seguida, utilizamos tais construções para definir a cohomologia de um grupo G com coeficientes em um G-módulo M, calculamos alguns grupos de cohomologia nos níveis baixos e damos um procedimento padrão para se obter uma resolução projetiva do grupo abeliano dos números inteiros visto como G-módulo trivial. Finalmente, aplicamos estes conceitos para abordar o problema da extensão de grupos, dando uma caracterização das extensões de um grupo abeliano M por um grupo qualquer G usando a cohomologia de grupos.

Palavras-chave: Funtores Ext e Tor, Extensões de grupo, Módulos projetivos e injetivos.

ABSTRACT

CARISSIMI, A. **Homological algebra and group cohomology**. 2020. 99 p. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2020.

In this work we approach basic concepts of category theory and apply these ideas to the category of modules over a given ring. We also develop the needed tools to study homological algebra, e.g. chain complexes and projective and injective resolutions and then we treat the Ext and Tor functors. After that, we use such constructions to define the cohomology of a group G with coefficients on a G-module M, we calculate some low level cohomology groups and give a standard procedure to obtain a projective resolution of the abelian group of the integers viewed as a trivial G-module. Finally, we apply these concepts to approach the problem of the group extensions, giving a characterization of the extensions of an abelian group M by a group G using group cohomology.

Keywords: Ext and Tor functors, Group extensions, Projective and injective modules.

SUMÁRIO

INTRODUÇÃO

Esta dissertação trata dos conceitos básicos e necessários para se estudar álgebra homológica, em especial a (co)homologia de grupos e o problema da extensão de grupos.

A álgebra homológica estuda homologia em um cenário algébrico geral. Esta disciplina tem suas origens na topologia algébrica e na álgebra abstrata e o seu desenvolvimento se deu intimamente ligado à teoria de categorias, já que, de maneira ampla, estuda funtores derivados e complexos de cadeia. A cohomologia de grupos utiliza as ferramentas da álgebra homológica para estudar grupos, ao analisar a ação de um grupo G sobre um G-módulo associado M e, assim, obter informações sobre o grupo G e também sobre o G-módulo M. Baseado no topologia algébrica e visualizando o grupo G como um espaço topológico, pode-se construir uma resolução projetiva semelhante ao complexo simplicial e, a partir deste, calcular as cohomologias do grupo G.

Iniciamos o texto tratando da teoria de categorias no primeiro capítulo, apresentando as definições de categorias, funtores e transformações naturais, assim como alguns conceitos acerca de morfismos e objetos, além de produtos e coprodutos e equalizadores e coequalizadores. No segundo capítulo especializamos os conceitos vistos no primeiro ao estudar a categoria de módulos sobre um anel. Também tratamos do grupos de homomorfismos de módulo e do produto tensorial de módulos e finalizamos com os conceitos de módulos projetivos e injetivos, centrais para o desenvolvimento da (co)homologia.

No terceiro capítulo definimos complexos e (co)homologia e provamos alguns resultados chave desse tema. Logo em seguida tratamos de resoluções projetivas e injetivas para então definirmos os funtores derivados $\mathrm{Tor}\,(-,-)$ e $\mathrm{Ext}\,(-,-)$, além de provarmos os principais teoremas do assunto.

Por fim, no quarto capítulo definimos a (co)homologia de grupos com coeficientes usando os funtores derivados definidos no capítulo anterior. Como exemplos iniciais calculamos as (co)homologias de grupos cíclicos, damos uma caracterização da (co)homologia no nível zero e também no nível um para o caso de módulos triviais. Além disso, construímos uma resolução projetiva do anel dos inteiros visto como módulo trivial sobre o grupo em questão e a usamos para dar uma descrição alternativa dos grupos de cohomologia. Finalmente, atacamos o problema da extensão de grupos, usando o que foi feito nas seções anteriores do capítulo, para relacionar o problema com os grupos de cohomologia no nível um e dois.

CAPÍTULO

1

TEORIA DE CATEGORIAS

Em todas as áreas da matemática costumamos estudar estruturas de diversos tipos: algébricas, topológicas, geométricas ou até mesmo uma mistura mas não limitando-se apenas a estas. Além de estudarmos cada objeto de determinada estrutura separadamente, também nos interessamos pelas maneiras com que estes objetos se comparam e se relacionam. De maneira simplista, podemos dizer que a teoria de categorias fornece um ambiente no qual podemos codificar tal organização da matemática, de maneira que uma categoria consiste em uma coleção de objetos, que podem ou não possuir alguma estrutura comum, e uma coleção de morfismos entre tais objetos que servem como instrumentos de comparação.

Seguindo esta linha de raciocínio, podemos ver categorias também como um tipo de estrutura, assim comparar categorias se torna uma ideia pertinente e isto se traduz no conceito de funtores. Veremos ainda que isto pode avançar mais um degrau, chegando à noção de transformação natural, que é o instrumento de comparação entre funtores.

Neste capítulo, apresentaremos as definições básicas desta teoria e construiremos uma base para depois estudarmos estes conceitos em uma categoria específica: a categoria de módulos sobre um anel. Tais conceitos básicos podem ser encontrados nos livros de Leinster (2014) e MacLane (1978), o primeiro traz uma apresentação básica da teoria, enquanto que o segundo é uma referência mais ampla, envolvendo conceitos mais avançados.

Na primeira seção deste capítulo definiremos o conceito de categoria, daremos alguns exemplos e finalizaremos com a ideia de dualidade, fundamental no estudo de teoria de categorias. Na segunda seção, trataremos de morfismos dentro de uma categoria e definiremos o conceito de objetos iniciais, finais e zero, presentes na categoria que estaremos interessados mais a frente. Na terceira seção veremos como podemos comparar duas categorias, por meio do conceito de funtor, em seguida, na quarta seção subiremos o degrau mencionado acima e definiremos a ideia de transformação natural. Por fim, na quinta seção, generalizaremos para categorias arbitrárias os conceitos de produto direto e soma direta de módulos e núcleo e conúcleo de homomorfismos,

definindo produtos, coprodutos, equalizadores e coequalizadores.

1.1 Categorias

Definição 1. Uma categoria C consiste em

- uma coleção de objetos $\mathrm{ob}(C)$;
- para cada par (A, B) de objetos de C um conjunto $C(A, B)$ de morfismos de A em B;
- para cada objeto $A \in \mathrm{ob}(C)$ um morfismo $1_A \in C(A, A)$;
- para cada par de morfismos $f \in C(A, B)$ e $g \in C(B, C)$, um terceiro morfismo $g \circ f \in C(A, C)$ chamado de composição (ou composta) de f e g;

cumprindo os axiomas

- se $f \in C(A, B)$, $g \in C(B, C)$ e $h \in C(C, D)$, então

$$h \circ (g \circ f) = (h \circ g) \circ f;$$

- se $f \in C(A, B)$, então

$$f \circ 1_A = f = 1_B \circ f.$$

Observação 1. Em geral, utilizaremos as notações simplificadas abaixo:

- $A \in C$ ao invés de $A \in \mathrm{ob}(C)$;
- $f : A \to B$ ou $A \xrightarrow{f} B$ ao invés de $f \in C(A, B)$;
- gf ao invés de $g \circ f$;
- se $f : A \to B$, então dizemos que A é o domínio de f e denotamos $A = \mathrm{Dom}(f)$, e dizemos que B é o codomínio (ou contradomínio) de f e denotamos $B = \mathrm{Codom}(f)$.

Exemplo 1. Alguns exemplos de categorias incluem:

1. $\mathfrak{Set}$: categoria cujos objetos são conjuntos e morfismos são funções com domínio e contradomínio específicos;
2. $\mathfrak{Group}$: objetos são grupos e morfismos são homomorfismos de grupo;
3. $\mathfrak{Ring}$: objetos são anéis com unidade e morfismos são homomorfismos de anel que preservam a unidade.

Exemplo 2. Para anéis com unidade A e B, temos as seguintes categorias:

1. ${}_A\mathfrak{Mod}$ dos A-módulos à esquerda e A-homomorfismos;
2. $\mathfrak{Mod}_B$ dos B-módulos à direita e B-homomorfismos;
3. ${}_A\mathfrak{Mod}_B$ dos (A, B)-bimódulos e (A, B)-homomorfismos.

Exemplo 3. Como casos particulares dos exemplos anteriores temos:

1. se $A = \mathbb{Z}$, então ${}_A\mathfrak{Mod} = \mathfrak{Ab}$ é a categoria dos grupos abelianos e homomorfismos de grupo;
2. se $A = \mathbb{K}$ um corpo, então ${}_A\mathfrak{Mod} = {}_{\mathbb{K}}\mathfrak{Vect}$ é a categoria dos $\mathbb{K}$-espaços vetoriais e K-transformações lineares.

Definição 2. Seja C uma categoria. A categoria oposta C^{op} de C consiste em:

- a mesma coleção de objetos de C;
- uma coleção de morfismos em correspondência biunívoca com os morfismos de C de tal maneira que um morfismo $f^{op} : B \to A$ em C^{op} corresponde a um morfismo $f : A \to B$ em C;
- para cada objeto A, o morfismo 1_A^{op} serve como identidade em C^{op};
- se $f^{op} : B \to A$ e $g^{op} : C \to B$, então $f : A \to B$ e $g : B \to C$, assim $f^{op} \circ g^{op} = (g \circ f)^{op}$.

Esta construção tem uma consequência fundamental na teoria, que é o chamado conceito de dualidade. Brevemente, isto significa que dada uma proposição que se aplica a qualquer categoria e é enunciada em termos puramente categóricos (envolvendo apenas objetos e morfismos), então existe uma proposição dual, interpretada na categoria oposta, bastando para isso inverter a direção dos morfismos originais. Veremos no decorrer do texto inúmeras situações nas quais a dualidade se aplica. Por questão de simplicidade, nem sempre enunciaremos as duas versões duais de uma mesma proposição ou definição, desta maneira, quando nos referirmos a algum resultado podemos estar nos referindo àquele enunciado ou ao seu dual que pode não ter sido enunciado, o contexto e as hipóteses servirão de guia nestes casos.

1.2 Definições complementares

Definição 3. Seja $f : A \to B$ um morfismo, então:

1. dizemos que f é um monomorfismo quando para $g, h : C \to A$ tais que $fg = fh$ temos que $g = h$;

2. dizemos que f é um epimorfismo quando para $g, h : B \to C$ tais que $gf = hf$ temos que $g = h$;

3. dizemos que f é um bimorfismo quando f é monomorfismo e epimorfismo simultaneamente;

4. dizemos que f é uma seção quando existe $g : B \to A$ tal que $gf = 1_A$;

5. dizemos que f é uma retração quando existe $g : B \to A$ tal que $fg = 1_B$;

6. dizemos que f é um isomorfismo quando f é seção e retração simultaneamente.

Será comum denotarmos monomorfismos por flechas do tipo $A \rightarrowtail B$ e epimorfismos por flechas do tipo $A \twoheadrightarrow B$.

Proposição 1. Para um morfismo $f : A \to B$ são equivalentes:

1. f é isomorfismo;

2. existe $g : B \to A$ tal que $gf = 1_A$ e $fg = 1_B$;

3. f é seção e epimorfismo simultaneamente;

4. f é retração e monomorfismo simultaneamente.

Demonstração. (1.)⇒(2.): Existem $g, h : B \to A$ tais que $gf = 1_A$ e $fg = 1_B$, logo

$$g = g1_B = g(fh) = (gf)h = 1_A h = h.$$

(2.)⇒(1.), (1.)⇒(3.) e (1.)⇒(4.): Imediatas da definição acima.

(3.)⇒(2.): Como f é seção, então existe $g : B \to A$ tal que $gf = 1_A$, logo $(fg)f = f = 1_B f$, mas sendo f epimorfismo, temos que $fg = 1_B$.

(4.)⇒(2.): É o dual de (3.)⇒(2.). □

Nas condições da proposição acima, concluímos que g é único, escrevemos $g = f^{-1}$, dizemos que f é inversível e que f^{-1} é o seu inverso. Note que por simetria f^{-1} também é um isomorfismo e $(f^{-1})^{-1} = f$. Além disso, dizemos que A e B são isomorfos e escrevemos $A \cong B$.

Proposição 2. Sejam $f : A \to B$ e $g : B \to C$ dois morfismos em uma categoria C. Então:

1. se f e g são monomorfismos, então gf é um monomorfismo.

2. se gf é um monomorfismo, então f é um monomorfismo.

3. se f e g são epimorfismos, então gf é um epimorfismo.

4. se gf é um epimorfismo, então g é um epimorfismo.

Demonstração. Por dualidade é suficiente mostrar (1.) e (2.). Para isso, sejam $h, h' : D \to A$.

(1.): se $gfh = gfh'$, então $fh = fh'$ pois g é um monomorfismo, logo $h = h'$ pois f é um monomorfismo.

(2.): se $fh = fh'$, então $gfh = gfh'$, logo $h = h'$ pois gf é um monomorfismo. □

Definição 4. Seja $A \in C$ um objeto, então:

1. dizemos que A é inicial quando para cada objeto $B \in C$ existe um único morfismo $A \to B$;
2. dizemos que A é final quando para cada objeto $B \in C$ existe um único morfismo $B \to A$;
3. dizemos que A é zero (ou nulo) quando A é inicial e final simultaneamente.

Observação 2. Note que a definição acima não garante a existência de objetos iniciais em dada categoria C. No entanto, quando existem, objetos iniciais são únicos a menos de um único isomorfismo, isto é, se A e B são objetos iniciais, então existe um único isomorfismo $A \to B$. O mesmo pode ser dito acerca de objetos finais e, consequentemente, acerca de objetos zero.

Se C possui um objeto zero, digamos Z, então para cada par de objetos $A, B \in C$ definimos o morfismo zero de A em B, denotado por $0_{A,B} : A \to B$, ou simplesmente $0 : A \to B$, como sendo a única composição $A \to Z \to B$. Disso segue que compor com zero em qualquer lado sempre é igual a zero.

1.3 Funtores

Definição 5. Sejam C e $\mathcal{D}$ categorias. Um funtor covariante $\mathsf{F} : C \to \mathcal{D}$ de C em $\mathcal{D}$ consiste em

- uma aplicação que a cada $A \in C$ leva a $\mathsf{F}(A) \in \mathcal{D}$;
- para cada par de objetos $A, B \in C$ uma aplicação $C(A, B) \to \mathcal{D}(\mathsf{F}(A), \mathsf{F}(B))$;

cumprindo os axiomas

- se $f : A \to B$ e $g : B \to C$, então

$$\mathsf{F}(gf) = \mathsf{F}(g)\mathsf{F}(f) : \mathsf{F}(A) \to \mathsf{F}(C);$$

- se $A \in C$, então

$$\mathsf{F}(1_A) = 1_{\mathsf{F}(A)}.$$

De maneira dual, podemos definir funtores contravariantes.

Definição 6. Sejam C e $\mathcal{D}$ categorias. Um funtor contravariante $\mathsf{F} : C \to \mathcal{D}$ de C em $\mathcal{D}$ consiste em

- uma aplicação que a cada $A \in C$ leva a $\mathsf{F}(A) \in \mathcal{D}$;
- para cada par de objetos $A, B \in C$ uma aplicação $C(A, B) \to \mathcal{D}(\mathsf{F}(B), \mathsf{F}(A))$;

cumprindo os axiomas

- se $f : A \to B$ e $g : B \to C$, então

$$\mathsf{F}(gf) = \mathsf{F}(f)\mathsf{F}(g) : \mathsf{F}(C) \to \mathsf{F}(A);$$

- se $A \in C$, então

$$\mathsf{F}(1_A) = 1_{\mathsf{F}(A)}.$$

Observação 3. Note que um funtor contravariante $\mathsf{F} : C \to \mathcal{D}$ é o mesmo que um funtor covariante $\mathsf{F} : C^{op} \to \mathcal{D}$. Por este motivo, trataremos apenas de funtores covariantes, a menos que especificado o contrário, e omitiremos o adjetivo de variância, nos referindo apenas a funtores, deixando clara a sua variância na presença ou ausência de uma categoria oposta como seu domínio.

Além disso, por questões de simplicidade, um morfismo no domínio de um funtor $\mathsf{F} : C^{op} \to \mathcal{D}$ será sempre representado por um morfismo $f : A \to B$ em C, apontando do seu domínio em C para o seu contradomínio em C. De maneira similar, a sua imagem será sempre representada como um morfismo $\mathsf{F}(f) : \mathsf{F}(B) \to \mathsf{F}(A)$, apontando do seu domínio para o seu contradomínio em $\mathcal{D}$.

Com estas convenções, se $f : A \to B$ e $g : B \to C$ são morfismos em C, então a sua composição será sempre denotada por $g \circ f : A \to C$. A imagem deste morfismo pelo funtor contravariante $\mathsf{F} : C^{op} \to \mathcal{D}$ é o morfismo $\mathsf{F}(g \circ f) : \mathsf{F}(C) \to \mathsf{F}(A)$, que é igual à composição $\mathsf{F}(f) \circ \mathsf{F}(g)$ de $\mathsf{F}(g) : \mathsf{F}(C) \to \mathsf{F}(B)$ e $\mathsf{F}(f) : \mathsf{F}(B) \to \mathsf{F}(A)$.

Resumindo, mesmo utilizando categorias opostas, tentaremos representar os morfismos e as composições na "direção correta".

Exemplo 4. Dada uma categoria C, existe um funtor identidade $1_C : C \to C$ que age identicamente sobre objetos e sobre morfismos de C.

Definição 7. Sejam $\mathsf{F} : C \to \mathcal{D}$ e $\mathsf{G} : \mathcal{D} \to \mathsf{E}$ funtores. Então o funtor composto (ou composição) de F e G é denotado por $\mathsf{G} \circ \mathsf{F} : C \to \mathsf{E}$ e leva cada objeto $A \in C$ ao objeto $\mathsf{G}(\mathsf{F}(A)) \in \mathcal{E}$ e cada morfismo $f : A \to B$ ao morfismo $\mathsf{G}(\mathsf{F}(f)) : \mathsf{G}(\mathsf{F}(A)) \to \mathsf{G}(\mathsf{F}(B))$. Em geral, utilizaremos a notação simplificada GF ao invés de $\mathsf{G} \circ \mathsf{F}$.

Definição 8. Um funtor $\mathsf{F} : C \to \mathcal{D}$ é dito um isomorfismo de categorias quando existe um funtor $\mathsf{G} : \mathcal{D} \to C$ tal que

$$\mathsf{GF} = 1_C \quad \text{e} \quad \mathsf{FG} = 1_{\mathcal{D}}.$$

Note que a definição de isomorfismo de categorias é análoga à de isomorfismo em uma categoria, portanto os comentários feitos após a definição de isomorfismo se aplicam aos funtores também. Em particular, neste caso, dizemos que C e $\mathcal{D}$ são categorias isomorfas e escrevemos $C \cong \mathcal{D}$.

Exemplo 5. Veremos à frente que para um anel com unidade A, temos os seguintes exemplos:

1. para A-módulos à esquerda (ou à direita) M e N, temos os funtores:

$$\mathrm{Hom}_A(M, -) : {}_A\mathfrak{Mod} \to \mathfrak{Ab} \quad \text{e} \quad \mathrm{Hom}_A(-, N) : {}_A\mathfrak{Mod}^{op} \to \mathfrak{Ab};$$

2. para cada A-módulo à direita M e cada A-módulo à esquerda N, temos os funtores:

$$M \otimes_A - : {}_A\mathfrak{Mod} \to \mathfrak{Ab} \quad \text{e} \quad - \otimes_A N : \mathfrak{Mod}_A \to \mathfrak{Ab}.$$

1.4 Transformações naturais

Definição 9. Sejam C e $\mathcal{D}$ categorias e $\mathsf{F}, \mathsf{G} : C \to \mathcal{D}$ funtores. Uma transformação natural $\eta : \mathsf{F} \Rightarrow \mathsf{G}$ de F em G é uma família

$$\{\alpha_A : \mathsf{F}(A) \to \mathsf{G}(A)\}_{A \in C}$$

de morfismos em $\mathcal{D}$ indexada pelos objetos de C tal que para cada $f : A \to B$ em C o diagrama abaixo é comutativo

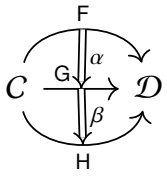
$$\begin{array}{ccc} \mathsf{F}(A) & \xrightarrow{\alpha_A} & \mathsf{G}(A) \\ {\scriptstyle \mathsf{F}(f)}\downarrow & & \downarrow{\scriptstyle \mathsf{G}(f)} \\ \mathsf{F}(B) & \xrightarrow[\alpha_B]{} & \mathsf{G}(B) \end{array}$$

Cada morfismo $\alpha_A : \mathsf{F}(A) \to \mathsf{G}(A)$ é chamado de componente da transformação natural α.

Exemplo 6. Dado um funtor $\mathsf{F} : C \to C$, existe uma transformação natural identidade $1_{\mathsf{F}} : \mathsf{F} \Rightarrow \mathsf{F}$ que possui como componentes os morfismos $(1_{\mathsf{F}})_A = 1_{\mathsf{F}(A)}$.

Definição 10. Sejam $\mathsf{F}, \mathsf{G}, \mathsf{H} : C \to \mathcal{D}$ funtores e $\alpha : \mathsf{F} \Rightarrow \mathsf{G}$ e $\beta : \mathsf{G} \Rightarrow \mathsf{H}$ transformações naturais. A transformação natural composta (ou composição) de α e β é denotada por $\beta \circ \alpha : \mathsf{F} \Rightarrow \mathsf{H}$ e possui como componentes os morfismos $(\beta \circ \alpha)_A = \beta_A \circ \alpha_A : \mathsf{F}(A) \to \mathsf{H}(A)$. Em geral, utilizaremos a notação simplificada $\beta\alpha$ ao invés de $\beta \circ \alpha$.

Graficamente, o contexto de uma composição de transformações naturais é representado pelo diagrama da esquerda. A naturalidade da composta decorre da naturalidade de cada transformação natural envolvida, representada pelo diagrama comutativo da direita.



$$\begin{array}{ccccc} \mathsf{F}(A) & \xrightarrow{\alpha_A} & \mathsf{G}(A) & \xrightarrow{\beta_A} & \mathsf{H}(A) \\ {\scriptstyle \mathsf{F}(f)}\downarrow & & \downarrow{\scriptstyle \mathsf{G}(f)} & & \downarrow{\scriptstyle \mathsf{H}(f)} \\ \mathsf{F}(B) & \xrightarrow[\alpha_B]{} & \mathsf{G}(B) & \xrightarrow[\beta_B]{} & \mathsf{H}(B) \end{array}$$

Definição 11. Uma transformação natural $\alpha : \mathsf{F} \Rightarrow \mathsf{G}$ é dita um isomorfismo natural quando existe uma transformação natural $\beta : \mathsf{G} \Rightarrow \mathsf{F}$ tal que

$$\beta\alpha = 1_{\mathsf{F}} \quad \text{e} \quad \alpha\beta = 1_{\mathsf{G}}.$$

Note que a definição de isomorfismo natural é análoga à de isomorfismo dentro de uma categoria, portanto os comentários feitos após a definição de isomorfismo se aplicam às transformações naturais também. Em particular, neste caso, dizemos que F e G são funtores isomorfos e escrevemos $\mathsf{F} \cong \mathsf{G}$.

Proposição 3. Uma transformação natural $\alpha : \mathsf{F} \Rightarrow \mathsf{G}$ é um isomorfismo natural se, e somente se, cada componente α_A, com $A \in C$ é um isomorfismo.

Demonstração. ($\Rightarrow$) Seja $\beta : \mathsf{G} \Rightarrow \mathsf{F}$ a transformação natural inversa de α, então para cada $A \in C$ temos que

$$1_{\mathsf{F}(A)} = (\beta\alpha)_A = \beta_A\alpha_A$$
$$1_{\mathsf{G}(A)} = (\alpha\beta)_A = \alpha_A\beta_A,$$

logo α_A é um isomorfismo com inversa β_A para cada $A \in C$.

($\Leftarrow$) Seja $\beta_A = (\alpha_A)^{-1}$ para cada $A \in C$, então temos que

$$1_{\mathsf{F}(A)} = \beta_A\alpha_A$$
$$1_{\mathsf{G}(A)} = \alpha_A\beta_A,$$

para cada $A \in C$.

Nos resta mostrar que $\beta = \{\beta_A\}_{A\in C}$ é uma transformação natural. Para isso seja $f : A \to B$ um morfismo em C, então

$$\begin{aligned} \mathsf{F}(f)\beta_A &= 1_{\mathsf{F}(A)}\mathsf{F}(A)\beta_A \\ &= \beta_B\alpha_B\mathsf{F}(f)\beta_A \\ &= \beta_B\mathsf{G}(f)\alpha_A\beta_A \\ &= \beta_B\mathsf{G}(f)1_{\mathsf{G}(A)} = \beta_B\mathsf{G}(f). \end{aligned}$$

□

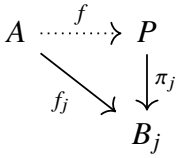
Dados funtores $\mathsf{F}, \mathsf{G} : C \to C$, dizemos que $\mathsf{F}(A) \cong \mathsf{G}(A)$ naturalmente em A quando F e G são funtores isomorfos.

Dado que funtores podem ser isomorfos, é possível relaxar a definição de isomorfismo de categorias e obter o conceito de equivalência de categorias.

Definição 12. Uma equivalência de categorias consiste em um par de funtores $\mathsf{F} : C \rightleftarrows \mathcal{D} : \mathsf{G}$ e isomorfismos naturais $\eta : 1_C \Rightarrow \mathsf{GF}$ e $\varepsilon : \mathsf{FG} \Rightarrow 1_{\mathcal{D}}$. Neste caso dizemos que C e $\mathcal{D}$ são categorias equivalentes e escrevemos $C \simeq \mathcal{D}$.

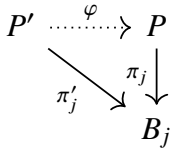
1.5 (Co)produtos e (co)equalizadores

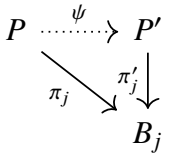
Definição 13. Seja $\{B_i\}_{i\in I}$ uma família de objetos de uma categoria C. Um produto dos objetos B_i é um par $(P; \{\pi_i\}_{i\in I})$ com $P \in C$ e $\pi_j : P \to B_j$ para cada $j \in I$ cumprindo a propriedade universal: para cada objeto A e morfismos $f_j : A \to B_j$ existe um único morfismo $f : A \to P$ tal que $\pi_j f = f_j$ para todo $j \in I$. Usualmente denominamos π_j por j-ésima projeção.



Proposição 4. Sejam $(P; \{\pi_i\}_{i\in I})$ e $(P'; \{\pi'_i\}_{i\in I})$ dois produtos da família $\{B_i\}_{i\in I}$. Então existe um único isomorfismo $\varphi : P' \to P$ tal que $\pi_j\varphi = \pi'_j$ para todo $j \in I$.

Demonstração. Para cada $j \in I$, usando as propriedades universais de P e P' obtemos a existência de φ e ψ, respectivamente, que tornam os diagramas abaixo comutativos.

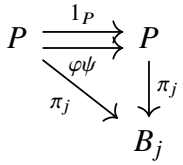


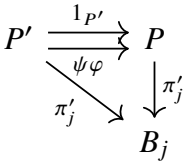


Como para cada $j \in I$ temos que

$$\pi_j\varphi\psi = \pi'_j\psi = \pi_j, \qquad \pi'_j\psi\varphi = \pi_j\varphi = \pi'_j,$$

então tanto 1_P quanto $\varphi\psi$ completam o primeiro diagrama comutativo abaixo e tanto $1_{P'}$ quanto $\psi\varphi$ completam o segundo diagrama comutativo abaixo.

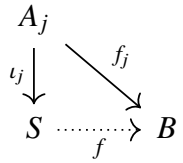




Segue da unicidade na definição de produto que $1_P = \varphi\psi$ e $1_{P'} = \psi\varphi$. □

Por conta dessa unicidade a menos de um único isomorfismo, podemos nos referir ao produto de um família $\{B_i\}_{i\in I}$ que será denotado por $\prod_{i\in I} B_i$, quando não houver dúvidas acerca das projeções. Denotaremos o produto de uma família finita $\{B_i\}_{i=1}^n$ por $B_1 \times \cdots \times B_n$, novamente quando não houver dúvidas acerca das projeções. Uma igualdade do tipo $P = \prod_{i\in I} B_i$ significa que foi feita a escolha de um objeto representante na classe de isomorfismos do produto.

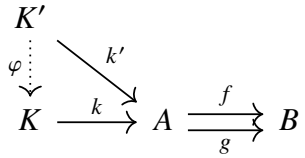
Definição 14. Seja $\{A_i\}_{i\in I}$ uma família de objetos de uma categoria C. Um coproduto dos objetos A_i é um par $(S; \{\iota_i\}_{i\in I})$ com $S \in C$ e $\iota_j : A_j \to S$ para cada $j \in I$ cumprindo a propriedade universal: para cada objeto B e morfismos $f_j : A_j \to B$ existe um único morfismo $f : S \to B$ tal que $f\iota_j = f_j$ para todo $j \in I$. Usualmente denominamos ι_j por j-ésima injeção.



Proposição 5. Sejam $(S; \{\iota_i\}_{i\in I})$ e $(S'; \{\iota'_i\}_{i\in I})$ dois coprodutos da família $\{A_i\}_{i\in I}$. Então existe um único isomorfismo $\psi : S' \to S$ tal que $\psi\iota'_j = \iota_j$ para todo $j \in I$.

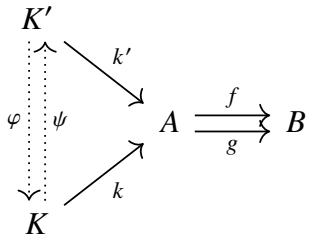
Por conta dessa unicidade a menos de um único isomorfismo, podemos nos referir ao coproduto de um família $\{A_i\}_{i\in I}$ que será denotado por $\coprod_{i\in I} A_i$, quando não houver dúvidas acerca das injeções. Denotaremos o coproduto de uma família finita $\{A_i\}_{i=1}^n$ por $A_1 + \cdots + A_n$, novamente quando não houver dúvidas acerca das injeções. Uma igualdade do tipo $S = \coprod_{i\in I} A_i$ significa que foi feita a escolha de um objeto representante na classe de isomorfismos do coproduto.

Definição 15. Sejam $f, g : A \to B$ morfismos paralelos. Um equalizador de f e g é um par $(K; k)$ com $K \in C$ e $k : K \to A$ tal que $fk = gk$, cumprindo a propriedade universal: para cada objeto K' e morfismo $k' : K' \to A$ tal que $fk' = gk'$ existe um único morfismo $\varphi : K' \to K$ tal que $k' = k\varphi$.



Proposição 6. Sejam $(K; k)$ e $(K'; k')$ dois equalizadores de f e g. Então existe um único isomorfismo $\varphi : K' \to K$ tal que $k\varphi = k'$.

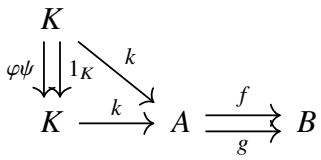
Demonstração. Usando as propriedades universais de $(K; k)$ e $(K'; k')$ obtemos a existência de φ e ψ, respectivamente, que tornam o diagrama abaixo comutativo.

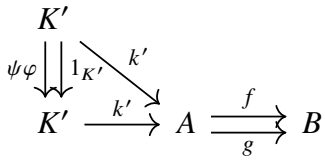


Como temos que

$$k\varphi\psi = k'\psi = k, \qquad\qquad k'\psi\varphi = k\varphi = k',$$

então tanto 1_K quanto $\varphi \circ \psi$ completam o primeiro diagrama comutativo abaixo e tanto $1_{K'}$ quanto $\psi \circ \varphi$ completam o segundo diagrama comutativo abaixo.



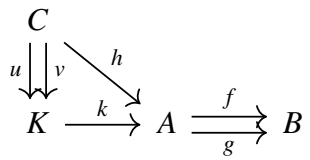


Segue da unicidade na definição de equalizador que $1_K = \varphi\psi$ e $1_{K'} = \psi\varphi$. □

Por conta dessa unicidade a menos de um único isomorfismo, podemos nos referir ao equalizador de f e g que será denotado por Equal(f, g). Dado que um equalizador é um par composto por um objeto e um morfismo , em alguns momentos nos referiremos apenas ao morfismo ou apenas ao objeto, desde que isto não gere dúvidas. Uma igualdade do tipo $K = \text{Equal}(f, g)$ significa que foi feita a escolha de um objeto representante na classe de isomorfismos do equalizador de f e g.

Proposição 7. Se $k = \text{Equal}(f, g)$, então k é um monomorfismo.

Demonstração. Sejam $u, v : C \to K$ dois morfismos tais que $ku = h = kv$, então temos que $fh = gh$. Assim, tanto u quanto v completam o diagrama comutativo abaixo.



Segue da unicidade na definição de equalizador que $u = v$. □

Proposição 8. Seja $f : A \to B$ um morfismo. Então Equal(f, f) sempre existe e é o par $(A; 1_A)$.

Demonstração. A prova segue diretamente da definição de equalizador. □

Proposição 9. Seja $k : K \to A$ um epimorfismo e equalizador. Então k é um isomorfismo.

Demonstração. Suponha que $(K; k)$ é o equalizador do par $f, g : A \to B$. Então $fk = gf$, mas k é um epimorfismo, logo $f = g$. Segue da proposição anterior e da Proposição 6 que existe um isomorfismo $k' : A \to K$ tal que $kk' = 1_A$, ou seja, k é um isomorfismo. □

Na presença de um objeto zero, o equalizador de um morfismo $f : A \to B$ e o morfismo zero $0 : A \to B$ é chamado de núcleo de f e denotado por $\mathrm{Ker}(f)$.

Proposição 10. Seja f um monomorfismo em uma categoria C com objeto zero 0. Se $fg = 0$ para algum morfismo g, então $g = 0$.

Demonstração. Se $fg = 0 = f0$, como f é um monomorfismo, temos que $g = 0$. □

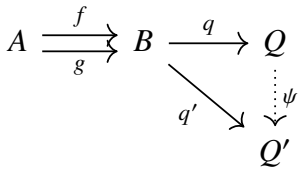
Proposição 11. Seja C uma categoria com objeto zero 0 e $f : A \to B$ um monomorfismo. Então $\mathrm{Ker}(f) = (0; 0)$.

Demonstração. Sabemos que $f0 = 0$. Agora, se $fg = 0$, pela proposição anterior segue que $g = 0$ e portanto g se fatora de maneira única pelo objeto 0. □

Proposição 12. Seja C uma categoria com objeto zero 0 e $0 : A \to B$ o morfismo zero. Então $\mathrm{Ker}(0) = (A; 1_A)$.

Demonstração. Sabemos que $01_A = 0$. Agora, se $g : K \to A$ é tal que $0g = 0$ (isso ocorre para qualquer g), então g se fatora de maneira única pela identidade de A como $g = 1_A g$ (isso também ocorre para qualquer g). □

Definição 16. Sejam $f, g : A \to B$ morfismos paralelos. Um coequalizador de f e g é um par $(Q; q)$ com $Q \in C$ e $q : B \to Q$ tal que $qf = qg$, cumprindo a propriedade universal: para cada objeto Q' e morfismo $q' : B \to Q'$ tal que $q'f = q'g$ existe um único morfismo $\psi : Q \to Q'$ tal que $\psi q = q'$.



Proposição 13. Sejam $(Q; q)$ e $(Q'; q')$ dois coequalizadores de f e g. Então existe um único isomorfismo $\psi : Q \to Q'$ tal que $\psi \circ q = q'$.

Por conta dessa unicidade a menos de um único isomorfismo, podemos nos referir ao coequalizador de f e g que será denotado por $\mathrm{Coequal}(f, g)$. Dado que um coequalizador é um par composto por um objeto e um morfismo , em alguns momentos nos referiremos apenas ao morfismo ou apenas ao objeto, desde que isto não gere dúvidas. Uma igualdade do tipo $Q = \mathrm{Coequal}(f, g)$ significa que foi feita a escolha de um objeto representante na classe de isomorfismos do coequalizador de f e g

Proposição 14. Se $q = \mathrm{Coequal}(f, g)$, então q é um epimorfismo.

Proposição 15. Seja $f : A \to B$ um morfismo. Então Coequal(f, f) sempre existe e é o par $(B, 1_B)$.

Proposição 16. Seja $q : B \to Q$ um monomorfismo e coequalizador. Então q é um isomorfismo.

Na presença de um objeto zero, o coequalizador de um morfismo $f : A \to B$ e o morfismo zero $0 : A \to B$ é chamado de conúcleo de f e denotado por Coker(f).

Proposição 17. Seja f um epimorfismo em uma categoria C com objeto zero 0. Se $gf = 0$ para algum morfismo g, então $g = 0$.

Proposição 18. Seja C uma categoria com objeto zero 0 e $f : A \to B$ um epimorfismo. Então Coker$(f) = (0; 0)$.

Proposição 19. Seja C uma categoria com objeto zero 0 e $0 : A \to B$ um morfismo zero. Então Coker$(0) = (B; 1_B)$.

CAPÍTULO

2

A CATEGORIA DE A-MÓDULOS

Neste capítulo, traduziremos os conceitos apresentados no capítulo anterior para o contexto de módulos sobre um anel. Além disso, daremos algumas propriedades e definições adicionais que nos serão úteis no decorrer do texto.

Na primeira seção, definiremos o conceito de módulos sobre um anel e apresentaremos algumas propriedades básicas, além das noções de submódulo e módulo quociente como casos particulares de equalizadores e coequalizadores. Na segunda seção construíremos o produto e o coproduto da categoria de módulos, na forma de somas e produtos diretos. Já na terceira e na quarta seções veremos a construção do grupo de homomorfismos e a construção do produto tensorial são funtores da categoria de módulos sobre um anel na categoria de grupos abelianos. Por fim, nas seções quinta e sexta definiremos módulos projetivos e injetivos, além de módulos livres e colivres, iniciando a nossa trajetória em direção à (co)homologia.

2.1 Definição e propriedades elementares

Durante este texto, ao nos referirmos a anéis estaremos considerando anéis que possuem unidade e não necessariamente são comutativos, naturalmente, ao falarmos de homomorfismos de anéis estaremos interessados naqueles que preservam unidades.

Denotaremos o centro de A por $Z(A) = \{a \in A; \forall b \in A, ab = ba\}$ e o subgrupo multiplicativo das unidades de A por $A^{\times} = \{a \in A; \exists b \in A, ba = 1_A = ab\}$. Além disso, A^{op} denotará o anel oposto de A que possui o mesmo grupo abeliano aditivo, mas cuja multiplicação é dada por $a \cdot_{op} b = b \cdot a$.

Definição 17. Seja A um anel. Um A-módulo à esquerda é um grupo abeliano (escrito aditiva-

mente) M juntamento com um homomorfismo de anéis

$$\varphi : A \to \mathrm{End}(M)$$
$$a \mapsto \varphi_a.$$

Denotaremos a imagem de $m \in M$ pelo endomorfismo φ_a por $\varphi_a(m) = a \cdot m$, ou simplesmente $\varphi_a(m) = am$.

É imediato da definição que o homomorfismo φ atua como uma multiplicação por escalar

$$\cdot : A \times M \to M$$
$$(a, m) \mapsto a \cdot m$$

que satisfaz os seguintes axiomas:

- $a_1 \cdot (a_2 \cdot m) = (a_1 a_2) \cdot m, \quad a_1, a_2 \in A, \quad m \in M$;
- $a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2, \quad a \in A, \quad m_1, m_2 \in M$;
- $(a_1 + a_2) \cdot m = a_1 \cdot m + a_2 \cdot m, \quad a_1, a_2 \in A, \quad m \in M$;
- $1_A \cdot m = m, \quad m \in M$.

Reciprocamente, dada uma função $\star : A \times M \to M$ que satisfaz os axiomas acima, obtemos um homomorfismo de anéis $\psi : A \to \mathrm{End}(M)$ que equipa M com estrutura de A-módulo à esquerda.

De maneira dual podemos definir um A-módulo à direita, no entanto, prova-se que todo A-módulo à direita é um A^{op}-módulo à esquerda. Desta maneira, trabalharemos apenas com A-módulos à esquerda, a menos que explicitado o contrário, e omitiremos o termo "à esquerda" sempre que não houver risco de ambiguidade.

Quando o anel A é comutativo, as noções de A-módulo à esquerda e A-módulo à direita coincidem, neste caso os termos "à esquerda" e "à direita" sempre poderão ser omitidos sem risco de ambiguidade.

Exemplo 7. Se $\mathbb{K}$ é um corpo, então V é um $\mathbb{K}$-módulo se, e somente se, V é um $\mathbb{K}$-espaço vetorial.

Exemplo 8. Se G é um grupo abeliano (escrito aditivamente), então G é um $\mathbb{Z}$-módulo com operação de multiplicação por escalar definida para $n \in \mathbb{Z}$ e $x \in G$ por

$$\begin{cases} 0x = 0; \\ nx = (n-1)x + x, & \text{se } n \geq 1; \\ nx = -((-n)x), & \text{se } n < 0. \end{cases}$$

A recíproca também é, por definição, verdadeira, se G é um $\mathbb{Z}$-módulo, então G é um grupo abeliano.

Exemplo 9. Seja A um anel e $I \subseteq A$ um ideal à esquerda, então I é um A-módulo à esquerda com a multiplicação por elementos de A na esquerda. Da mesma maneira, se $I \subseteq A$ é um ideal à direita, então I é um A-módulo à direita com a multiplicação por elementos de A na direita.

Exemplo 10. Seja A um anel comutativo. Então o anel de polinômios em qualquer número de indeterminadas com coeficientes em A, denotado por $A[X_1, \ldots, X_n]$ no caso de finitas indeterminadas e $A[X_1, X_2, \ldots]$ no caso de infinitas indeterminadas, é um A-módulo.

Definição 18. Sejam M e N A-módulos. Um A-homomorfismo de M em N é uma função $\varphi : M \to N$ que satisfaz

- $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2), \quad m_1, m_2 \in M$;
- $\varphi(am) = a\varphi(m), \quad a \in A, \quad m \in M$.

Exemplo 11. Se $\mathbb{K}$ é um corpo e V e W são $\mathbb{K}$-espaços vetoriais, então $T : V \to W$ é um $\mathbb{K}$-homomorfismo se, e somente se, T é uma $\mathbb{K}$-transformação linear.

Exemplo 12. Se G e H são grupos abelianos, então $\varphi : G \to H$ é um $\mathbb{Z}$-homomorfismo se, e somente se, φ é um homomorfismo de grupos.

Definição 19. Sejam A e B anéis. Um (A, B)-bimódulo é um grupo abeliano M que é um A-módulo à esquerda e um B-módulo à direita simultaneamente tal que

- $(am)b = a(mb), \quad a \in A, \quad b \in B, \quad m \in M$.

Definição 20. Um homomorfismo de (A, B)-bimódulos é um homomorfismo de A-módulos à esquerda que é simultaneamente um homomorfismo de B-módulos à direita.

Exemplo 13. Todo A-módulo M, tanto à esquerda como à direita, é um $(Z(A), Z(A))$-bimódulo via $am = ma$ para $m \in M$ e $a \in A$.

Observação 4. Para todo M um A-módulo, a função identidade Id_M de M é um A-homomorfismo. Além disso, se $\varphi : M \to N$ e $\psi : N \to P$ são A-homomorfismos, então $\psi\varphi : M \to P$ é um A-homomorfismo. Como a composição de funções é associativa, então a composição de A-homomorfismos é associativa. Isto prova que os A-módulos à esquerda, reciprocamente os A-módulos à direita, juntamente com os A-homomorfismos formam uma categoria, já citada anteriormente, que é denotada por ${}_A\mathfrak{Mod}$, reciprocamente $\mathfrak{Mod}_A$. Da mesma maneira, (A, B)-bimódulos juntamente com (A, B)-homomorfismos formam uma categoria denotada por ${}_A\mathfrak{Mod}_B$.

Definição 21. Seja M um A-módulo. Um A-submódulo N de M é um subgrupo aditivo $N \subseteq M$ que equipado com a mesma operação de multiplicação por escalar de M (restrita a N) é também

um A-módulo. Todo A-submódulo vem equipado com um A-homomorfismo injetor canônico de inclusão $N \to M$ dado por $n \mapsto n$.

Definição 22. Seja M um A-módulo e N um A-submódulo de M. O A-módulo quociente de M por N é o grupo abeliano quociente M/N equipado com a multiplicação por escalar

$$\begin{aligned} \cdot : A \times (M/N) &\to M/N \\ (a, \overline{m}) = (a, m + N) &\mapsto \overline{am} = am + N, \end{aligned}$$

que o torna também um A-módulo. Todo A-módulo quociente vem equipado com um A-homomorfismo sobrejetor canônico de projeção $M \to M/N$ dado por $m \mapsto m + N$.

Definição 23. Seja $\varphi : M \to N$ um A-homomorfismo. Então:

1. o núcleo de φ, denotado por $\mathrm{Ker}(\varphi)$ é o conjunto $\{m \in M; \varphi(m) = 0\}$;
2. a imagem de φ, denotada por $\mathrm{Img}(\varphi)$ é o conjunto $\{n \in N; \exists m \in M : \varphi(m) = n\}$;
3. o conúcleo de φ, denotado por $\mathrm{Coker}(\varphi)$ é o quociente $N/\mathrm{Img}(\varphi)$;
4. a coimagem de φ, denotada por $\mathrm{Coimg}(\varphi)$ é o quociente $M/\mathrm{Ker}(\varphi)$.

Proposição 20. Seja $\varphi : M \to N$ um A-homomorfismo. Então $\mathrm{Ker}(\varphi)$ é um A-submódulo de M e $\mathrm{Img}(\varphi)$ é um A-submódulo de N. Consequentemente $\mathrm{Coker}(\varphi)$ e $\mathrm{Coimg}(\varphi)$ são A-módulos.

Note que dado um morfismo $\psi : P \to M$ tal que $\varphi\psi = 0$, temos que $\mathrm{Img}(\psi) \subseteq \mathrm{Ker}(\varphi)$, portanto ψ pode ser fatorado de maneira única pelo núcleo de φ. Isto prova que o A-módulo $\mathrm{Ker}(\varphi)$ juntamente com a sua inclusão em M é o núcleo no sentido categórico.

$$P \longrightarrow \mathrm{Ker}(\varphi) \rightarrowtail M$$

$$p \longmapsto p \longmapsto \psi(p)$$

Da mesma maneira, se $\psi : N \to P$ é tal que $\psi\varphi = 0$, temos que $\mathrm{Img}(\varphi) \subseteq \mathrm{Ker}(\psi)$, portanto ψ pode ser fatorado de maneira única pelo conúcleo de φ. Novamente, isto prova que o A-módulos $\mathrm{Coker}(\varphi)$ juntamente com a sua projeção de N é o conúcleo no sentido categórico.

$$M \twoheadrightarrow \mathrm{Coker}(\varphi) \longrightarrow P$$

$$m \longmapsto m + \mathrm{Ker}(\varphi) \longmapsto \psi(m)$$

Interpretando os conceitos de monorfismo e epimorfismo na categoria de A-módulos (à esquerda ou à direita) obtemos a proposição abaixo.

Proposição 21. Seja A um anel e $\varphi : M \to N$ um A-homomorfismo. Então

1. φ é um monomorfismo se, e somente se, φ é injetor;
2. φ é um epimorfismo se, e somente se, φ é sobrejetor;
3. φ é um isomorfismo se, e somente se, φ é bijetor.

Demonstração. 1. ($\Rightarrow$): Considere os morfismos nulo e inclusão $0, \iota : \mathrm{Ker}(\varphi) \to M$. Temos que $\varphi\iota = \varphi 0$, então $\iota = 0$ e $\mathrm{Ker}(\varphi) = 0$, isto é, φ é injetivo.

1.($\Leftarrow$): Sejam $\alpha, \beta : M' \to M$ A-homomorfismos tais que $\varphi\alpha = \varphi\beta$ e $m' \in M'$. Então

$$\varphi(\alpha(m')) = \varphi(\beta(m')) \Rightarrow \alpha(m') = \beta(m'),$$

logo $\alpha = \beta$ e φ é monomorfismo.

2.($\Rightarrow$): Considere os morfismos nulo e projeção $0, \pi : N \to \mathrm{Coker}(\varphi)$. Temos que $\pi\varphi = 0\varphi$, então $\pi = 0$ e $\mathrm{Coker}(\varphi) = 0$, isto é, φ é sobrejetor.

2.($\Leftarrow$): Sejam $\alpha, \beta : N \to N'$ A-homomorfismos tais que $\alpha\varphi = \beta\varphi$ e $n \in N$. Da hipótese existe $m \in M$ tal que $\varphi(m) = n$, então

$$\alpha(n) = \alpha(\varphi(m')) = \beta(\varphi(m')) = \beta(n),$$

logo $\alpha = \beta$ e φ é epimorfismo.

3.($\Rightarrow$): Sendo isomorfismo, segue que φ é monomorfismo e epimorfismo. Pelos itens anteriores segue que φ é injetor e sobrejetor, logo bijetor.

3.($\Leftarrow$): Sendo bijetor, φ tem uma função inversa $\psi : N \to M$. Agora, se $n_1, n_2 \in N$ e $a \in A$, então existem $m_1, m_2 \in M$ tais que $\varphi(m_1) = n_1$ e $\varphi(m_2) = n_2$, assim

$$\psi(an_1 + n_2) = \psi(\varphi(am_1 + m_2)) = am_1 + m_2 = a\psi(m_1) + \psi(m_2),$$

logo ψ é um A-homomorfismo e junto com φ forma um par de isomorfismos. □

Teorema 1 (Teorema do Isomorfismo). Seja $\varphi : M \to N$ um A-homomorfismo. Então

$$\mathrm{Coimg}(\varphi) \cong \mathrm{Img}(\varphi).$$

Demonstração. Defina $\tilde{\varphi} : \mathrm{Coimg}(\varphi) \to \mathrm{Img}(\varphi)$ dado por $\tilde{\varphi}(m + \mathrm{Ker}(\varphi)) = \varphi(m)$ para $m \in M$. □

Definição 24. Uma sequência de módulos e homomorfismos

$$M_0 \xrightarrow{\varphi_0} M_1 \xrightarrow{\varphi_1} \cdots \xrightarrow{\varphi_{n-1}} M_n \xrightarrow{\varphi_n} M_{n+1}$$

é dita exata em M_j, com $1 \leq j \leq n$, quando $\mathrm{Img}(\varphi_{j-1}) = \mathrm{Ker}(\varphi_j)$. Esta sequência é dita exata quando for exata em M_j para todo $1 \leq j \leq n$.

Uma sequência exata do tipo

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

é chamada de sequência exata curta.

Exemplo 14. Como consequência imediata da definição temos:

1. $0 \longrightarrow M \xrightarrow{\varphi} N$ é exata se, e somente se, φ é injetivo;
2. $M \xrightarrow{\psi} N \longrightarrow 0$ é exata se, e somente se, ψ é sobrejetivo;
3. se $\varphi : M \to N$ é um A-homomorfismo, então as sequências abaixo são exatas

   $0 \longrightarrow \mathrm{Ker}(\varphi) \xrightarrow{\iota} M \xrightarrow{\pi} M/\mathrm{Ker}(\varphi) \longrightarrow 0$

   $0 \longrightarrow \mathrm{Img}(\varphi) \xrightarrow{\mu} N \xrightarrow{\varepsilon} N/\mathrm{Img}(\varphi) \longrightarrow 0$

2.2 Somas e produtos

A partir de agora, deixaremos de explicitar o anel sobre o qual os módulos estão sendo construídos sempre que não houver risco de confusão.

Nesta seção definiremos somas e produtos diretos de uma família de módulos, em seguida, demonstraremos as suas respectivas propriedades universais que os caracterizam como o coproduto e o produto na categoria de módulos.

Definição 25. Seja $\{M_j\}_{j\in J}$ uma família de A-módulos. A soma direta dos módulos M_j é o módulo denotado por

$$\bigoplus_{j\in J} M_j$$

cujos elementos são famílias $(x_j)_{j\in J}$ tais que $x_j \in M_j$ para todo $j \in J$ e $x_j \neq 0$ apenas para um número finito de índices. A adição e a multiplicação por escalar são dadas coordenada a coordenada, isto é, se $(x_j)_{j\in J}, (y_j)_{j\in J} \in \bigoplus_{j\in J} M_j$ e $a \in A$, então

$$(x_j)_{j\in J} + (y_j)_{j\in J} = (x_j + y_j)_{j\in J} \quad \text{e} \quad a(x_j)_{j\in J} = (ax_j)_{j\in J}.$$

Para cada $k \in J$, a k-ésima injeção é o homomorfismo

$$\iota_k : M_k \to \bigoplus_{j\in J} M_j$$

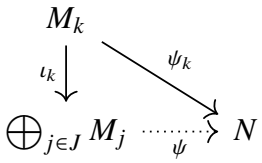
que leva um elemento $m_k \in M_k$ na família $(x_j)_{j\in J}$ tal que $x_k = m_k$ e $x_j = 0$ para $j \neq k$.

A soma direta juntamente com as injeções cumpre a propriedade universal abaixo.

Teorema 2 (Propriedade Universal da Soma Direta)**.** Sejam N um módulo e $\{\psi_j : M_j \to N\}_{j\in J}$ uma família de homomorfismos. Então existe um único homomorfismo

$$\psi : \bigoplus_{j\in J} M_j \to N \quad \text{tal que} \quad \psi\iota_k = \psi_k \quad \text{para todo } k \in J.$$

Tal propriedade pode ser visualizada mais facilmente através do diagrama abaixo, ela afirma que existe ψ, representado pela flecha tracejada, tal que para cada $k \in J$, o diagrama abaixo é comutativo.



Demonstração. Defina $\psi : \bigoplus_{j\in J} M_j \to N$ dado por $\psi((m_j)_{j\in J}) = \sum_{j\in J} \psi_j(m_j)$. □

Desta maneira a soma direta juntamente com as injeções está totalmente caracterizada a menos de um único isomorfismo, isto é, se existe outro módulo S e outra família de homomorfismos que cumprem a mesma propriedade universal, então a soma direta definida como acima e o módulo S são isomorfos de uma única maneira possível e este isomorfismo é compatível com as injeções e os homomorfismos dados.

Definição 26. Seja $\{N_j\}_{j\in J}$ uma família de módulos. O produto direto dos módulos N_j é o módulo denotado por

$$\prod_{j\in J} N_j$$

cujos elementos são famílias $(x_j)_{j\in J}$ tais que $x_j \in N_j$ para todo $j \in J$ (sem nenhuma outra restrição). A adição e a multiplicação por escalar são dadas coordenada a coordenada, isto é, se $(x_j)_{j\in J}, (y_j)_{j\in J} \in \prod_{j\in J} N_j$ e $a \in A$, então

$$(x_j)_{j\in J} + (y_j)_{j\in J} = (x_j + y_j)_{j\in J} \quad \text{e} \quad a(x_j)_{j\in J} = (ax_j)_{j\in J}.$$

Para cara $k \in J$, a k-ésima projeção é o homomorfismo

$$\pi_k : \prod_{j\in J} N_j \to N_k$$

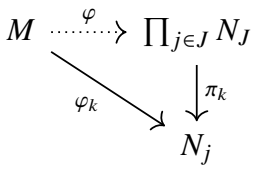
que leva uma família $(x_j)_{j\in J}$ no elemento $x_k \in N_k$.

Note que se J for finito, então a soma e o produto direto coincidem. O produto direto juntamente com as projeções cumpre a propriedade universal abaixo.

Teorema 3 (Propriedade Universal do Produto Direto)**.** Sejam M um módulo e $\{\varphi_j : M \to N_j\}_{j\in J}$ uma família de homomorfismos. Então existe um único homomorfismo

$$\varphi : M \to \prod_{j\in J} N_j \quad \text{tal que} \quad \pi_k\varphi = \varphi_k \quad \text{para todo } k \in J.$$

Tal propriedade pode ser visualizada mais facilmente através do diagrama abaixo, ela afirma que existe φ, representado pela flecha tracejada, tal que para cada $k \in J$, o diagrama abaixo é comutativo.



Demonstração. Defina $\varphi : M \to \prod_{j\in J} N_j$ dado por $\varphi(m) = (\varphi_j(m))_{j\in J}$ para $m \in M$. □

Assim como para a soma direta, o produto direto juntamente com as projeções está totalmente caracterizado a menos de um único isomorfismo, isto é, se existe outro módulo T e outra família de homomorfismos que cumprem a mesma propriedade universal, então o produto direto construído acima e o módulo T são isomorfos de uma maneira única, além disso, esse isomorfismo é compatível com as projeções e os homomorfismos dados.

2.3 O funtor grupo de homomorfismos

Nesta seção construiremos o grupo abeliano de A-homomorfismos entre dois A-módulos à esquerda ou dois A-módulos à direita e estudaremos sua relação com somas diretas, produtos diretos e sequências exatas.

Definição 27. Sejam M e N A-módulos. O grupo abeliano de homomorfismos de M em N será denotado por $\mathrm{Hom}_A(M, N)$. A adição é definida ponto a ponto

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m), \quad \varphi, \psi \in \mathrm{Hom}_A(M, N), \quad m \in M$$

No caso particular em que $A = \mathbb{Z}$ denotaremos $\mathrm{Hom}_{\mathbb{Z}}(M, N) = \mathrm{Hom}(M, N)$.

Exemplo 15. Sejam $m, n \in \mathbb{N}$. Se $d = \mathrm{mdc}(m, n)$, então:

$$\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}.$$

Seja $L : \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/d\mathbb{Z}$ dada para $f \in \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$, tal que $f(1 + m\mathbb{Z}) = k + n\mathbb{Z}$, por

$$L(f) = k + d\mathbb{Z}.$$

Para mostrar que L é um $\mathbb{Z}$-homomorfismo sejam $a, b \in \mathbb{Z}$ e $f, g \in \mathrm{Hom}\,(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ tais que $f(1 + m\mathbb{Z}) = k + n\mathbb{Z}$ e $g(1 + m\mathbb{Z}) = l + n\mathbb{Z}$, então

$$\begin{aligned} L(af + bg) &= (af + bg)(1 + m\mathbb{Z}) \\ &= af(1 + m\mathbb{Z}) + bg(1 + m\mathbb{Z}) \\ &= a(k + n\mathbb{Z}) + b(l + n\mathbb{Z}) \\ &= aL(f) + bL(g). \end{aligned}$$

Agora note que sendo $\mathbb{Z}/m\mathbb{Z}$ cíclico, temos que qualquer $\mathbb{Z}$-homomorfismo de $\mathbb{Z}/m\mathbb{Z}$ em $\mathbb{Z}/n\mathbb{Z}$ é unicamente determinado pela imagem de $1 + m\mathbb{Z}$, desta maneira, se $f, g \in \mathrm{Hom}\,(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ são tais que $f \neq g$, então $L(f) = f(1 + m\mathbb{Z}) \neq g(1 + m\mathbb{Z}) = L(g)$ e portanto L é injetor.

Por fim, dado $k + d\mathbb{Z} \in \mathbb{Z}/d\mathbb{Z}$ podemos definir

$$f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

dada por $f(1 + m\mathbb{Z}) = k + n\mathbb{Z}$ e assim teremos $L(f) = k + d\mathbb{Z}$. Portanto, L é sobrejetor e segue o isomorfismo.

Observação 5. Sob algumas condições, $\mathrm{Hom}_A\,(M, N)$ pode ter mais estrutura:

1. se M é um (A, B)-bimódulo e N é um A-módulo à esquerda, então $\mathrm{Hom}_A\,(M, N)$ é um B-módulo à esquerda via

$$(b\varphi)(m) = \varphi(mb), \quad b \in B, \quad \varphi \in \mathrm{Hom}_A\,(M, N), \quad m \in M;$$

2. se M é um (B, A)-bimódulo e N é um A-módulo à direita, então $\mathrm{Hom}_A\,(M, N)$ é um B-módulo à direita via

$$(\varphi b)(m) = \varphi(bm), \quad b \in B, \quad \varphi \in \mathrm{Hom}_A\,(M, N), \quad m \in M;$$

3. se M é um A-módulo à esquerda e N é um (A, B)-bimódulo, então $\mathrm{Hom}_A\,(M, N)$ é um B-módulo à direita via

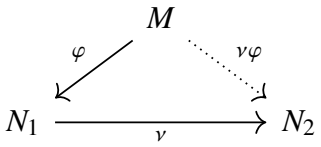
$$(\varphi b)(m) = (\varphi(m))b, \quad b \in B, \quad \varphi \in \mathrm{Hom}_A\,(M, N), \quad m \in M;$$

4. se M é um A-módulo à direita e N é um (B, A)-bimódulo, então $\mathrm{Hom}_A\,(M, N)$ é um B-módulo à esquerda via

$$(b\varphi)(m) = b(\varphi(m)), \quad b \in B, \quad \varphi \in \mathrm{Hom}_A\,(M, N), \quad m \in M.$$

Na sequência, construiremos homomorfismos de grupo induzidos por A-homomorfismos. Seja $\nu : N_1 \to N_2$ um A-homomorfismo, então para cada A-homomorfismo $\varphi : M \to N_1$ podemos associar um A-homomorfismo $\nu\varphi : M \to N_2$. Esta associação $\varphi \mapsto \nu\varphi$ é um homomorfismo de grupos.

$$\begin{aligned} \nu_* : \mathrm{Hom}_A(M, N_1) &\to \mathrm{Hom}_A(M, N_2) \\ \varphi &\mapsto \nu_*(\varphi) = \nu\varphi. \end{aligned}$$

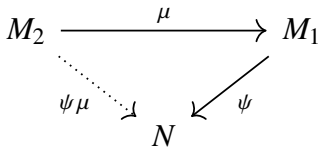


Observação 6. Além disso, valem as seguintes propriedades:

1. se $\nu : N_1 \to N_2$ e $\nu' : N_2 \to N_3$, então
$$(\nu'\nu)_* = \nu'_*\nu_* : \mathrm{Hom}_A(M, N_1) \to \mathrm{Hom}_A(M, N_3);$$
2. se $\nu : N \to N$ é a identidade, então $\nu_* : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N)$ é a identidade também;
3. se $\nu, \nu' : N_1 \to N_2$, então $(\nu + \nu')_* = \nu_* + \nu'_* : \mathrm{Hom}_A(M, N_1) \to \mathrm{Hom}_A(M, N_2)$;
4. se $N = 0$, então $\mathrm{Hom}_A(M, N) = 0$;
5. se $\nu = 0 : N_1 \to N_2$, então $\nu_* = 0_* = 0 : \mathrm{Hom}_A(M, N_1) \to \mathrm{Hom}_A(M, N_2)$.

Por outro lado, seja $\mu : M_2 \to M_1$ um A-homomorfismo, então para cada A-homomorfismo $\psi : M_1 \to N$ podemos associar um A-homomorfismo $\psi\mu : M_2 \to N$. Esta associação $\psi \mapsto \psi\mu$ é um homomorfismo de grupos.

$$\begin{aligned} \mu^* : \mathrm{Hom}_A(M_1, N) &\to \mathrm{Hom}_A(M_2, N) \\ \psi &\mapsto \mu^*(\psi) = \psi\mu. \end{aligned}$$



Observação 7. Além disso, valem as seguintes propriedades:

1. se $\mu : M_3 \to M_2$ e $\mu' : M_2 \to M_1$, então
$$(\mu'\mu)^* = \mu^*\mu'^* : \mathrm{Hom}_A(M_1, N) \to \mathrm{Hom}_A(M_3, N);$$
2. se $\mu : M \to M$ é a identidade, então $\mu^* : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N)$ é a identidade também;
3. se $\mu, \mu' : M_2 \to M_1$, então $(\mu + \mu')^* = \mu^* + \mu'^* : \mathrm{Hom}_A(M_1, N) \to \mathrm{Hom}_A(M_2, N)$;
4. se $M = 0$, então $\mathrm{Hom}_A(M, N) = 0$;
5. se $\mu = 0 : M_2 \to M_1$, então $\mu^* = 0^* = 0 : \mathrm{Hom}_A(M_1, N) \to \mathrm{Hom}_A(M_2, N)$.

Proposição 22. Seja

$$0 \longrightarrow N' \xrightarrow{\varphi} N \xrightarrow{\psi} N''$$

uma sequência exata de A-módulos. Então para cada A-módulo M, a sequência de grupos abelianos induzida abaixo é exata:

$$0 \longrightarrow \mathrm{Hom}_A(M, N') \xrightarrow{\varphi_*} \mathrm{Hom}_A(M, N) \xrightarrow{\psi_*} \mathrm{Hom}_A(M, N'')$$

Demonstração. Primeiramente tome $\alpha : M \to N'$ tal que $\varphi_*(\alpha) = 0$, então $\varphi(\alpha(m)) = 0$ para todo $m \in M$, da injetividade de φ temos que $\alpha(m) = 0$ para todo $m \in M$, logo $\alpha = 0$ e portanto φ_* é injetivo.

Agora tome $\beta : M \to N$ tal que $\beta = \varphi_*(\alpha) = \varphi\alpha$ para algum $\alpha : M \to N'$, então $\psi_*(\beta) = \psi\beta = \psi\varphi\alpha = 0\alpha = 0$, portanto $\mathrm{Img}(\varphi_*) \subseteq \mathrm{Ker}(\psi_*)$.

Por fim tome $\beta : M \to N$ tal que $\psi * (\beta) = 0$, logo $\psi(\beta(m)) = 0$ para todo $m \in M$, isto é, $\beta(m) \in \mathrm{Ker}(\psi) = \mathrm{Img}(\varphi)$ para todo $m \in M$, assim, da injetividade de φ, para cada $m \in M$ existe um único $n' \in N'$ tal que $\beta(m) = \varphi(n')$, defina $\alpha : M \to N'$ dado por $\alpha(m) = n'$, então temos $\beta = \varphi\alpha = \varphi_*(\alpha)$, portanto $\mathrm{Ker}(\psi_*) \subseteq \mathrm{Img}(\varphi)$. □

Proposição 23. Seja

$$M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

uma sequência exata de A-módulos. Então para cada A-módulo N, a sequência de grupos abelianos induzida abaixo é exata:

$$0 \longrightarrow \mathrm{Hom}_A(M'', N) \xrightarrow{\psi_*} \mathrm{Hom}_A(M, N) \xrightarrow{\varphi_*} \mathrm{Hom}_A(M', N)$$

Demonstração. Primeiramente tome $\alpha : M'' \to N$ tal que $\psi^*(\alpha) = 0$, então $\alpha(\psi(m)) = 0$ para todo $m \in M$, da sobrejetividade de ψ temos que $\alpha(m'') = 0$ para todo $m'' \in M''$, logo $\alpha = 0$ e portanto ψ^* é injetivo.

Agora tome $\beta : M \to N$ tal que $\beta = \psi^*(\alpha)$ para algum $\alpha : M'' \to N$, então $\varphi^*(\beta) = \beta\varphi = \alpha\psi\varphi = \alpha 0 = 0$, portanto $\mathrm{Img}(\psi^*) \subseteq \mathrm{Ker}(\varphi^*)$.

Por fim tome $\beta : M \to N$ tal que $\varphi^*(\beta) = 0$, logo $\beta(\varphi(m')) = 0$ para todo $m' \in M'$. Da sobrejetividade de ψ, para cada $m'' \in M''$ existe $m \in M$ tal que $m'' = \psi(m)$, assim, defina $\alpha : M'' \to N$ dado por $\alpha(m'') = \beta(m)$. Note que α está bem definido, pois se $\psi(m_1) = m'' = \psi(m_2)$, então $\psi(m_1 - m_2) = 0$, logo $m_1 - m_2 \in \mathrm{Ker}(\psi) = \mathrm{Img}(\varphi)$ e assim $m_1 - m_2 = \varphi(m')$ para algum $m' \in M'$, logo $\beta(m_1) - \beta(m_2) = \beta(m_1 - m_2) = \beta(\varphi(m')) = 0$, isto é, $\beta(m_1) = \beta(m_2)$. Segue que $\beta = \alpha\psi = \psi^*(\alpha)$, portanto $\mathrm{Ker}(\varphi^*) \subseteq \mathrm{Img}(\psi^*)$. □

Proposição 24. Sejam N um módulo e $\{M_j\}_{j\in J}$ uma família de módulos. Então existe um isomorfismo de grupos

$$\mathrm{Hom}_A\left(\bigoplus_{j\in J} M_j, N\right) \cong \prod_{j\in J} \mathrm{Hom}_A\left(M_j, N\right).$$

Demonstração. Por um lado defina $f \mapsto (f\iota_j)_{j\in J}$, com $\iota_i : M_i \to \bigoplus_{j\in J} M_j$ as injeções da soma direta. Por outro lado defina $(g_j)_{j\in J} \mapsto g$, com g dada pela propriedade universal da soma direta. Claramente temos homomorfismos de grupos inversos um do outro, portanto segue o isomorfismo desejado. □

Proposição 25. Sejam M um módulo e $\{N_j\}_{j\in J}$ uma família de módulos. Então existe um isomorfismo de grupos

$$\mathrm{Hom}_A\left(M, \prod_{j\in J} N_j\right) \cong \prod_{j\in J} \mathrm{Hom}_A\left(M, N_j\right).$$

Demonstração. Por um lado defina $f \mapsto (\pi_j f)_{j\in J}$, com $\pi_i : \prod_{j\in J} N_j \to N_i$ as projeções do produto direto. Por outro lado defina $(g_j)_{j\in J} \mapsto g$, com g dada pela propriedade universal do produto direto. Claramente temos homomorfismos de grupos inversos um do outro, portanto segue o isomorfismo desejado. □

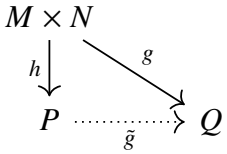
2.4 O funtor produto tensorial

Agora voltaremos a nossa atenção ao produto tensorial de A-módulos e estudaremos sua relação com somas diretas, produtos diretos e sequências exatas.

Definição 28. Sejam M um A-módulo à direita, N um A-módulo à esquerda e P um grupo abeliano. Uma função $f : M \times N \to P$ é dita A-biaditiva quando

- $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$ para todo $m_1, m_2 \in M$, $n \in N$;
- $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$ para todo $m \in M$, $n_1, n_2 \in N$;
- $f(ma, n) = f(m, an)$ para todo $a \in A$, $m \in M$, $n \in N$.

Definição 29. Sejam M um A-módulo à direita e N um A-módulo à esquerda. Um produto tensorial de M e N é um grupo abeliano P juntamente com uma função A-biaditiva $h : M\times N \to P$ tal que para todo grupo abeliano Q e toda função A-biaditiva $g : M \times N \to Q$ existe um único homomorfismo de grupos $\tilde{g} : P \to Q$ tal que $\tilde{g}h = g$.



Teorema 4. O produto tensorial de M e N existe.

Demonstração. Denote por $F(M \times N)$ o grupo abeliano livre gerado pelo produto cartesiano $M \times N$ e G o subgrupo de $F(M \times N)$ gerado pelos elementos da forma

- $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$, com $m_1, m_2 \in M$, $n \in N$;
- $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$, com $m \in M$, $n_1, n_2 \in N$;
- $(ma, n) - (m, an)$, com $a \in A$, $m \in M$, $n \in N$.

Afirmamos que o quociente $P = F(M \times N)/G$ juntamente com a aplicação A-biaditiva $p : M \times N \to F(M \times N) \to F(M \times N)/G$ é um produto tensorial de M e N. Denotaremos a imagem de $(m, n) \in M \times N$ por $m \otimes n$, desta maneira os elementos de P podem ser escritos, de maneira não necessariamente única, como $\sum_{i=1}^{k} m_i \otimes n_i$ com $m_i \in M$ e $n_i \in N$ para todo $i = 1, \ldots, k$.

Seja Q um grupo abeliano e $q : M \times N \to Q$ uma aplicação A-biaditiva, então definimos $\tilde{q} : P \to Q$ dada por $\tilde{q}\left(\sum_{i=1}^{k} m_i \otimes n_i\right) = \sum_{i=1}^{k} q(m_i, n_i)$. Claramente temos que $\tilde{q}$ é um homomorfismo de grupos tal que $\tilde{q}p = q$.

Agora, se $q' : P \to Q$ é um homomorfismo de grupos tal que $q'p = q$, então

$$\begin{aligned} q'\left(\sum_{i=1}^{k} m_i \otimes n_i\right) &= \sum_{i=1}^{k} q'(m_i \otimes n_i) \\ &= \sum_{i=1}^{k} q'(p(m_i, n_i)) \\ &= \sum_{i=1}^{k} q(m_i, n_i) \\ &= \tilde{q}\left(\sum_{i=1}^{k} m_i \otimes n_i\right), \end{aligned}$$

isto é, $q' = \tilde{q}$. □

Como o produto tensorial existe e cumpre uma propriedade universal, então, como já vimos várias vezes, este objeto juntamente com os morfismos adequados está unicamente determinado a menos de um único isomorfismo.

No caso particular em que $A = \mathbb{Z}$ denotaremos $M \otimes_{\mathbb{Z}} N = M \otimes N$.

Exemplo 16. Sejam $m, n \in \mathbb{N}$. Se $d = \text{mdc}(m, n)$, então:

$$\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}.$$

Observação 8. Sob algumas condições, $M \otimes_A N$ pode ter mais estrutura:

1. se M é um (B, A)-bimódulo, então $M \otimes_A N$ é um B-módulo à esquerda via

$$b(m \otimes n) = bm \otimes n, \quad b \in B, \quad m \in M, \quad n \in N;$$

2. se N é um (A, B)-bimódulo, então $M \otimes_A N$ é um B-módulo à direita via

$$(m \otimes n)b = m \otimes nb, \quad b \in B, \quad m \in M, \quad n \in N.$$

Em certo sentido, o produto tensorial é comutativo, associativo e possui elemento neutro. De maneira explícita temos os resultados abaixo que podem ser encontrados em Atiyah e MacDonald (1969, p. 26).

Observação 9. Sejam M um A-módulo à direita e N um A-módulo à esquerda. Então existem isomorfismos de grupos:

$$M \otimes_A N \cong N \otimes_{A^{op}} M;$$

$$M \cong M \otimes_A A;$$

$$N \cong A \otimes_A N.$$

Se M é um A-módulo à direita, N um (A, B)-bimódulo e P um B-módulo à esquerda então

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P).$$

Na sequência, construiremos homomorfismos de grupos induzidos por A-homomorfismos.

Seja $\nu : N_1 \to N_2$ um homomorfismo de A-módulos à esquerda, então temos um homomorfismo de grupos $Id_M \otimes_A \nu : M \otimes_A N_1 \to M \otimes_A N_2$ tal que $(Id_M \otimes_A \nu)(m \otimes n_1) = m \otimes \nu(n_1)$, $m \in M$, $n_1 \in N_1$.

Observação 10. Além disso, valem as seguintes propriedades:

1. se $\nu : N_1 \to N_2$ e $\nu' : N_2 \to N_3$, então

$$Id_M \otimes_A (\nu'\nu) = (Id_M \otimes_A \nu')(Id_M \otimes_A \nu) : M \otimes_A N_1 \to M \otimes_A N_3;$$

2. se $\nu : N \to N$ é a identidade, então $Id_M \otimes_A \nu : M \otimes_A N \to M \otimes_A N$ é a identidade também;

3. se $\nu, \nu' : N_1 \to N_2$, então $Id_M \otimes_A (\nu + \nu') = Id_M \otimes_A \mu + Id_M \otimes_A \mu' : M \otimes_A N_1 \to M \otimes_A N_2$;

4. se $N = 0$, então $M \otimes_A N = 0$;

5. se $\nu = 0 : N_1 \to N_2$, então $Id_M \otimes_A \nu = Id_M \otimes_A 0 = 0 : M \otimes_A N_1 \to M \otimes_A N_2$.

Por outro lado, seja $\mu : M_1 \to M_2$ um homomorfismo de A-módulos à direita, então temos um homomorfismo de grupos $\mu \otimes_A Id_N : M_1 \otimes_A N \to M_2 \otimes_A N$ tal que $(\mu \otimes_A Id_N)(m_1 \otimes n) = \mu(m_1) \otimes n$, $m_1 \in M_1$, $n \in N$.

Observação 11. Além disso, valem as seguintes propriedades:

1. se $\mu : M_1 \to M_2$ e $\mu' : M_2 \to M_3$, então

$$(\mu'\mu) \otimes_A Id_N = (\mu' \otimes_A Id_N)(\mu \otimes_A Id_N) : M_1 \otimes_A N \to M_3 \otimes_A N;$$

2. se $\mu : M \to M$ é a identidade, então $\mu \otimes_A Id_N : M \otimes_A N \to M \otimes_A N$ é a identidade também;

3. se $\mu, \mu' : M_1 \to M_2$, então $(\mu+\mu') \otimes_A Id_N = \nu \otimes_A Id_N + \nu' \otimes_A Id_N : M_1 \otimes_A N \to M_2 \otimes_A N$;

4. se $M = 0$, então $M \otimes_A N = 0$;

5. se $\mu = 0 : M_1 \to M_2$, então $\mu \otimes_A Id_N = 0 \otimes_A Id_N = 0 : M_1 \otimes_A N \to M_2 \otimes_A N$.

Proposição 26. Seja

$$N' \xrightarrow{\varphi} N \xrightarrow{\psi} N'' \longrightarrow 0$$

uma sequência exata de A-módulos à esquerda. Então para cada A-módulo à direita M, a sequência de grupos abelianos induzida abaixo é exata:

$$M \otimes_A N' \xrightarrow{Id_M \otimes_A \varphi} M \otimes_A N \xrightarrow{Id_M \otimes_A \psi} M \otimes_A N'' \longrightarrow 0$$

Demonstração. Como

$$Id_M \otimes_A \psi Id_M \otimes_A \varphi = (Id_M Id_M) \otimes_A (\psi\varphi) = Id_M \otimes_A 0 = 0,$$

então $\mathrm{Img}(Id_M \otimes_A \varphi) \subseteq \mathrm{Ker}(Id_M \otimes_A \psi)$.

Do que foi provado acima, temos que $Id_M \otimes_A \psi$ induz um homomorfismo

$$\overline{\psi} : \frac{M \otimes_A N}{\mathrm{Img}(Id_M \otimes_A \varphi)} \to M \otimes_A N''$$

dado por $\overline{\psi}(m \otimes n + \mathrm{Img}(Id_M \otimes_A \varphi)) = m \otimes \psi(n)$. Denotando por

$$\pi : M \otimes_A N \to \frac{M \otimes_A N}{\mathrm{Img}(Id_M \otimes_A \varphi)}$$

a projeção natural, temos que $\overline{\psi}\pi = Id_M \otimes_A \psi$, já que

$$(\overline{\psi}\pi)(m \otimes n) = m \otimes \psi(n) = (Id_M \otimes_A \psi)(m \otimes n).$$

Definimos agora

$$\rho : M \times N'' \to \frac{M \otimes_A N}{\mathrm{Img}(Id_M \otimes_A \varphi)}$$

como segue: se $(m, n'') \in M \times N''$, então existe $n \in N$ tal que $\psi(n) = n''$, assim fazemos $\rho(m, n'') = m \otimes n + \mathrm{Img}(Id_M \otimes_A \varphi)$. Agora, se $n_1, n_2 \in N$ são tais que $\psi(n_1) = n'' = \psi(n_2)$, então $n_1 - n_2 \in \mathrm{Ker}(\psi) = \mathrm{Img}(\varphi)$, logo existe $n' \in N'$ tal que $\varphi(n') = n_1 - n_2$, portanto $m \otimes (n_1 - n_2) = m \otimes \varphi(n') \in \mathrm{Img}(Id_M \otimes_A \varphi)$.

Segue que ρ está bem definida, além disso, claramente ρ é A-biaditiva, então, pela propriedade universal do produto tensorial, existe um A-homomorfismo

$$\overline{\rho} : M \otimes_A N'' \to \frac{M \otimes_A N}{\mathrm{Img}(Id_M \otimes_A \varphi)}$$

dado por $\overline{\rho}(m \otimes n'') = m \otimes n + \mathrm{Img}(Id_M \otimes_A \varphi)$ com $\varphi(n) = n''$. Claramente temos que $\overline{\psi}$ e $\overline{\rho}$ são inversos um do outro, logo

$$\mathrm{Ker}(Id_M \otimes_A \psi) = \mathrm{Ker}(\overline{\psi}\pi) = \mathrm{Ker}(\pi) = \mathrm{Img}(Id_M \otimes_A \varphi).$$

Se $\sum_{i=1}^{k} m_i \otimes n_i'' \in M \otimes_A N''$, então existem $n_i \in N$ tais que $\psi(n_i) = n_i''$ para cada $i = 1, \ldots, k$. Assim

$$(Id_M \otimes_A \psi)\left(\sum_{i=1}^{k} m_i \otimes n_i\right) = \sum_{i=1}^{k} m_i \otimes \psi(n_i) = \sum_{i=1}^{k} m_i \otimes n_i''.$$

Segue que $Id_M \otimes_A \psi$ é sobrejetor. □

Proposição 27. Seja

$$M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

uma sequência exata de A-módulos à direita. Então para cada A-módulo à esquerda N, a sequência de grupos abelianos induzida abaixo é exata:

$$M' \otimes_A N \xrightarrow{\varphi \otimes_A Id_N} M \otimes_A N \xrightarrow{\psi \otimes_A Id_N} M'' \otimes_A N \longrightarrow 0$$

Demonstração. A prova é análoga à da proposição anterior. □

Proposição 28. Seja M um A-módulo à direita e $\{N_j\}_{j \in J}$ uma família de A-módulos à esquerda. Então existe um isomorfismo de grupos

$$M \otimes_A \left(\bigoplus_{j \in J} N_j\right) \cong \bigoplus_{j \in J} (M \otimes_A N_j).$$

Demonstração. Por um lado defina a aplicação A-biaditiva $f : M \times \left(\bigoplus_{j \in J} N_j\right) \to \bigoplus_{j \in J}(M \otimes_A N_J)$ dada por $(m, (n_j)_{j \in J}) \mapsto (m \otimes n_j)_{j \in J}$ que dá origem, pela propriedade universal do produto tensorial, a um homomorfismo de grupos $\tilde{f} : M \otimes_A \left(\bigoplus_{j \in J} N_j\right) \to \bigoplus_{j \in J}(M \otimes_A N_j)$ tal que $m \otimes (n_j)_{j \in J} \mapsto (m \otimes n_j)_{j \in J}$.

Por outro lado considere a família de A-homomorfismos $g_i : M \otimes_A N_i \to M \otimes_A \left(\bigoplus_{j \in J} N_j\right)$ dados por $m \otimes n_i \mapsto m \times \iota_i(n_i)$, induzida pelas injeções canônicas $\iota_i : N_i \to \bigoplus_{j \in J} N_j$ para cada $i \in J$, que dá origem, pela propriedade universal da soma direta, a um homomorfismo de grupos $\tilde{g} : \bigoplus_{j \in J}(M \otimes_A N_j) \to M \otimes_A \left(\bigoplus_{j \in J} N_j\right)$ tal que $(m \otimes n_j)_{j \in J} \mapsto m \otimes \sum_{j \in J} \iota_j(n_j)$.

Desta maneira temos homomorfismos de grupos inversos um do outro, portanto segue o isomorfismo desejado. □

Proposição 29. Seja N um A-módulo à esquerda e $\{M_j\}_{j\in J}$ uma família de A-módulos à direita. Então existe um isomorfismo de grupos

$$\varepsilon : \left(\bigoplus_{j\in J} M_j\right) \otimes_A N \to \bigoplus_{j\in J}(M_j \otimes_A N).$$

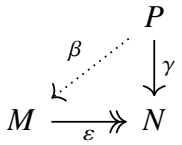
Demonstração. A prova é muito semelhante à da proposição anterior. □

2.5 Módulos projetivos e módulos livres

Nesta seção trataremos de duas classes importantes de módulos: projetivos e livres. Os primeiros possuem uma relação íntima com os grupos de homomorfismos, fazendo com que sequências exatas sejam preservadas. Os últimos são módulos que possuem base, portanto se aproximam dos espaços vetoriais, além de possuírem a interessante propriedade de que todo módulo é o quociente de algum módulo livre.

Definição 30. Um A-módulo P é dito projetivo quando para todo A-homomorfismo sobrejetor $\varepsilon : M \to N$ e para todo A-homomorfismo $\gamma : P \to N$ existir um A-homomorfismo $\beta : P \to M$ tal que $\varepsilon\beta = \gamma$.

Visualmente temos o diagrama comutativo abaixo.



Proposição 30. Uma soma direta $\bigoplus_{j\in J} P_j$ é projetiva se, e somente se, cada P_j é projetivo.

Demonstração. Suponha $\bigoplus_{j\in J} P_j$ projetiva e tome $i \in J$ fixo. Sejam $\varepsilon : M \to N$ um A-homomorfismo sobrejetor e $\gamma_i : P_i \to N$ um A-homomorfismo qualquer. Denotando para $k \in J$, $k \neq i$, o A-homomorfismo nulo por $0 = \gamma_k : P_k \to N$, obtemos, pela propriedade universal da soma direta, um A-homomorfismo $\gamma : \bigoplus_{j\in J} P_j \to N$ tal que $\gamma_j = \gamma\iota_j$ para cada $j \in J$.

Da hipótese temos que existe $\beta : \bigoplus_{j\in J} P_j \to M$ tal que $\varepsilon\beta = \gamma$. Assim, fazendo $\beta_i = \beta\iota_i$ temos que $\varepsilon\beta_i = \varepsilon\beta\iota_i = \gamma\iota_i = \gamma_i$. Provamos assim que P_i é projetivo e da arbitrariedade de $i \in J$ segue a implicação desejada.

Suponha agora que P_j é projetivo para cada $j \in J$. Sejam $\varepsilon : M \to N$ um A-homomorfismo sobrejetor e $\beta : \bigoplus_{j\in J} P_j \to N$ um A-homomorfismo qualquer. Da hipótese temos que para cada $j \in J$ existe um A-homomorfismo $\beta_j : P_j \to M$ tal que $\varepsilon\beta_j = \gamma\iota_j$.

Pela propriedade universal da soma direta, existe $\beta : \bigoplus_{j\in J} P_j \to M$ tal que para cada $j \in J$ temos $\beta_j = \beta\iota_j$. Assim segue que $\gamma\iota_j = \varepsilon\beta_j = \varepsilon\beta\iota_j$, logo $\gamma = \varepsilon\beta_j$. Provando assim que $\bigoplus_{j\in J} P_j$ é projetivo. □

Sejam M um A-módulo e $S \subseteq A$ um subconjunto de M. Considere o conjunto $\langle S \rangle$ de todos os elementos da forma $\sum_{s \in S} a_s s$ com $a_s \in A$ para todo $s \in S$ e $a_s \neq 0$ apenas para um número finito de índices. Prova-se que $\langle S \rangle$ é o menor submódulo de M que contém S.

Se para o conjunto S o submódulo $\langle S \rangle$ é todo o módulo M, dizemos que S é um conjunto de geradores para M ou que M é gerado por S. Quando M admite um conjunto finito de geradores dizemos que M é finitamente gerado.

Exemplo 17. Seja A um anel. Então temos alguns exemplos de A-módulos finitamente gerados:

1. Um módulo gerado por apenas um único elemento é chamado de módulo cíclico;
2. Se $A = \mathbb{Z}$, então A-módulos finitamente gerados são exatamente os grupos abelianos finitamente gerados;
3. Se $A = \mathbb{K}$ é um corpo, então A-módulos finitamente gerados são exatamente os K-espaços vetoriais de dimensão finita.

Um conjunto S de geradores para M é chamado de base quando for linearmente independente, ou seja, quando cumprir que se $\sum_{s \in S} a_s s = 0$, então $a_s = 0$ para todo $s \in S$, equivalentemente quando cada elemento $m \in M$ for expresso de maneira única na forma $m = \sum_{s \in S} a_s s$, com $a_s \in A$ para todo $s \in S$ e $a_s \neq 0$ apenas para um número finito de índices.

Se S é uma base para o módulo M dizemos que M é livre sobre o conjunto S. Se M for livre sobre algum conjunto, possivelmente desconhecido, dizemos que M é um módulo livre.

Exemplo 18. Seja A um anel. Então temos alguns exemplos de A-módulos livres:

1. O próprio anel A é um A-módulo livre com base formada por qualquer unidade;
2. Mais geralmente, um ideal I de A é um A-módulo livre se, e somente se, I é um ideal principal gerado por um elemento não divisor de zero, neste caso qualquer gerador constitui uma base para I;
3. Se A é comutativo, então o anel de polinômios em uma indeterminada $A[X]$ é um A-módulo livre com uma base canônica $\{1, X, X^2, \dots\}$.

Na sequência damos uma caracterização dos módulos livres.

Proposição 31. Suponha que o A-módulo P é livre sobre o conjunto S. Então $P \cong \bigoplus_{s \in S} A$, com o anel A visto como A-módulo. Reciprocamente, $\bigoplus_{s \in S} A$ é livre sobre o conjunto $\{1_s; s \in S\}$, sendo que para cada $r \in S$, temos $1_r = (a_s)_{s \in S}$ tal que $a_r = 1$ e $a_s = 0$ para $s \neq r$.

Demonstração. Defina um A-homomorfismo $\varphi : P \to \bigoplus_{s \in S} A$ como segue: cada elemento $p \in P$ é escrito de maneira única na forma $p = \sum_{j \in J} a_s s$, faça $\varphi(p) = (a_s)_{s \in S}$.

Por outro lado, para cada $r \in S$ defina um A-homomorfismo $\psi_r : A \to P$ dado por $\psi_r(a) = ar$. Pela propriedade universal da soma direta, obtemos um A-homomorfismo $\psi : \bigoplus_{s\in S} A \to P$ tal que $\psi\iota_r = \psi_r$ para cada $r \in S$ e $\iota_r : A \to \bigoplus_{s\in S} A$ as injeções canônicas.

Os A-homomorfismos φ e ψ são inversos um do outro, portanto temos o isomorfismo desejado.

Reciprocamente, devemos mostrar que o conjunto $T = \{1_s; s \in S\}$ é uma base para $Q = \bigoplus_{s\in S} A$.

Se $(a_s)_{s\in S} \in \bigoplus_{s\in S} A$, então $(a_s)_{s\in S} = \sum_{s\in S} a_s 1_s$, logo T gera Q. Além disso, se $\sum_{s\in S} a_s 1_s = 0$, então $(a_s)_{s\in S} = (0)_{s\in S}$, ou seja, $a_s = 0$ para todo $s \in S$. □

A proposição seguinte dá a propriedade universal que caracteriza um módulo livre.

Proposição 32 (Propriedade Universal dos módulos livres). Seja P um A-módulo livre sobre o conjunto S. Para todo A-módulo M e toda função $f : S \to M$, existe um único A-homomorfismo $\varphi : P \to M$ que estende f.

Demonstração. Denote $f(s) = m_s$ para cada $s \in S$. Agora se $p = \sum_{s\in S} a_s s$, então defina $\varphi(p) = \sum_{s\in S} a_s m_s$. □

Teorema 5. Todo módulo é quociente de algum módulo livre (portanto projetivo).

Demonstração. Seja $S \subseteq M$ um conjunto de geradores para o A-módulo M. Defina a função $f : S \to \bigoplus_{s\in s} A$ dada por $f(r) = (a_s)_{s\in s}$ com $a_r = 1$ e $a_s = 0$ para $s \neq r$.

Claramente a extensão $\varphi : M \to \bigoplus_{s\in S} A$ de f pela propriedade universal dos módulos livres é um A-homomorfismo sobrejetor, portanto, segue o isomorfismo desejado pelo Teorema do Isomorfismo. □

Observação 12. Sejam $M \neq 0$ um A-módulo, $\varepsilon : M \to N$ um A-homomorfismo sobrejetor e $\gamma : A \to N$ um A-homomorfismo qualquer. Como A é um módulo livre com base $\{1_A\}$, então γ está definido por $\gamma(1_A) = n \in N$. Sendo ε sobrejetor, existe $m \in M$ tal que $\varepsilon(m) = n = \gamma(1_A)$. Defina $\beta : A \to M$ por $\beta(1_A) = m$.

Isto mostra que A é um A-módulo projetivo. Pela caracterização dos módulos livre temos que todo módulo livre é projetivo.

Teorema 6. Para um A-módulo P são equivalentes:

1. P é projetivo;
2. para toda sequência exata curta $0 \longrightarrow L \xrightarrow{\mu} M \xrightarrow{\varepsilon} N \longrightarrow 0$ de A-módulos a sequência induzida abaixo é exata

$$0 \longrightarrow \mathrm{Hom}_A(P, L) \xrightarrow{\mu_*} \mathrm{Hom}_A(P, M) \xrightarrow{\varepsilon_*} \mathrm{Hom}_A(P, N) \longrightarrow 0;$$

3. se $\varepsilon : M \to P$ é um A-homomorfismo sobrejetivo, então existe um A-homomorfismo $\beta : P \to M$ tal que $\varepsilon\beta = 1_P$;

4. P é um somando direto de todo módulo para o qual P é um quociente;

5. P é um somando direto de algum módulo livre.

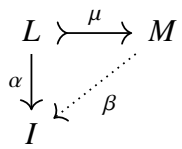
A prova deste teorema pode ser encontrada em Hilton e Stammbach (1996, p. 25).

2.6 Módulos injetivos e colivres

Aqui abordaremos os módulos injetivos, que possuem uma relação com os grupos de homomorfismos, fazendo com que sequências exatas sejam preservadas, com uma diferença em relação aos módulos projetivos. Já os módulos colivres formam uma classe que dualiza algumas das propriedades dos módulos livres.

Definição 31. Um A-módulo I é dito injetivo quando para todo A-homomorfismo injetor $\mu : L \to M$ e para todo A-homomorfismo $\alpha : L \to I$ existir um A-homomorfismo $\beta : M \to I$ tal que $\beta\mu = \alpha$.

Visualmente temos o diagrama comutativo abaixo.



Proposição 33. Um produto direto $\prod_{j\in J} I_j$ é injetivo se, e somente se, cada I_j é projetivo.

Demonstração. A prova é dual àquela dada para a soma direta. □

Considere $A^* = \mathrm{Hom}\,(A, \mathbb{Q}/\mathbb{Z})$ o grupo abeliano de homomorfismos de grupo de A em $\mathbb{Q}/\mathbb{Z}$, que é um A-módulo à esquerda (ou à direita) via a estrutura de A.

Definição 32. Dizemos que um A-módulo M é colivre quando $M \cong \prod_{j\in J} A^*$, isto é, quando M for isomorfo a algum produto direto de cópias de A^*.

Observação 13. Em Hilton e Stammbach (1996) mostra-se que A^* é um A-módulo injetivo. Pela definição de módulos colivres temos que todo módulo colivre é injetivo. Além disso, também é demonstrado o importante teorema abaixo.

Teorema 7. Todo módulo é submódulo de algum módulo colivre (portanto injetivo).

Finalmente, podemos enunciar o teorema abaixo, caracterizando os módulos injetivos.

Teorema 8. Para um A-módulo I são equivalentes:

1. I é injetivo;
2. para toda sequência exata curta $0 \longrightarrow L \xrightarrow{\mu} M \xrightarrow{\varepsilon} N \longrightarrow 0$ de A-módulos a sequência induzida abaixo é exata

$$0 \longrightarrow \mathrm{Hom}_A(N, I) \xrightarrow{\varepsilon^*} \mathrm{Hom}_A(M, I) \xrightarrow{\mu^*} \mathrm{Hom}_A(L, I) \qquad 0;$$

3. se $\mu : I \to M$ é um A-homomorfismo injetor, então existe um A-homomorfismo $\beta : M \to I$ tal que $\beta\mu = 1_P$;
4. I é um fator direto de todo módulo para o qual I é um submódulo;
5. I é um fator direto de algum módulo colivre.

A prova deste teorema é dual à do Teorema 6.

CAPÍTULO

3

CONCEITOS (CO)HOMOLÓGICOS

Neste capítulo trataremos da teoria básica de (co)homologia na categoria de módulos sobre um anel. Iniciaremos definindo complexos e (co)homologia na primeira seção para em seguida tratar de resoluções projetivas e injetivas na segunda seção. Na sequência, definiremos as principais ferramentas da teoria, os funtores Tor (,) e Ext (,) nas seções segunda e terceira, respectivamente, e apresentando a sequência exata longa de (co)homologia obtida a partir de uma sequência exata curta.

3.1 Complexos e homologia

Definição 33. Seja A um anel. Dizemos que uma sequência de A-módulos e A-homomorfismos

$$(M_\bullet, d_\bullet): \qquad \cdots \longrightarrow M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \longrightarrow \cdots$$

é um complexo de cadeia (ou simplesmente complexo) quando $d_{i-1}d_i = 0$ para todo $i \in \mathbb{Z}$.

Definição 34. Seja A um anel. Dizemos que uma sequência de A-módulos e A-homomorfismos

$$(M^\bullet, d^\bullet): \qquad \cdots \longrightarrow M^{i-1} \xrightarrow{d^{i-1}} M^i \xrightarrow{d^i} M^{i+1} \longrightarrow \cdots$$

é um cocomplexo de cadeia (ou simplesmente cocomplexo) quando $d^i d^{i-1} = 0$ para todo $i \in \mathbb{Z}$.

Observação 14. Será usual denotar um complexo $(M_\bullet, d_\bullet)$ simplesmente por $M_\bullet$ quando isto não causar confusão. Analogamente simplifica-se a notação para cocomplexos.

Observação 15. Dado um complexo $(M_\bullet, d_\bullet)$, é possível visualizá-lo como um cocomplexo reindexando seus termos: $M^i = M_{-i}$ e $(d^i : M^i \to M^{i+1}) = (d_{-i} : M_{-i} \to M_{-i-1})$. Com isso em mente, alguns resultados serão enunciados apenas em termos de complexos, com a sua validade para cocomplexos sendo verificada de maneira imediata pela correspondência acima.

Exemplo 19. Alguns exemplos imediatos de complexos (ou cocomplexos) são:

1. todo A-módulo M pode ser visto como um complexo no qual um dos termos é M, os demais são zero e os A-homomorfismos são todos nulos;

2. todo A-homomorfismo $f : M \to N$ pode ser visto como um complexo no qual um dos termos é M, o seguinte termo é N, os demais são zero, o A-homomorfismo de M para N é f e o restante é nulo;

3. toda sequência exata é um complexo, em particular, toda sequência exata curta é um complexo, bastando completar à esquerda e à direita com zeros;

4. qualquer sequência de A-módulos $\{M_i\}_{i\in\mathbb{Z}}$ pode ser vista como um complexo no qual todos os A-homomorfismos são nulos;

5. em particular no item acima, o complexo formado por todos os termos zero e todos os A-homomorfismos nulos é dito o complexo nulo e denotado por $0_\bullet$.

Definição 35. Um morfismo de cadeia (ou um morfismo de complexos) $f_\bullet : M_\bullet \to M'_\bullet$ é uma família de A-homomorfismos $\{f_i : M_i \to M'_i\}_{i\in\mathbb{Z}}$ tais que o diagrama abaixo é comutativo para cada $i \in \mathbb{Z}$:

$$\begin{array}{ccc} M_i & \xrightarrow{f_i} & M'_i \\ \downarrow{\scriptstyle d_i} & & \downarrow{\scriptstyle d'_i} \\ M_{i-1} & \xrightarrow{f_{i-1}} & N_{i-1}. \end{array}$$

A composição de morfismos de cadeia $f_\bullet : M_\bullet \to M'_\bullet$ e $g_\bullet : M'_\bullet \to M''_\bullet$ é dada pontualmente, isto é, $g_\bullet f_\bullet = \{g_i f_i\}_{i\in\mathbb{Z}}$.

Além disso, todo complexo $M_\bullet$ possui um morfismo de cadeia identidade $Id_{M_\bullet} = \{Id_{M_i}\}_{i\in\mathbb{Z}}$ e dados dois morfismos de cadeia $f_\bullet, g_\bullet : M_\bullet \to M'_\bullet$ sua soma é definida pontualmente, isto é, $f_\bullet + g_\bullet = \{f_i + g_i\}_{i\in\mathbb{Z}}$.

Observação 16. Com a definição acima concluímos que complexos de cadeia e morfismos de cadeia formam uma categoria que será denotada por $\mathfrak{Comp}_A$.

Definição 36. Dizemos que uma sequência de complexos de cadeia e morfismos de cadeia

$$\cdots \longrightarrow M'_\bullet \xrightarrow{f_\bullet} M_\bullet \xrightarrow{g_\bullet} M''_\bullet \longrightarrow \cdots$$

é exata quando

$$\cdots \longrightarrow M'_i \xrightarrow{f_i} M_i \xrightarrow{g_i} M''_i \longrightarrow \cdots$$

é uma sequência exata para cada $i \in \mathbb{Z}$. Em particular uma sequência exata curta de complexos é do tipo

$$0_\bullet \longrightarrow M'_\bullet \xrightarrow{f_\bullet} M_\bullet \xrightarrow{g_\bullet} M''_\bullet \longrightarrow 0_\bullet.$$

Definição 37. Dado um complexo

$$(M_\bullet, d_\bullet): \qquad \cdots \longrightarrow M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \longrightarrow \cdots$$

definimos o seu i-ésimo grupo de homologia como sendo o quociente

$$H_i(M_\bullet) = \frac{\mathrm{Ker}(d_i)}{\mathrm{Img}(d_{i+1})}.$$

Definição 38. Dado um cocomplexo

$$(M^\bullet, d^\bullet): \qquad \cdots \longrightarrow M^{i-1} \xrightarrow{d^{i-1}} M_i \xrightarrow{d^i} M^{i+1} \longrightarrow \cdots$$

definimos o seu i-ésimo grupo de cohomologia como sendo o quociente

$$H^i(M^\bullet) = \frac{\mathrm{Ker}(d^i)}{\mathrm{Img}(d^{i-1})}.$$

Proposição 34. Para cada $i \in \mathbb{Z}$, a construção $H_i(-) : \mathfrak{Comp}_A \to \mathfrak{Ab}$ é funtorial e vale que $H_i(f_\bullet + g_\bullet) = H_i(f_\bullet) + H_i(g_\bullet)$.

Demonstração. Já definimos a ação de $H_i(-)$ em complexos, nos resta definir nos morfismos de cadeia. Seja $f_\bullet : M_\bullet \to M'_\bullet$ um morfismo de cadeia, então $H_i(f_\bullet) : H_i(M_\bullet) \to H_i(M'_\bullet)$ é dado por $m + \mathrm{Img}(d_{i+1}) \mapsto f_i(m) + \mathrm{Img}(d'_{i+1})$.

Precisamos mostrar que se $m \in \mathrm{Ker}(d_i)$, então $f_i(m) \in \mathrm{Ker}(d'_i)$. Mas isto decorre imediatamente da definição de morfismo de cadeia, pois

$$0 = f_{i-1}(d_i(m)) = d'_i(f_i(m)).$$

Agora devemos mostrar que a definição acima não depende da escolha do representante. Suponha então $m_1 + \mathrm{Img}(d_{i+1}) = m_2 + \mathrm{Img}(d_{i+1})$, logo $m_1 - m_2 = d_{i+1}(x)$, com $x \in M_{i+1}$, assim

$$f_i(m_1) - f_i(m_2) = f_i(m_1 - m_2) = f_i(d_{i-1}(x)) = d'_{i+1}(f_{i+1}(x))$$

e portanto $f_i(m_1) + \mathrm{Img}(d'_{i+1}) = f_i(m_2) + \mathrm{Img}(d'_{i+1})$.

Temos que $H_i(f_\bullet)$ é um homomorfismo de grupos, pois

$$\begin{aligned} H_i(f_\bullet)((m_1 + \mathrm{Img}(d_{i+1})) + (m_2 + \mathrm{Img}(d_{i+1}))) &= H_i(f_\bullet)((m_1 + m_2) + \mathrm{Img}(d_{i+1})) \\ &= f_i(m_1 + m_2) + \mathrm{Img}(d_{i+1}) \\ &= (f_i(m_1) + f_i(m_2)) + \mathrm{Img}(d_{i+1}) \\ &= (f_i(m_1) + \mathrm{Img}(d_{i+1})) + (f_i(m_2) + \mathrm{Img}(d_{i+1})). \end{aligned}$$

Claramente $H_i(Id_{M_\bullet}) = Id_{H_i(M_\bullet)}$. Além disso, se $f_\bullet : M_\bullet \to M'_\bullet$ e $g_\bullet : M'_\bullet \to M''_\bullet$, então

$$\begin{aligned} H_i(g_\bullet f_\bullet)(m + \mathrm{Img}(d_{i+1})) &= (g_i f_i)(m) + \mathrm{Img}(d''_{i+1}) \\ &= g_i(f_i(m)) + \mathrm{Img}(d''_{i+1}) \\ &= H_i(g_\bullet)(f_i(m) + \mathrm{Img}(d'_{i+1})) \\ &= H_i(g_\bullet)(H_i(f_\bullet)(m + \mathrm{Img}(d_{i+1}))) \\ &= (H_i(g_\bullet)H_i(f_\bullet))(m + \mathrm{Img}(d_{i+1})). \end{aligned}$$

Por fim, se $f_\bullet, g_\bullet : M_\bullet \to M'_\bullet$, segue que

$$\begin{aligned} H_i(f_\bullet + g_\bullet)(m + \mathrm{Img}(d_{i+1})) &= (f_i + g_i)(m) + \mathrm{Img}(d'_{i+1}) \\ &= (f_i(m) + g_i(m)) + \mathrm{Img}(d'_{i+1}) \\ &= (f_i(m) + \mathrm{Img}(d'_{i+1})) + (g_i(m) + \mathrm{Img}(d'_{i+1})) \\ &= H_i(f_\bullet)(m + \mathrm{Img}(d_{i+1})) + H_i(g_\bullet)(m + \mathrm{Img}(d_{i+1})) \\ &= (H_i(f_\bullet) + H_i(g_\bullet))(m + \mathrm{Img}(d_{i+1})). \end{aligned}$$

□

Observação 17. Será usual denotar $H_i(f_\bullet)$ por f_* ou f_{i*}.

Lema 1 (Lema da serpente)**.** Dado o diagrama comutativo de A-módulos e A-homomorfismos com linhas exatas abaixo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & N' & \xrightarrow{\sigma} & N & \xrightarrow{\tau} & N'' & \longrightarrow & 0 \end{array}$$

existe uma sequência exata

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Ker}(f) & \xrightarrow{\overline{\alpha}} & \mathrm{Ker}(g) & \xrightarrow{\overline{\beta}} & \mathrm{Ker}(h) \\ & & & \searrow^{\omega} & & & \\ & & \mathrm{Coker}(f) & \xrightarrow{\overline{\sigma}} & \mathrm{Coker}(g) & \xrightarrow{\overline{\tau}} & \mathrm{Coker}(h) \longrightarrow 0. \end{array}$$

Teorema 9 (Sequência exata longa de homologias)**.** Dada uma sequência exata de curta de complexos

$$0_\bullet \longrightarrow M'_\bullet \xrightarrow{f_\bullet} M_\bullet \xrightarrow{g_\bullet} M''_\bullet \longrightarrow 0_\bullet,$$

existe uma sequência exata longa de A-módulos e A-homomorfismos

$$\begin{array}{ccccccc} & & & & & & \cdots \\ & & & & & \swarrow & \\ & & H_i(M'_\bullet) & \xrightarrow{f_{i*}} & H_i(M_\bullet) & \xrightarrow{g_{i*}} & H_i(M''_\bullet) \\ & & & \searrow^{\omega_i} & & & \\ & & H_{i-1}(M'_\bullet) & \xrightarrow{f_{i-1*}} & H_{i-1}(M_\bullet) & \xrightarrow{g_{i-1*}} & H_{i-1}(M''_\bullet) \\ & \swarrow & & & & & \\ \cdots & & & & & & . \end{array}$$

Demonstração. Considere o diagrama comutativo abaixo com linhas exatas que representa uma parte da sequência exata curta de complexos do enunciado:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M'_{i+1} & \xrightarrow{f_{i+1}} & M_{i+1} & \xrightarrow{g_{i+1}} & M''_{i+1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'_{i+1}} & & \downarrow{\scriptstyle d_{i+1}} & & \downarrow{\scriptstyle d''_{i+1}} & & \\
0 & \longrightarrow & M'_{i} & \xrightarrow{f_{i}} & M_{i} & \xrightarrow{g_{i}} & M''_{i} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'_{i}} & & \downarrow{\scriptstyle d_{i}} & & \downarrow{\scriptstyle d''_{i}} & & \\
0 & \longrightarrow & M'_{i-1} & \xrightarrow{f_{i-1}} & M_{i-1} & \xrightarrow{g_{i-1}} & M''_{i-1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'_{i-1}} & & \downarrow{\scriptstyle d_{i-1}} & & \downarrow{\scriptstyle d''_{i-1}} & & \\
0 & \longrightarrow & M'_{i-2} & \xrightarrow{f_{i-2}} & M_{i-2} & \xrightarrow{g_{i-2}} & M''_{i-2} & \longrightarrow & 0.
\end{array}$$

Aplicando o Lema 1 às duas primeiras linhas do diagrama comutativo acima obtemos a primeira linha do diagrama comutativo abaixo, aplicando o Lema 1 às duas últimas linhas do diagrama comutativo acima obtemos a segunda linha do diagrama comutativo abaixo:

$$\begin{array}{ccccccccc}
 & & \dfrac{M'_i}{\mathrm{Img}(d'_{i+1})} & \xrightarrow{\overline{f_i}} & \dfrac{M_i}{\mathrm{Img}(d_{i+1})} & \xrightarrow{\overline{g_i}} & \dfrac{M''_i}{\mathrm{Img}(d''_{i+1})} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} & & \\
0 & \longrightarrow & \mathrm{Ker}(d'_{i-1}) & \xrightarrow{\overline{f_{i-1}}} & \mathrm{Ker}(d_{i-1}) & \xrightarrow{\overline{f_{i-1}}} & \mathrm{Ker}(d''_{i-1}) & &
\end{array}$$

cujos homomorfismos verticais são dados por $d(m + \mathrm{Img}(d_{i+1})) = d_i(m)$, que estão bem definidos por causa das inclusões $\mathrm{Img}(d_{i+1}) \subseteq \mathrm{Ker}(d_i)$ e $\mathrm{Img}(d_i) \subseteq \mathrm{Ker}(d_{i-1})$. A comutatividade do diagrama segue pois

$$\begin{aligned}
d(\overline{f_i}(m' + \mathrm{Img}(d'_{i+1}))) &= d(f_i(m') + \mathrm{Img}(d_{i+1})) \\
&= d_i(f_i(m')) \\
&= f_{i-1}(d'_i(m')) \\
&= \overline{f_{i-1}}(d'_i(m')) \\
&= \overline{f_{i-1}}(d'(m' + \mathrm{Img}(d'_{i+1}))).
\end{aligned}$$

Note que

$$\mathrm{Ker}(d) = \{m' + \mathrm{Img}(d_{i+1}); d_i(m') = 0\} = \frac{\mathrm{Ker}(d_i)}{\mathrm{Img}(d_{i+1})} = H_i(M_\bullet)$$

e

$$\mathrm{Img}(d) = \mathrm{Img}(d_i),$$

logo

$$\mathrm{Coker}(d) = \frac{\mathrm{Ker}(d_{i-1})}{\mathrm{Img}(d)} = \frac{\mathrm{Ker}(d_{i-1})}{\mathrm{Img}(d_i)} = H_{i-1}(M_\bullet).$$

Aplicando o Lema 1 no diagrama comutativo acima obtemos a sequência exata desejada. □

De maneira dual, obtemos a sequência exata longa de cohomologias a partir de uma sequência exata curta de cocomplexos de cadeia.

Teorema 10 (Sequência exata longa de cohomologias)**.** Dada uma sequência exata de curta de cocomplexos

$$0^\bullet \longrightarrow M'^\bullet \xrightarrow{f^\bullet} M^\bullet \xrightarrow{g^\bullet} M''^\bullet \longrightarrow 0^\bullet,$$

existe uma sequência exata longa de A-módulos e A-homomorfismos

$$\begin{array}{l} \cdots \\ \curvearrowright \\ H^i(M'^\bullet) \xrightarrow{f^i_*} H^i(M^\bullet) \xrightarrow{g^i_*} H^i(M''^\bullet) \\ \curvearrowright \quad \omega^i \\ H^{i+1}(M'^\bullet) \xrightarrow{f^{i+1}_*} H^{i+1}(M^\bullet) \xrightarrow{g^{i+1}_*} H^{i+1}(M''^\bullet) \\ \curvearrowright \\ \cdots \qquad . \end{array}$$

Definição 39. Sejam $f_\bullet, g_\bullet : M_\bullet \to M'_\bullet$ dois morfismos de cadeia. Dizemos que $f_\bullet$ é homotópico a $g_\bullet$, o que denotamos por $f_\bullet \simeq g_\bullet$, quando existe uma família de A-homomorfismos $\{s_i : M_n \to M'_{i+1}\}$ tais que para todo $i \in \mathbb{Z}$ temos

$$f_i - g_i = d'_{i+1}s_i + s_{i-1}d_i.$$

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & M_{i+1} & \xrightarrow{d_{i+1}} & M_i & \xrightarrow{d_i} & M_{i-1} & \longrightarrow & \cdots \\ & & \downarrow\downarrow & \overset{s_i}{\swarrow} & \downarrow\downarrow & \overset{s_{i-1}}{\swarrow} & \downarrow\downarrow & & \\ \cdots & \longrightarrow & M'_{i+1} & \xrightarrow[d'_{i+1}]{} & M'_i & \xrightarrow[d'_i]{} & M'_{i-1} & \longrightarrow & \cdots \end{array}$$

Definição 40. Um morfismo de cadeia $f_\bullet$ é dito homotopicamente nulo quando $f_\bullet \simeq 0_\bullet$. Um complexo de cadeia $M_\bullet$ é dito contrátil, ou que possui homotopia contrátil, quando $Id_{M_\bullet} \simeq 0_\bullet$.

Teorema 11. Se $f_\bullet, g_\bullet : M_\bullet \to M'_\bullet$ são morfismos de cadeia homotópicos, então para todo $i \in \mathbb{Z}$ temos

$$f_{i*} = g_{i*} : H_i(M_\bullet) \to H_i(M'_\bullet).$$

Demonstração. Se $m \in \mathrm{Ker}(d_i)$, então temos

$$f_i(m) - g_i(z) = d'_{i+1}(s_i(m)) + s_{i-1}(d_i(m)) = d'_{i+1}(s_i(m)) + s_{i-1}(0) = d'_{i+1}(s_i(m)) \in \mathrm{Img}(d'_{i+1}),$$

logo $f_{i*} = g_{i*}$. □

Proposição 35. Seja $M_\bullet$ um complexo de cadeia contrátil, então $M_\bullet$ é uma sequência exata.

Demonstração. Como para cada $i \in \mathbb{Z}$ temos que $Id_{M_i*} : H_i(M_\bullet) \to H_i(M_\bullet)$ é o homomorfismo identidade, $0_{i*} : H_i(M_\bullet) \to H_i(M_\bullet)$ é o homomorfismo nulo e estes coincidem por hipótese, então temos que $\dfrac{\mathrm{Ker}(d_i)}{\mathrm{Img}(d_{i+1})} = H_i(M_\bullet) = 0$, logo $\mathrm{Ker}(d_i) = \mathrm{Img}(d_{i+1})$ para cada $i \in \mathbb{Z}$. □

3.2 Resoluções projetivas e injetivas

Definição 41. Seja M um A-módulo. Uma resolução projetiva de M é umcomplexo exato

$$(P_\bullet, d_\bullet): \qquad \cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0$$

no qual P_i é projetivo para todo $i \in \mathbb{N}$.

Dada uma resolução projetiva de M como na definição acima, a sua resolução projetiva deletada é o complexo

$$(P^M_\bullet, d_\bullet): \qquad \cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \longrightarrow 0.$$

Note que ao deletarmos o objeto M da resolução não estamos perdendo informação, já que $M \cong \mathrm{Coker}(d_1)$.

Definição 42. Seja M um A-módulo. Uma resolução injetiva de M é um cocomplexo exato

$$(I^\bullet, d^\bullet): \qquad 0 \longrightarrow M \xrightarrow{\mu} I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \longrightarrow \cdots$$

no qual I^i é injetivo para todo $i \in \mathbb{N}$.

Dada uma resolução injetiva de M como na definição acima, a sua resolução injetiva deletada é o cocomplexo

$$(I^\bullet_M, d^\bullet): \qquad 0 \longrightarrow I^0 \xrightarrow{d^0} I_1 \xrightarrow{d^1} I^2 \longrightarrow \cdots.$$

Note que ao deletarmos o objeto M da resolução não estamos perdendo informação, já que $M \cong \mathrm{Ker}(d^0)$.

Proposição 36. Todo módulo possui uma resolução livre (portanto projetiva) e uma resolução colivre (portanto injetiva).

Demonstração. Sabemos que todo para todo A-módulo M existe um A-módulo projetivo P_0 e um A-homomorfismo sobrejetor $\varepsilon : P_0 \to M$. Tome $K_1 = \mathrm{Ker}(\varepsilon)$ juntamente com a sua inclusão $i_1 : K_1 \to P_0$, então existe um A-módulo projetivo P_1 e um A-homomorfismo sobrejetor $p_1 : P_1 \to K_1$. Defina $d_1 = i_1 p_1 : P_1 \to P_0$, então temos que $\mathrm{Ker}(\varepsilon) = K_1 = \mathrm{Img}(d_1)$. Repetindo o processo obtemos a resolução desejada.

Para resoluções injetivas a construção é dual. Em cada caso, o diagrama comutativo correspondente abaixo ajuda a visualizar todo o processo.

$$\cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0$$

$$\begin{array}{ccccccccccc} & & & & P_2 & & P_1 & & P_0 & & \\ & & & \nearrow^{p_2} & & \searrow^{i_2} & & \nearrow^{p_1} & & \searrow^{i_1} & \\ 0 & \longrightarrow & M & \xrightarrow{\mu} & & K_2 & & K_1 & & \longrightarrow & 0 \end{array}$$

$$0 \longrightarrow M \xrightarrow{\mu} E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E^2 \longrightarrow \cdots$$

$$\begin{array}{ccccccccccc} & & & & E^0 & & E^1 & & E^2 & & \\ & & & \nearrow^{p^0} & & \searrow^{i^0} & & \nearrow^{p^1} & & \searrow^{i^1} & \\ 0 & \longrightarrow & M & \xrightarrow{\mu} & & Q^0 & & Q^1 & & \longrightarrow & \cdots \end{array}$$

□

Exemplo 20. Sejam $k, m, n \in \mathbb{N} \setminus \{0, 1\}$ tais que $k = mn$. Então $\mathbb{Z}_m$ e $\mathbb{Z}_n$ são $\mathbb{Z}_k$-módulos via $\overline{r} \cdot \overline{s} = \overline{rs}$ para $\overline{r} \in \mathbb{Z}_k$ e $\overline{s} \in \mathbb{Z}_m$ ou $\overline{s} \in \mathbb{Z}_n$. Considere os homomorfismos de grupo abaixo com seus respectivos núcleos e imagens

$$\begin{array}{cccc} m\cdot : \mathbb{Z}_k \to \mathbb{Z}_k & n\cdot : \mathbb{Z}_k \to \mathbb{Z}_k & \mu : \mathbb{Z}_k \to \mathbb{Z}_m & \nu : \mathbb{Z}_k \to \mathbb{Z}_n \\ \overline{r} \mapsto \overline{mr} & \overline{r} \mapsto \overline{nr} & \overline{r} \mapsto \overline{r} & \overline{r} \mapsto \overline{r} \\ \operatorname{Ker}(m\cdot) = \langle \overline{n} \rangle & \operatorname{Ker}(n\cdot) = \langle \overline{m} \rangle & \operatorname{Ker}(\mu) = \langle \overline{m} \rangle & \operatorname{Ker}(\nu) = \langle \overline{n} \rangle \\ \operatorname{Img}(m\cdot) = \langle \overline{m} \rangle & \operatorname{Img}(n\cdot) = \langle \overline{n} \rangle. & \operatorname{Img}(\mu) = \mathbb{Z}_m & \operatorname{Img}(\nu) = \mathbb{Z}_n. \end{array}$$

Perceba que é possível construir uma sequência exata longa

$$\cdots \longrightarrow \mathbb{Z}_k \xrightarrow{m\cdot} \mathbb{Z}_k \xrightarrow{n\cdot} \mathbb{Z}_k \xrightarrow{m\cdot} \mathbb{Z}_k \xrightarrow{n\cdot} \mathbb{Z}_k \longrightarrow \cdots .$$

Truncando esta sequência no lugar adequado e "colando" o homomorfismo correto, obtemos uma resolução projetiva de $\mathbb{Z}_m$ ou de $\mathbb{Z}_n$, apresentadas abaixo:

$$\cdots \longrightarrow \mathbb{Z}_k \xrightarrow{m\cdot} \mathbb{Z}_k \xrightarrow{n\cdot} \mathbb{Z}_k \xrightarrow{m\cdot} \mathbb{Z}_k \xrightarrow{\mu} \mathbb{Z}_m \longrightarrow 0$$

$$\cdots \longrightarrow \mathbb{Z}_k \xrightarrow{n\cdot} \mathbb{Z}_k \xrightarrow{m\cdot} \mathbb{Z}_k \xrightarrow{n\cdot} \mathbb{Z}_k \xrightarrow{\nu} \mathbb{Z}_n \longrightarrow 0.$$

Lema 2 (Lema da ferradura)**.** Considere o diagrama abaixo formado por uma linha exata e

resoluções projetivas nas colunas :

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & P_1 & & Q_1 & & & & \\
 & & \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle e_1} & & & & \\
 & & P_0 & & Q_0 & & & & \\
 & & \downarrow{\scriptstyle \varepsilon} & & \downarrow{\scriptstyle \pi} & & & & \\
0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Então o diagrama comutativo abaixo possui linhas exatas e resoluções projetivas nas colunas:

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_1 & \xrightarrow{f_1} & P_1 \oplus Q_1 & \xrightarrow{g_1} & Q_1 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d_1 \oplus e_1} & & \downarrow{\scriptstyle e_1} & & \\
0 & \longrightarrow & P_0 & \xrightarrow{f_0} & P_0 \oplus Q_0 & \xrightarrow{g_0} & Q_0 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varepsilon} & & \downarrow{\scriptstyle \varepsilon \oplus \pi} & & \downarrow{\scriptstyle \pi} & & \\
0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Lema 3 (Lema da comparação)**.** Seja $f : M \to M'$ um A-homomorfismo e considere o diagrama abaixo no qual as linhas representam resoluções projetivas:

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\
 & & & & & & & & \downarrow{\scriptstyle f} & & \\
\cdots & \longrightarrow & P'_2 & \xrightarrow{d'_2} & P'_1 & \xrightarrow{d'_1} & P'_0 & \xrightarrow{\varepsilon'} & M' & \longrightarrow & 0
\end{array}$$

Então existe um morfismo de cadeia $f_\bullet : P_\bullet^M \to P_\bullet'^{M'}$ tal que $f\varepsilon = \varepsilon' f_0$, além disso, quaisquer dois morfismos de cadeia que completem o diagrama são homotópicos. Neste caso dizemos que $f_\bullet$ é um morfismo de cadeia sobre f.

Lema 4 (Lema curto dos cinco)**.** Considere o diagrama comutativo abaixo de A-módulos e A-homomorfismos cujas linhas são exatas e suponha que φ' e φ'' são isomorfismos. Então φ é um isomorfismo.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M' & \longrightarrow & M & \xrightarrow{\varepsilon} & M'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi'} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi''} & & \\
0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0.
\end{array}$$

As provas dos três lemas anteriores podem ser encontradas em Rotman (2009), além disso, as versões dos primeiros lemas para resoluções injetivas também são verdadeiras e suas demonstrações são duais.

3.3 Os funtores $\mathrm{Tor}_i(-,-)$

Sejam M um A-módulo à direita e N um A-módulo à esquerda. Para uma resolução projetiva de M

$$(P_\bullet, d_\bullet): \qquad \cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0,$$

aplicando o funtor $F(-) = - \otimes_A N$ à resolução projetiva deletada obtemos o complexo abaixo

$$F(P_\bullet^M): \qquad \cdots \longrightarrow F(P_2) \xrightarrow{F(d_2)} F(P_1) \xrightarrow{F(d_1)} F(P_0) \longrightarrow 0.$$

Tomando homologia no i-ésimo nível definimos o seguinte grupo

$$\mathrm{Tor}_i^A(M,N) = H_i(F(P_\bullet^M)) = \frac{\mathrm{Ker}(F(d_i))}{\mathrm{Img}(F(d_{i+1}))}.$$

Dado um A-homomorfismo $f: M \to M'$ e resoluções projetivas $(P_\bullet, d_\bullet)$ e $(P'_\bullet, d'_\bullet)$ de M e M', respectivamente, pelo Lema 3 existe um morfismo de cadeia $f_\bullet: P_\bullet^M \to P_\bullet^{'M'}$. Aplicando o funtor $F(-) = - \otimes_A N$ temos um morfismo de cadeia induzido $F(f_\bullet): F(P_\bullet^M) \to F(P_\bullet^{'M'})$ e tomando homologia no i-ésimo nível obtemos o homomorfismo de grupos

$$\mathrm{Tor}_i^A(f,N) = H_i(F(f)): \mathrm{Tor}_i^A(M,N) \to \mathrm{Tor}_i^A(M',N).$$

Proposição 37. As homologias $\mathrm{Tor}_i^A(M,N)$ são independentes da escolha de resolução projetiva de M.

Demonstração. Considere duas resoluções projetivas de M

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\
 & & & & & & & & \downarrow Id_M & & \\
\cdots & \longrightarrow & P'_2 & \xrightarrow{d'_2} & P'_1 & \xrightarrow{d'_1} & P'_0 & \xrightarrow{\varepsilon'} & M & \longrightarrow & 0
\end{array}$$

pelo Lema 3 existe um morfismo de cadeia $f_\bullet: P_\bullet^M \to P_\bullet^{'M}$ sobre Id_M. Aplicando o funtor $F(-) = - \otimes_A N$ obtemos um morfismo de cadeia $F(f_\bullet): F(P_\bullet^M) \to F(P_\bullet^{'M})$ sobre $F(Id_M) = Id_{F(M)}$. Este último morfismo de cadeia induz, para cada $i \in \mathbb{Z}$, um homomorfismo

$$\sigma: H_i(F(P_\bullet^M)) \to H_i(F(P_\bullet^{'M})).$$

Invertendo o sentido de Id_M no diagrama acima, novamente pelo Lema 3, existe um morfismo de cadeia $g_\bullet: P_\bullet^{'M} \to P_\bullet^M$ sobre Id_M. Aplicando o funtor $F(-) = - \otimes_A N$ obtemos um

morfismo de cadeia $F(g_\bullet) : F(P'^M_\bullet) \to F(P^M_\bullet)$ sobre $F(Id_M) = Id_{F(M)}$. Este último morfismo de cadeia induz, para cada $i \in \mathbb{Z}$, um homomorfismo

$$\tau : H_i(F(P'^M_\bullet)) \to H_i(F(P^M_\bullet)).$$

Agora, temos que $g_\bullet f_\bullet$ é um morfismo de cadeia sobre Id_M, pelo Lema da comparação, temos que $g_\bullet f_\bullet \simeq Id_{P^M_\bullet}$. De maneira similar temos $f_\bullet g_\bullet \simeq Id_{P'^M_\bullet}$. Logo também são homotópicos os morfismos de cadeia

$$F(g_\bullet)F(f_\bullet) = F(g_\bullet f_\bullet) \simeq F(Id_{P^M_\bullet}) = Id_{F(P^M_\bullet)}$$

e

$$F(f_\bullet)F(g_\bullet) = F(f_\bullet g_\bullet) \simeq F(Id_{P'^M_\bullet}) = Id_{F(P'^M_\bullet)}.$$

Passando à homologia temos $\tau\sigma = Id_{H_i(F(P^M_\bullet))}$ e $\sigma\tau = Id_{H_i(F(P'^M_\bullet))}$. □

Corolário 1. Para P um A-módulo à direita projetivo e N um A-módulo à esquerda temos, para todo $i \geq 1$,

$$\mathrm{Tor}_i^A(P, N) = 0.$$

Demonstração. Sendo P projetivo, tome a resolução projetiva abaixo

$$0 \longrightarrow P \xrightarrow{1_P} P \longrightarrow 0.$$

□

Proposição 38. Para quaisquer A-módulos à direita M e à esquerda N, temos

$$\mathrm{Tor}_0^A(M, N) \cong M \otimes_A N.$$

Demonstração. Considere uma resolução projetiva de M

$$\cdots \longrightarrow P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0.$$

Como $- \otimes_A N$ é um funtor exato à direita, temos a sequência exata abaixo

$$P_1 \otimes_A N \xrightarrow{d_{1*}} P_0 \otimes_A N \xrightarrow{\varepsilon_*} M \otimes_A N \longrightarrow 0.$$

Por definição de homologia e pelo Teorema do Isomorfismo temos que

$$\mathrm{Tor}_0^A(M, N) = \frac{P_0 \otimes_A N}{\mathrm{Img}(d_{1*})} = \frac{P_0 \otimes_A N}{\mathrm{Ker}(\varepsilon_*)} \cong M \otimes_A N.$$

□

De maneira dual, podemos tomar uma resolução projetiva do A-módulo à esquerda N, aplicar o funtor $G(-) = M \otimes_A -$ e calcular as homologias obtendo os grupos abelianos

$$\operatorname{tor}_i^A(M, N).$$

Estas homologias são independentes da escolha de resolução projetiva de N, se anulam nos níveis $i \geq 1$ quando N é projetivo e coincidem com o produto tensorial no nível $i = 0$.

O teorema a seguir nos garante que estas construções são equivalentes. Sua demonstração pode ser encontrada em Rotman (2009, p. 355).

Teorema 12. Sejam M um A-módulo à direita e N um A-módulo à esquerda. Então para cada $i \geq 0$ temos

$$\operatorname{Tor}_i^A(M, N) \cong \operatorname{tor}_i^A(M, N).$$

Dados um A-módulo à esquerda N e uma sequência exata curta de A-módulos à direita

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

temos uma sequência exata longa de homologia

$$\begin{array}{l} \cdots \\ \operatorname{Tor}_2^A(M', N) \xrightarrow{f_{2*}} \operatorname{Tor}_2^A(M, N) \xrightarrow{g_{2*}} \operatorname{Tor}_2^A(M'', N) \\ \qquad\qquad \omega_2 \\ \operatorname{Tor}_1^A(M', N) \xrightarrow{f_{1*}} \operatorname{Tor}_1^A(M, N) \xrightarrow{g_{1*}} \operatorname{Tor}_1^A(M'', N) \\ \qquad\qquad \omega_1 \\ M' \otimes_A N \xrightarrow{f_*} M \otimes_A N \xrightarrow{g_*} M'' \otimes_A N \longrightarrow 0. \end{array}$$

De maneira similar, dados um A-módulo à direita M e uma sequência exata curta de A-módulos à esquerda

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$$

temos uma sequência exata longa de homologia

$$\begin{array}{l} \cdots \\ \operatorname{Tor}_2^A(M, N') \xrightarrow{f_{2*}} \operatorname{Tor}_2^A(M, N) \xrightarrow{g_{2*}} \operatorname{Tor}_2^A(M, N'') \\ \qquad\qquad \omega_2 \\ \operatorname{Tor}_1^A(M, N') \xrightarrow{f_{1*}} \operatorname{Tor}_1^A(M, N) \xrightarrow{g_{1*}} \operatorname{Tor}_1^A(M, N'') \\ \qquad\qquad \omega_1 \\ M \otimes_A N' \xrightarrow{f_*} M \otimes_A N \xrightarrow{g_*} M \otimes_A N'' \longrightarrow 0. \end{array}$$

3.4 Os funtores $\mathrm{Ext}^i_A(-,-)$

Sejam M e N dois A-módulos à esquerda (ou à direita). Para uma resolução projetiva de M

$$(P_\bullet, d_\bullet): \qquad \cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0,$$

aplicando o funtor $F(-) = \mathrm{Hom}_A(-, N)$ à resolução projetiva deletada obtemos o cocomplexo abaixo

$$F(P^M_\bullet): \qquad 0 \longrightarrow F(P_0) \xrightarrow{F(d_1)} F(P_1) \xrightarrow{F(d_2)} F(P_2) \longrightarrow \cdots.$$

Tomando cohomologia no i-ésimo nível definimos o seguinte grupo

$$\mathrm{Ext}^i_A(M,N) = H^i(F(P^M_\bullet)) = \frac{\mathrm{Ker}(F(d_{i+1}))}{\mathrm{Img}(F(d_i))}.$$

Dado um A-homomorfismo $f: M' \to M$ e resoluções projetivas $(P'_\bullet, d'_\bullet)$ e $(P_\bullet, d_\bullet)$ de M' e M, respectivamente, pelo Lema 3 existe um morfismo de cadeia $f_\bullet: P'^{M'}_\bullet \to P^M_\bullet$. Aplicando o funtor $F(-) = \mathrm{Hom}_A(-, N)$ temos um morfismo de cadeia induzido $F(f_\bullet): F(P^M_\bullet) \to F(P'^{M'}_\bullet)$ e tomando cohomologia no i-ésimo nível obtemos o homomorfismo de grupos

$$\mathrm{Ext}^i_A(f, N) = H^i(F(f)): \mathrm{Ext}^i_A(M,N) \to \mathrm{Ext}^i_A(M', N).$$

Proposição 39. As cohomologias $\mathrm{Ext}^i_A(M,N)$ são independentes da escolha de resolução projetiva de M.

Demonstração. A demonstração deste fato é análoga àquela dada para as homologias $\mathrm{Tor}^A_i(M,N)$. □

Corolário 2. Para P um A-módulo à esquerda projetivo e N um A-módulo à esquerda temos, para todo $i \geq 1$,

$$\mathrm{Ext}^i_A(P,N) = 0.$$

Demonstração. Novamente, este fato segue de P ser projetivo e possuir a resolução projetiva abaixo

$$0 \longrightarrow P \xrightarrow{1_P} P \longrightarrow 0.$$

□

Proposição 40. Para quaisquer A-módulos M e N, temos

$$\mathrm{Ext}^0_A(M,N) \cong \mathrm{Hom}_A(M,N).$$

Demonstração. Considere uma resolução projetiva de M

$$\cdots \longrightarrow P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0.$$

Como $\mathrm{Hom}_A(-, N)$ é um funtor exato à esquerda, temos a sequência exata abaixo

$$0 \longrightarrow \mathrm{Hom}_A(M, N) \xrightarrow{\varepsilon^*} \mathrm{Hom}_A(P_0, N) \xrightarrow{d_1^*} \mathrm{Hom}_A(P_1, N)$$

Por definição de cohomologia e pelo Teorema do Isomorfismo temos que

$$\mathrm{Ext}_A^0(M, N) = \frac{\mathrm{Ker}(d_1^*)}{0} = \frac{\mathrm{Img}(\varepsilon^*)}{0} \cong \mathrm{Hom}_A(M, N).$$

□

De maneira dual, podemos tomar uma resolução injetiva do A-módulo N, aplicar o funtor $G(-) = \mathrm{Hom}_A(M, -)$ e calcular as cohomologias obtendo os grupos abelianos

$$\mathrm{ext}_A^i(M, N).$$

Estas cohomologias são independentes da escolha de resolução injetiva de N, se anulam nos níveis $i \geq 1$ quando N é injetivo e coincidem com o grupo de homomorfismos no nível $i = 0$.

O teorema a seguir é a versão para o funtor Ext (,) do Teorema 12 e sua demonstração é análoga à do teorema citado.

Teorema 13. Sejam M e N A-módulos à esquerda (ou à direita). Então para cada $i \geq 0$ temos

$$\mathrm{Ext}_A^i(M, N) \cong \mathrm{ext}_A^i(M, N).$$

Dados um A-módulo à esquerda (ou à direita) M e uma sequência exata curta de A-módulos à esquerda (ou à direita)

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$$

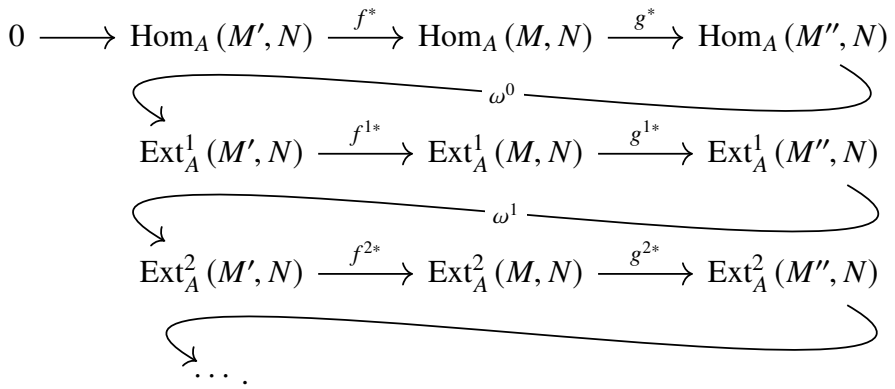
temos uma sequência exata longa de cohomologia

$$\begin{array}{l}
0 \longrightarrow \mathrm{Hom}_A(M, N') \xrightarrow{f_*} \mathrm{Hom}_A(M, N) \xrightarrow{g_*} \mathrm{Hom}_A(M, N'') \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \overset{\omega^0}{\curvearrowright} \\
\mathrm{Ext}_A^1(M, N') \xrightarrow{f_*^1} \mathrm{Ext}_A^1(M, N) \xrightarrow{g_*^1} \mathrm{Ext}_A^1(M, N'') \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \overset{\omega^1}{\curvearrowright} \\
\mathrm{Ext}_A^2(M, N') \xrightarrow{f_*^2} \mathrm{Ext}_A^2(M, N) \xrightarrow{g_*^2} \mathrm{Ext}_A^2(M, N'') \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \curvearrowright \\
\cdots .
\end{array}$$

De maneira similar, dados um A-módulo à esquerda (ou à direita) N e uma sequência exata curta de A-módulos à esquerda (ou à direita)

$$0 \longrightarrow M'' \xrightarrow{g} M \xrightarrow{f} M' \longrightarrow 0$$

temos uma sequência exata longa de cohomologia



CAPÍTULO

4

(CO)HOMOLOGIA DE GRUPOS

Neste último capítulo trataremos do objetivo central desta dissertação: a cohomologia de grupos. Traremos as definições básicas da teoria, faremos o cálculo de alguns grupos de homologia e de cohomologia e finalizaremos atacando o problema da extensão de grupos. Os resulados apresentados aqui podem ser encontrados em vários livros que tratam de álgebra homológica e de cohomologia de grupos, em especial, citamos os livros de Brown (1982), Rotman (2014), Hilton e Stammbach (1996) e Lluis-Puebla (2005) que serviram de base para este trabalho.

Na primeira seção deste capítulo final, definiremos a álgebra de um grupo sobre um anel e particularizaremos para o anel dos números inteiros, construindo o anel integral de um grupo, e finalizaremos com o conceito de módulo sobre um grupo. Na segunda seção definiremos a homologia e a cohomologia de grupos com coeficientes em um módulo sobre o grupo. Na terceira seção passaremos ao cálculo da homologia e cohomologia de grupos cíclicos. Em seguida, na quarta seção, apresentaremos uma resolução projetiva do anel dos números inteiros, baseada na construção topológica do complexo simplicial de um espaço topológico e a utilizaremos para dar um descrição alternativa dos grupos de cohomologia na quinta seção.

Nas seções seguintes deste capítulo, calcularemos alguns grupos de homologia e cohomologia, na sexta seção os grupos no nível zero enquanto que na sétima seção os grupos no nível um para o caso de módulos triviais. Finalmente, na oitava e nona seções trataremos do problema da extensão de grupos utilizando os grupos de cohomologia no nível um e dois para responder a este problema sob uma hipótese adicional.

O problema da extensão de grupos consiste em dados dois grupos K e Q, encontrar todos os grupos E, a menos de isomorfismo, que possuem um subgrupo normal isomorfo a K com quociente associado isomorfo a Q, neste caso dizemos que E é uma extensão de K por Q.

Como ressaltado por Rotman (2009), a importância desse problema pode ser percebida através do Teorema de Jordan-Hölder como segue. Suponha que um grupo E possui uma série

de composição

$$E = K_0 \geq K_1 \geq \cdots \geq K_{n-1} \geq K_n = \{1\}$$

com grupos quociente simples $Q_i = K_{i-1}/K_i$ para todo $i \geq 1$. Como $K_n = \{1\}$, então $Q_n = K_{n-1}$. Se pudéssemos resolver o problema da extensão de grupos, então K_{n-2} poderia ser recuperado de Q_n e Q_{n-1}, já que é uma extensão de $K_{n-1} = Q_n$ por Q_{n-1}. De maneira semelhante, K_{n-3} poderia ser recuperado de Q_n, Q_{n-1} e Q_{n-2}, já que é uma extensão de K_{n-2} por Q_{n-2}. Iterando esta construção, poderíamos recuperar o grupo E usando os grupos simples Q_i. Como os grupos simples finitos já foram completamente classificados, então ao resolver o problema da extensão de grupos teríamos uma descrição completa de todos os grupos finitos.

4.1 A álgebra de grupo

Seja G um grupo escrito multiplicativamente e A um anel comutativo com unidade. A A-álgebra de grupo de G sobre A, denotada por $A[G]$, é o conjunto de somas formais do tipo

$$\alpha = \sum_{g \in G} a_g g$$

com $a_g \in A$ para todo $g \in G$ e $a_g \neq 0$ apenas para um número finito de índices.

As operações de adição, multiplicação e multiplicação por escalar estão definidas por

$$\begin{aligned}
\alpha + \beta &= \left(\sum_{g \in G} a_g g\right) + \left(\sum_{g \in G} b_g g\right) = \sum_{g \in G} (a_g + b_g) g, \\
\alpha \cdot \beta &= \left(\sum_{g \in G} a_g g\right) \cdot \left(\sum_{h \in G} b_h h\right) = \sum_{g,h \in G} (a_g b_h)(gh), \\
a \cdot \alpha &= a \cdot \left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a a_g g.
\end{aligned}$$

Podemos reescrever o produto $\alpha \cdot \beta$ como

$$\alpha \cdot \beta = \sum_{u \in G} C_u u \quad \text{com} \quad C_u = \sum_{gh=u} a_g b_h.$$

Note ainda que G pode ser mergulhado em $A[G]$ pela identificação: $g \mapsto 1_A g$ e que os elementos do tipo $1_A g$ são inversíveis com inversos dados por $1_A g^{-1}$.

No exemplo abaixo damos uma caracterização das álgebras de grupo para produtos diretos de grupos cíclicos finitos. Lembrando que se G e H são dois grupos, então $G \times H$ é o grupo cujo conjunto de elementos é o produto cartesiano dos conjuntos de elementos de G por H e cuja operação é definida pontualmente. Para uma família $\{G_i\}_{i=0}^n$ de grupos, o seu produto direto será denotado por $\prod_{i=0}^n G_i$.

Exemplo 21. Sejam $\{G_i = \langle g_i \rangle\}_{i=0}^n$ uma família finita de grupos cíclicos finitos de ordem m_i, respectivamente, e A um anel comutativo com unidade. Então

$$A\left[\prod_{i=0}^{n} G_i\right] \cong \frac{A[X_1, \ldots, X_n]}{(X_1^{m_1} - 1, \ldots, X_n^{m_n} - 1)}.$$

Para simplificar a notação usaremos $x_i = X_i + (X_1^{m_1} - 1, \ldots, X_n^{m_n} - 1)$ e e_i o elemento neutro de G_i, para $i = 0, \ldots, n$, $P = \prod_{i=0}^n G_i$ e $I = (X_1^{m_1} - 1, \ldots, X_n^{m_n} - 1)$. Para mostrar o isomorfismo basta provar que os homomorfismos de anéis inversos um do outro abaixo estão bem definidos:

$$\begin{aligned} \varphi : A\left[\prod_{i=0}^{n} G_i\right] &\longrightarrow \frac{A[X_1, \ldots, X_n]}{(X_1^{m_1} - 1, \ldots, X_n^{m_n} - 1)} \\ (g_1^{j_1}, \ldots, g_n^{j_n}) &\longmapsto x_1^{j_1} \cdots x_n^{j_n}, \end{aligned}$$

$$\begin{aligned} \psi : \frac{A[X_1, \ldots, X_n]}{(X_1^{m_1} - 1, \ldots, X_n^{m_n} - 1)} &\longrightarrow A\left[\prod_{i=0}^{n} G_i\right] \\ x_1^{j_1} \cdots x_n^{j_n} &\longmapsto (g_1^{j_1}, \ldots, g_n^{j_n}). \end{aligned}$$

É claro que φ está bem definido e não há nada a ser verificado. Só nos resta mostrar que ψ é independente da escolha de representantes para a classe de equivalência.

Sejam $p = p(X_1, \ldots, X_n), q = q(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ tais que $\overline{p} = p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n) = \overline{q}$, então $p - q \in I$, isto é, existem $r_1, \ldots, r_n \in A[X_1, \ldots, X_n]$ tais que $p = q + r_1(X_1^{m_1} - 1) + \cdots + r_n(X_n^{m_n} - 1)$, logo

$$\begin{aligned} \psi(\overline{p}) &= \psi(\overline{q + r_1(X_1^{m_1} - 1) + \cdots + r_n(X_n^{m_n} - 1)}) \\ &= \psi(\overline{q} + \overline{r_1}(x_1^{m_1} - 1) + \cdots + \overline{r_n}(x_n^{m_n} - 1)) \\ &= \psi(\overline{q}) + \psi(\overline{r_1})\psi(x_1^{m_1} - 1) + \cdots + \psi(\overline{r_n})\psi(x_n^{m_n} - 1) \\ &= \psi(\overline{q}) + \psi(\overline{r_1})((g_1, e_2, \ldots, e_n)^{m_1} - 1) + \cdots + \psi(\overline{r_n})((e_1, \ldots, e_{n-1}, g_n)^{m_n} - 1) \\ &= \psi(\overline{q}) + \psi(\overline{r_1})(1 - 1) + \cdots + \psi(\overline{r_n})(1 - 1) \\ &= \psi(\overline{q}). \end{aligned}$$

Se $A = \mathbb{K}$ é um corpo, então a álgebra de grupo do exemplo acima é noetheriana e traz grande interesse, pois aparece no estudo de Geometria Algébrica clássica.

A partir daqui interpretaremos as definições anteriores para o anel dos números inteiros $A = \mathbb{Z}$. A $\mathbb{Z}$-álgebra de grupo $\mathbb{Z}[G]$ é chamada de anel integral do grupo G (lembre que $\mathbb{Z}$-álgebra e anel são conceitos equivalentes assim como $\mathbb{Z}$-módulo e grupo abeliano).

Exemplo 22. Seja $G = \langle g \rangle$ o grupo cíclico de ordem infinita e $\mathbb{Z}$ o anel dos números inteiros. Então

$$\mathbb{Z}[G] \cong \mathbb{Z}[X, X^{-1}].$$

De fato, as aplicações $g \mapsto X$ e $X \mapsto g$ induzem homomorfismos de anéis inversos um do outro. O anel $\mathbb{Z}[X, X^{-1}]$ é chamado de anel de polinômios de Laurent, nele os polinômios podem possuir potências negativas da indeterminada X. Este é mais um exemplo interessante, pois este anel é local, já que é isomorfo à localização do anel $\mathbb{Z}[X]$ no ideal maximal $\mathfrak{m} = (X)$.

Proposição 41. Para todo grupo G escrito multiplicativamente e para todo anel A temos a seguinte bijeção

$$\mathfrak{Ring}(\mathbb{Z}[G], A) \cong \mathfrak{Group}(G, A^{\times}),$$

entre o conjunto de homomorfismos de anel de $\mathbb{Z}[G]$ em B e o conjunto de homomorfismos de grupo de G em $A^{\times}$.

Demonstração. Dado um homomorfismo de anéis $\varphi : \mathbb{Z}[G] \to A$, temos que φ preserva o produto e as unidades, então $\overline{\varphi} = \varphi|_G : G \to A^{\times}$ é um homomorfismo de grupos. Por outro lado, dado um homomorfismo de grupos $\psi : G \to A^{\times}$, defina $\tilde{\psi} : \mathbb{Z}[G] \to A$ por

$$\tilde{\psi}\left(\sum_{g \in G} z_g g\right) = \sum_{g \in G} z_g \psi(g).$$

As aplicações $\varphi \mapsto \overline{\varphi}$ e $\psi \mapsto \tilde{\psi}$ são inversas um da outra e portanto temos a bijeção desejada. □

Definição 43. Seja G um grupo escrito multiplicativamente. Um G-módulo à esquerda é um grupo abeliano M juntamente com um homomorfismo de grupos

$$\begin{aligned} \psi : G &\to \mathrm{Aut}(M) \\ g &\mapsto \psi_g \end{aligned}$$

Exemplo 23. Considere os grupos $G = \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\} \cong C_2 = \{1, a\}$ e $M = \mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$. Veremos que M pode ser visto como G-módulo e calcularemos de quantas maneiras distintas isto pode ocorrer.

Para que M possa ser visto como G-módulo, devemos encontrar um homomorfismo de grupos $\varphi : G \to \mathrm{Aut}(M)$, mas $\mathrm{Aut}(M) = \{Id_M, \mu : \overline{2} \mapsto \overline{3}\} \cong G$, então isso é o mesmo que encontrar um endomorfismo de G, mas $\mathrm{End}(G) = \{0, Id_G\}$, isto é, M pode ser visto como G-módulo de duas maneiras diferentes.

$$\begin{aligned} G &\xrightarrow{0} G \xrightarrow{\cong} \mathrm{Aut}(M) \\ 1 &\longmapsto 1 \longmapsto Id_M \\ a &\longmapsto 1 \longmapsto Id_M \end{aligned} \qquad \begin{aligned} G &\xrightarrow{Id_G} G \xrightarrow{\cong} \mathrm{Aut}(M) \\ 1 &\longmapsto 1 \longmapsto Id_M \\ a &\longmapsto a \longmapsto \mu \end{aligned}$$

Denotamos a imagem de um elemento $m \in M$ pela ação de um automorfismo ψ_g por $\psi_g(m) = g \cdot m$, ou simplesmente $\psi_g(m) = gm$.

Segue da definição que o homomorfismo ψ atua como uma multiplicação por escalar

$$\begin{aligned} \cdot : G \times M &\to M \\ (g, m) &\mapsto g \cdot m \end{aligned}$$

que satisfaz os seguintes axiomas:

- $g_1 \cdot (g_2 \cdot m) = (g_1 g_2) \cdot m, \quad g_1, g_2 \in G, \quad m \in M$;
- $g \cdot (m_1 + m_2) = g \cdot m_1 + g \cdot m_2, \quad g \in G, \quad m_1, m_2 \in M$;
- $1_G \cdot m = m, \quad m \in M$.

Reciprocamente, dada uma função $* : G \times M \to M$ que satisfaz os axiomas acima, obtemos um homomorfismo de grupos $\varphi : G \to \mathrm{Aut}(M)$ que equipa M com uma estrutura de G-módulo à esquerda.

De maneira dual, um G-módulo à direita é o mesmo que um G^{op}-módulo à esquerda, aqui G^{op} é o grupo oposto de G, no qual a operação é dada por $g \cdot_{op} h = h \cdot g$ para todo $g, h \in G$. Além disso, todo G-módulo à esquerda M pode ser visto como um G-módulo à direita, e vice versa, via a identificação $gm = mg^{-1}$, para $g \in G$ e $m \in M$.

Agora lembraremos a definição de módulo para o anel $A[G]$ a fim de mostrar que G-módulos e $A[G]$-módulos são conceitos equivalentes.

Definição 44. Seja G um grupo escrito multiplicativamente. Um $A[G]$-módulo é um grupo abeliano M juntamente com um homomorfismo de anéis

$$\varphi : A[G] \to \mathrm{End}(M).$$

Como para qualquer grupo abeliano M temos que $\mathrm{Aut}(M) = (\mathrm{End}(M))^\times$, então pela bijeção provada anteriormente, podemos ver M tanto como um G-módulo quanto como um $A[G]$-módulo.

Um G-módulo M será dito trivial se o seu homomorfismo de estrutura $\psi : G \to \mathrm{Aut}(M)$ for trivial, ou seja, se todos os elementos de G agirem como a identidade em M. Perceba que todo grupo abeliano pode ser visto como um G-módulo trivial, em particular, o grupo abeliano do anel A sempre será considerado um G-módulo trivial.

4.2 Definição de (co)homologia de grupos

Pela bijeção provada entre homomorfismos de grupo e homomorfismos de anéis, o homomorfismo de grupos trivial de G em $\mathbb{Z}^\times = \{1, -1\}$ que leva todo $g \in G$ em $1 \in \mathbb{Z}^\times$, induz

um homomorfismo de anéis $\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$ chamado de homomorfismo de aumento de $\mathbb{Z}[G]$. O núcleo de ε será chamado de ideal de aumento de $\mathbb{Z}[G]$ e denotado por I_G. Um elemento típico de I_G é da forma $\sum_{g\in G} z_g g$ tal que $\sum_{g\in G} z_g = 0$.

Lema 5. Seja G um grupo escrito multiplicativamente. Então:

1. Como grupo abeliano I_G é livre sobre o conjunto $W = \{g - 1; g \in G, g \neq 1\}$;
2. Seja S um conjunto de geradores de G. Então, como $\mathbb{Z}[G]$-módulo, I_G é gerado por $S - 1 = \{s - 1; s \in S\}$.

Demonstração. (1.) Para mostrar esta afirmação devemos provar que W é uma base para I_G, isto é, mostrar que W é um conjunto gerador de I_G linearmente independente.

Para isso considere a combinação linear

$$\alpha_1(g_1 - 1) + \cdots + \alpha_n(g_n - 1) = 0$$

com $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$ e $g_1, \ldots, g_n \in G$, então temos

$$\alpha_1 g_1 + \cdots + \alpha_n g_n + (-\alpha_1 - \cdots - \alpha_n) \cdot 1 = 0,$$

mas como $\mathbb{Z}[G]$ como grupo abeliano é livre sobre G, então $\alpha_1 = \cdots = \alpha_n = 0$ e portanto W é um conjunto linearmente independente.

Agora seja $\sum_{g\in G} z_g g \in I_G$, então $\sum_{g\in G} z_g = 0$ e assim $\sum_{g\in G} z_g g = \sum_{g\in G, g\neq 1} z_g(g - 1)$, isto é, W gera I_G.

(2.) Da parte 1 deste lema temos que é suficiente mostrar que se $g \in G$ e $g \neq 1$, então $g - 1 \in \langle S - 1\rangle$ o G-módulo gerado por $S - 1$.

Primeiramente note que se $g, h \in G$, então

$$\begin{aligned} gh - 1 &= g(h - 1) + (g - 1), \\ g^{-1} - 1 &= -g^{-1}(g - 1), \\ g &= s_1^{e_1} \cdots s_k^{e_k} \end{aligned}$$

com $s_1, \ldots, s_k \in S$ e $e_1, \ldots, e_k \in \{1, -1\}$. Assim, procederemos por indução sobre k.

Se $g = s_1^{e_1}$, então $g - 1 = s_1^{e_1} - 1$ e assim

$$g - 1 = \begin{cases} s_1 - 1, & \text{se } e_1 = 1 \\ -s_1^{-1}(s_1 - 1), & \text{se } e_1 = -1, \end{cases}$$

e em ambos os casos temos $g - 1 \in \langle S - 1\rangle$.

Se $g = s_1^{e_1} \cdots s_k^{e_k}$, então $g - 1 = s_1^{e_1}(s_2^{e_2} \cdots s_k^{e_k} - 1) + (s_1^{e_1} - 1)$, pela hipótese de indução temos $s_1^{e_1}, s_2^{e_2} \cdots s_k^{e_k} \in \langle S - 1\rangle$, logo $g - 1 \in \langle S - 1\rangle$. □

A partir desta seção usaremos G ao invés de $\mathbb{Z}[G]$ nos símbolos $M \otimes_G N$, $\mathrm{Hom}_G(M,N)$, $\mathrm{Tor}_i^G(M,N)$ e $\mathrm{Ext}_G^i(M,N)$.

Definição 45. O i-ésimo grupo de cohomologia de G com coeficientes no G-módulo M é o grupo abeliano

$$H^i(G,M) = \mathrm{Ext}_G^i(\mathbb{Z},M).$$

O i-ésimo grupo de homologia de G com coeficientes no G-módulo M é o grupo abeliano

$$H_i(G,M) = \mathrm{Tor}_i^G(M,\mathbb{Z}).$$

Lembrando que $\mathbb{Z}$ deve ser visto como G-módulo trivial. Temos ainda que $H^i(G,-)$ e $H_i(G,-)$ são funtores covariantes e podem ser obtidos pelo seguinte procedimento: tome $P_\bullet$ uma resolução projetiva de $\mathbb{Z}$ como G-módulo; forme a resolução projetiva deletada $P_\bullet^{\mathbb{Z}}$ e obtenha os complexos $\mathrm{Hom}_G\left(P_\bullet^{\mathbb{Z}}, M\right)$ e $M \otimes_G P_\bullet^{\mathbb{Z}}$; calcule a (co)homologia no nível i.

4.3 (Co)homologia de grupos cíclicos

Nesta seção calcularemos as homologias e as cohomologias de grupos cíclicos. Começando por grupos cíclicos infinitos e finalizando com grupos cíclicos finitos.

Exemplo 24. Considere $G = \langle g \rangle \cong \mathbb{Z}$ um grupo cíclico de ordem infinita e seja M um G-módulo. Então temos a seguinte resolução projetiva (livre) de $\mathbb{Z}$ como G-módulo trivial

$$\cdots \longrightarrow 0 \longrightarrow \mathbb{Z}[G] \xrightarrow{d\cdot} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0,$$

aqui $d\cdot$ é a multiplicação por $d = (g-1)$, cuja imagem é $\mathrm{Img}(d\cdot) = \{\alpha(g-1); \alpha \in \mathbb{Z}[G]\} = I_G = \mathrm{Ker}(\varepsilon)$ e que é claramente injetiva.

Deletando $\mathbb{Z}$, aplicando o funtor $M \otimes_G -$ e substituindo os isomorfismos adequados, obtemos o complexo

$$\cdots \longrightarrow 0 \longrightarrow M \xrightarrow{d\cdot} M \longrightarrow 0.$$

Deletando $\mathbb{Z}$, aplicando o funtor $\mathrm{Hom}_G(-,M)$ e substituindo os isomorfismos adequados, obtemos o cocomplexo

$$0 \longrightarrow M \xrightarrow{d\cdot} M \longrightarrow 0 \longrightarrow \cdots.$$

Por fim, calculando as homologias e cohomologias obtemos

$$H_i(G,M) = \begin{cases} M_G, & \text{se } i = 0; \\ M^G, & \text{se } i = 1; \\ 0, & \text{se } i \geq 2. \end{cases} \qquad H^i(G,M) = \begin{cases} M^G, & \text{se } i = 0; \\ M_G, & \text{se } i = 1; \\ 0, & \text{se } i \geq 2. \end{cases}$$

Aqui $M_G = M/\{m(g-1); m \in M\}$ é o grupo dos coinvariantes e $M^G = \{m \in M; m(g-1) = 0\}$ é o grupo dos invariantes.

Exemplo 25. Considere $G = \langle g | g^n = 1 \rangle \cong \mathbb{Z}/n\mathbb{Z}$ um grupo cíclico finito de ordem n e seja M um G-módulo. Então temos a seguinte resolução projetiva de $\mathbb{Z}$ como G-módulo trivial

$$\cdots \longrightarrow \mathbb{Z}[G] \xrightarrow{n\cdot} \mathbb{Z}[G] \xrightarrow{d\cdot} \mathbb{Z}[G] \xrightarrow{n\cdot} \mathbb{Z}[G] \xrightarrow{d\cdot} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0,$$

aqui $d\cdot$ e $n\cdot$ são a multiplicação por $d = g - 1$ e por $n = 1 + g + \cdots + g^{n-1}$, respectivamente. Assim, $d \cdot n\cdot = n \cdot d\cdot$ é a multiplicação por $g^n - 1 = 0$ e então temos que $\mathrm{Img}(d\cdot) \subseteq \mathrm{Ker}(n\cdot)$ e $\mathrm{Img}(n\cdot) \subseteq \mathrm{Ker}(d\cdot)$, além disso claramente $\varepsilon d\cdot = 0$ e, portanto, $\mathrm{Img}(d\cdot) \subseteq \mathrm{Ker}(\varepsilon)$.

Por outro lado, denotando os elementos de $\mathbb{Z}[G]$ na forma $a = \sum_{i=0}^{n-1} a_i g^i$ temos que

- se $\varepsilon(a) = 0$, então $a = d \cdot b$ com $b_i = a_{i+1} + \cdots + a_{n-1}$ para $0 \leq i \leq n-2$ e $b_{n-1} = 0$, portanto $\mathrm{Ker}(\varepsilon) \subseteq \mathrm{Img}(d\cdot)$;
- se $d \cdot a = 0$, então $a = n \cdot b$ com $b_0 = a_0$ e $b_i = 0$ para $1 \leq i \leq n-1$, portanto $\mathrm{Ker}(d\cdot) \subseteq \mathrm{Img}(n\cdot)$;
- se $n \cdot a = 0$, então $\varepsilon(a) = 0$, portanto $\mathrm{Ker}(n\cdot) \subseteq \mathrm{Ker}(\varepsilon) \subseteq \mathrm{Img}(d\cdot)$.

Isso prova a exatidão necessária na resolução acima.

Deletando $\mathbb{Z}$, aplicando o funtor $M \otimes_G -$ e substituindo os isomorfismos adequados, obtemos o complexo

$$\cdots \longrightarrow M \xrightarrow{n\cdot} M \xrightarrow{d\cdot} M \xrightarrow{n\cdot} M \xrightarrow{d\cdot} M \longrightarrow 0.$$

Deletando $\mathbb{Z}$, aplicando o funtor $\mathrm{Hom}_G(-, M)$ e substituindo os isomorfismos adequados, obtemos o cocomplexo

$$0 \longrightarrow M \xrightarrow{d\cdot} M \xrightarrow{n\cdot} M \xrightarrow{d\cdot} M \xrightarrow{n\cdot} M \longrightarrow \cdots.$$

Note que $n(gm - m) = 0$ e $gn(m) = n(m)$ para todo $m \in M$, portanto $n\cdot : M \to M$ induz um homomorfismo de grupos $\overline{n\cdot} : M_G \to M^G$. Este homomorfismo é tal que

$$\mathrm{Ker}(\overline{n\cdot}) \cong \frac{\mathrm{Ker}(n\cdot)}{\mathrm{Img}(d\cdot)}$$
$$\mathrm{Coker}(\overline{n\cdot}) \cong \frac{\mathrm{Ker}(d\cdot)}{\mathrm{Img}(n\cdot)}.$$

Por fim, calculando as homologias e cohomologias obtemos

$$H_i(G, M) = \begin{cases} M_G, & \text{se } i = 0; \\ \mathrm{Coker}(\overline{n\cdot}), & \text{se } i > 0 \text{ com } i \text{ ímpar}; \\ \mathrm{Ker}(\overline{n\cdot}), & \text{se } i > 0 \text{ com } i \text{ par}. \end{cases}$$

$$H^i(G, M) = \begin{cases} M^G, & \text{se } i = 0; \\ \mathrm{Ker}(\overline{n\cdot}), & \text{se } i > 0 \text{ com } i \text{ ímpar}; \\ \mathrm{Coker}(\overline{n\cdot}), & \text{se } i > 0 \text{ com } i \text{ par}. \end{cases}$$

4.4 Resoluções padrão de $\mathbb{Z}$ como G-módulo trivial

Nesta seção calcularemos uma resolução projetiva de $\mathbb{Z}$ visto como $\mathbb{Z}[G]$-módulo trivial.

Seja $G^{i+1} = \{(g_0, \ldots, g_i); g_j \in G, j = 0, \ldots, i\}$ e considere o grupo abeliano livre $B_i(G)$ com base G^{i+1}, isto é, elementos de $B_i(G)$ são somas finitas formas de elementos de G^{i+1} com coeficientes inteiros. Podemos dar uma estrutura de G-módulo a $B_i(G)$ via

$$g(g_0, \ldots, g_i) = (gg_0, \ldots, gg_i), \quad g, g_0, \ldots, g_i \in G.$$

Agora para $0 \leq j \leq i$ seja $\hat{d}_j : G^{i+1} \to G^i$ a função dada por $(g_0, \ldots, g_i) \mapsto (g_0, \ldots, g_{j-1}, g_{j+1}, \ldots, g_i)$ e considere o G-homomorfismo induzido $d_j : B_i(G) \to B_{i-1}(G)$. Finalmente, defina o G-homomorfismo $\partial_i : B_i(G) \to B_{i-1}(G)$ dado por

$$\partial_i = \sum_{j=0}^{i} (-1)^j d_j.$$

Teorema 14. A sequência de G-módulos e G-homomorfismos abaixo, com ε o homomorfismo de aumento, é uma resolução livre de $\mathbb{Z}$ visto como G-módulo trivial.

$$\cdots \longrightarrow B_2(G) \xrightarrow{\partial_2} B_1(G) \xrightarrow{\partial_1} B_0(G) \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

Esta resolução é chamada de resolução padrão não normalizada de $\mathbb{Z}$ como G-módulo trivial.

Demonstração. Claramente temos que cada $B_i(G)$ é um G-módulo livre com base $\{(1_G, g_1, \ldots, g_i); g_j \in G, j = 1, \ldots, i\}$.

Temos que $\varepsilon\partial_1 = 0$. De fato,

$$\varepsilon(\partial_1(g_0, g_1)) = \varepsilon(g_1 - g_0) = 1 - 1 = 0.$$

Para mostrar que $\partial_{i-1}\partial_i = 0$ para $i \geq 2$, primeiramente note que $0 \leq j < k \leq i$ vale $d_j d_k = d_{k-1} d_j$. De fato,

$$\begin{aligned} d_j(d_k(g_0, \ldots, g_i) &= d_j(g_0, \ldots, g_{k-1}, g_{k+1}, \ldots, g_i) \\ &= (g_0, \ldots, g_{j-1}, g_{j+1}, \ldots, g_{k-1}, g_{k+1}, \ldots, g_i) \\ &= d_{k-1}(g_0, \ldots, g_{j-1}, g_{j+1}, \ldots, g_i) \\ &= d_{k-1}(d_j(g_0, \ldots, g_i)). \end{aligned}$$

Então temos

$$\begin{aligned}\partial_{i-1}\partial_i &= \partial_{i-1}\left(\sum_{j=1}^{i}(-1)^j d_j\right)\\ &= \sum_{k=0}^{i-1}(-1)^k d_k\left(\sum_{j=1}^{i}(-1)^j d_j\right)\\ &= \sum_{k=0}^{i-1}\left(\sum_{j=0}^{i}(-1)^{j+k}(d_k d_j)\right)\\ &= \sum_{k<j}(-1)^{k+j}(d_k d_j) + \sum_{j\leq k}(-1)^{k+j}(d_k d_j).\end{aligned}$$

Note que existe uma bijeção entre as famílias de índices

$$A = \{(k,j); 0 \leq k < j, 0 < j \leq i\} \text{ e } B = \{(k',j'); j' \leq k' \leq i-1, 0 \leq j' < i\}$$

dada por

$$(k,j) \mapsto (k',j') = (j-1,k) \quad \text{e} \quad (k',j') \mapsto (k,j) = (j',k'+1).$$

Sob esta bijeção temos as correspondências

$$\begin{aligned}(-1)^{k+j} &\mapsto (-1)^{k+j-1}\\ d_k d_j &\mapsto d_{j-1}d_k,\end{aligned}$$

mas da observação acima temos que termos correspondentes se anulam e portanto a soma é zero, como queríamos demonstrar.

Para a exatidão mostraremos que $(B_\bullet(G);\partial_\bullet)$ tem homotopia contrátil.

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & B_2(G) & \xrightarrow{\partial_2} & B_1(G) & \xrightarrow{\partial_1} & B_0(G) & \xrightarrow{\varepsilon} & \mathbb{Z} & \longrightarrow & 0\\
 & & \downarrow Id & \swarrow s_1 & \downarrow Id & \swarrow s_0 & \downarrow Id & \swarrow s_{-1} & \downarrow Id & & \\
\cdots & \longrightarrow & B_2(G) & \xrightarrow[\partial_2]{} & B_1(G) & \xrightarrow[\partial_1]{} & B_0(G) & \xrightarrow{\varepsilon} & \mathbb{Z} & \longrightarrow & 0.
\end{array}$$

Defina $s_{-1}:\mathbb{Z}\to B_0(G)$ por $s_{-1}(1)=1_G$, então para $z\in\mathbb{Z}$ temos

$$\varepsilon(s_{-1}(z)) = \varepsilon(z\cdot 1_G) = z.$$

Para $i\geq 0$ defina $s_i : B_i(G)\to B_{i-1}(G)$ por $s_i(g_0,\ldots,g_i) = (1_G,g_0,\ldots,g_i)$. Então para $g\in G$ temos

$$(s_{-1}\varepsilon + \partial_1 s_0)(g) = s_{-1}(\varepsilon(g)) + \partial_1(s_0(g)) = s_{-1}(1) + \partial_1(1_G,g) = 1_G + g - 1_G = g$$

e para $i\geq 1$, $0\leq j\leq i$ e $(g_0,\ldots,g_i)\in G^{i+1}$ temos

$$\begin{aligned}(d_{j+1}s_i - s_{i-1}d_j)(g_0,\ldots,g_i) &= d_{j+1}(s_i(g_0,\ldots,g_i)) - s_{i-1}(d_j(g_0,\cdots,g_i))\\ &= d_{j+1}(1_G,g_0,\ldots,g_i) - s_{i-1}(g_0,\ldots,g_{j-1},g_{j+1},\ldots,g_i)\\ &= (1_G,g_0,\ldots,g_{j-1},g_{j+1},\ldots,g_i) - (1_G,g_0,\ldots,g_{j-1},g_{j+1},\ldots,g_i)\\ &= 0,\end{aligned}$$

e finalmente concluímos que

$$\begin{aligned}
\partial_{i+1}s_i + s_{i-1}\partial_i &= \sum_{j=0}^{i+1}(-1)^j(d_j s_i) + s_{i-1}\left(\sum_{j=0}^{i}(-1)^j d_j\right) \\
&= \sum_{j=0}^{i+1}(-1)^j(d_j s_i) + \sum_{j=0}^{i}(-1)^j(s_{i-1}d_j) \\
&= d_0 s_i + \sum_{j=0}^{i}(-1)^{j+1}(d_{j+1}s_i) + \sum_{j=0}^{i}(-1)^j(s_{i-1}d_j) \\
&= d_0 s_i + \sum_{j=0}^{i}(-1)^j(s_{i-1}d_j - d_{j+1}s_i) \\
&= d_0 s_i = Id_{B_i(G)}.
\end{aligned}$$

□

Considere agora $D_i(G) \subseteq B_i(G)$ o subgrupo gerado pelas $(i+1)$-uplas $(g_0, \ldots, g_i)$ tais que $g_{k-1} = g_k$ para algum $1 \leq k \leq i$, tais $(i+1)$-uplas serão chamadas de degeneradas.

Temos que $D_i(G)$ é um G-submódulo de $B_i(G)$, gerado pelas $(i+1)$-uplas $(1_G, g_1, \ldots, g_i)$ degeneradas. Além disso, $\partial_i(D_i(G)) \subseteq D_{i+1}(G)$, pois se $(g_0, \ldots, g_i)$ é degenerada, suponha que $(g_0, \ldots, g_{k-1}, g_k, \ldots, g_i)$ com $g_{k-1} = g_k$, então $\partial_i(g_0, \ldots, g_i)$ é uma combinação linear i-uplas degeneradas somada ao termo

$$(-1)^{k-1}(g_0, \ldots, g_{k-2}, g, g_{k+1} \ldots, g_i) + (-1)^k(g_0, \ldots, g_{k-2}, g, g_{k+1}, \ldots, g_i), \qquad \text{com } g = g_{k-1} = g_k,$$

que é claramente zero. Assim, concluímos que $(D_\bullet(G), \partial_\bullet)$ é um cocomplexo de cadeia chamado de subcocomplexo degenerado de $(B_\bullet(G), \partial_\bullet)$. Aqui chamamos atenção ao fato que $D_0 = 0$, por convenção.

Note que a homotopia contrátil de $(B_\bullet(G), \partial_\bullet)$ é tal que $s_i(D_i(G)) \subseteq D_{i+1}(G)$ para todo $i \leq 0$, consequentemente, passando ao cocomplexo formado pelos quocientes $\overline{B}_i(G) = \dfrac{B_i(G)}{D_i(G)}$, concluímos que cada G-módulo $\overline{B}_i(G)$ é livre, com base formada pela $(i+1)$-uplas $(g_0, \ldots, g_i)$ tais que $g_{k-1} \neq g_k$ para todo $1 \leq k \leq i$, e $(\overline{B}_\bullet(G), \overline{\partial}_\bullet)$ é uma resolução live de $\mathbb{Z}$ visto como G-módulo trivial, chamada de resolução padrão normalizada de $\mathbb{Z}$ como G-módulo trivial.

4.5 Descrição alternativa dos grupos de cohomologia

A resolução livre padrão não normalizada de $\mathbb{Z}$ dada na seção anterior nos permite calcular explicitamente os grupos de cohomologia $H^i(G, M)$. Na sequência daremos uma caracterização alternativa de tais grupos.

Seja N um G-módulo à esquerda. Definimos o cocomplexo $(C^\bullet(G, M), \delta^\bullet)$ como segue. Para $i < 0$ fazemos $C^i(G, M) = 0$. Para $i \geq 0$, definimos $C^i(G, M)$ como o grupo abeliano das

funções de G^i em M com adição dada pontualmente. Por convenção, escolhemos G^0 como sendo o conjunto unitário $\{1_G\}$ composto apenas pelo elemento neutro de G. Os homomorfismos são dados por

$$\begin{aligned} \delta^i : C^{i-1}(G,M) &\to C^i(G,M) \\ f &\mapsto \delta^i(f) = \sum_{j=0}^{i} d^j(f) \end{aligned}$$

com $d^j : C^{i-1}(G,M) \to C^i(G,M)$ definida por

$$d^j(f)(g_1,\ldots,g_i) = \begin{cases} g_1 \cdot f(g_2,\ldots,g_i), & \text{se } j = 0 \\ f(g_1,\ldots,g_{j-1},g_jg_{j+1},g_{j+2},\ldots,g_i), & \text{se } 1 \leq j \leq i-1 \\ f(g_1,\ldots,g_{i-1}), & \text{se } j = i. \end{cases}$$

Note que temos $C^0(G,M) \cong M$ e $\delta^1 : C^0(G,M) \to C^1(G,M)$ dada por $\delta^1(m)(g) = gm - m$ para todo $m \in M$ e $g \in G$. O fato de que $(C^\bullet(G,M), \delta^\bullet)$ é realmente um cocomplexo segue do teorema abaixo.

Teorema 15. Seja G um grupo escrito multiplicativamente e M um G-módulo. Então para todo $i \in \mathbb{N}$, o i-ésimo grupo de cohomologia do cocomplexo $(C^\bullet(G,M), \delta^\bullet)$ é isomorfo a $H^i(G,M)$.

Demonstração. Usando a resolução padrão de $\mathbb{Z}$ como G-módulo

$$\cdots \longrightarrow B_2(G) \xrightarrow{\partial_2} B_1(G) \xrightarrow{\partial_1} B_0(G) \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

podemos calcular os grupos de cohomologia $H^i(G,M)$ que são obtidos a partir do cocomplexo abaixo

$$0 \longrightarrow \mathrm{Hom}_G(B_0(G),M) \xrightarrow{\partial_1^*} \mathrm{Hom}_G(B_1(G),M) \xrightarrow{\partial_2^*} \mathrm{Hom}_G(B_2(G),M) \longrightarrow \cdots$$

Provaremos o teorema mostrando que o cocomplexo acima é isomorfo ao cocomplexo abaixo que foi construído na discussão anterior

$$0 \longrightarrow C^0(G,M) \xrightarrow{\delta^1} C^1(G,M) \xrightarrow{\delta^2} C^2(G,M) \longrightarrow \cdots.$$

Para isso, definimos os seguintes homomorfismos de grupo para cada $i \in \mathbb{Z}$

$$\begin{aligned} \alpha_i &: \mathrm{Hom}_G(B_i(G),M) \longrightarrow C^i(G,M) \\ \beta_i &: C^i(G,M) \longrightarrow \mathrm{Hom}_G(B_i(G),M) \end{aligned}$$

dados por

$$\begin{aligned} \alpha_i(\varphi)(g_1,\ldots,g_i) &= \varphi(1_G, g_1, g_1g_2, \ldots, g_1\cdots g_i) \\ \beta_i(f)(g_0,\ldots,g_i) &= g_0 \cdot f(g_0^{-1}g_1, g_1^{-1}g_2, \ldots, g_{i-1}^{-1}g_i). \end{aligned}$$

Temos que para cada $i \in \mathbb{N}$ α_i e β_i são inversos um do outro, pois para $\varphi \in \mathrm{Hom}_G(B_i(G), M)$, $f \in C^i(G, M)$, $(g_1, \ldots, g_i) \in G^i$ e $(g_0, \ldots, g_i) \in G^{i+1}$ vale:

$$\begin{aligned}
\beta_i(\alpha_i(\varphi))(g_0, \ldots, g_i) &= g_0\alpha_i(\varphi)(g_0^{-1}g_1, g_1^{-1}g_2, \ldots, g_{i-1}^{-1}g_i) \\
&= g_0\varphi(1_G, g_0^{-1}g_1, \ldots, g_0^{-1}g_i) \\
&= \varphi(g_0, \ldots, g_i), \\
\alpha_i(\beta_i(f))(g_1, \ldots, g_i) &= \beta_i(f)(1_G, g_1, g_1g_2, \ldots, g_1 \cdots g_i) \\
&= 1_G f(g_1, \ldots, g_i) \\
&= f(g_1, \ldots, g_i).
\end{aligned}$$

Por fim, nos resta apenas mostrar que $\alpha_\bullet$ e $\beta_\bullet$ são morfismos de cocomplexos, basta então provar que para todo $i \geq 1$ e para todo $0 \leq j \leq i$ o diagrama abaixo é comutativo, isto provará também que $(C^\bullet(G, M), \delta^\bullet)$ é, realmente, um cocomplexo.

$$\begin{array}{ccc}
\mathrm{Hom}_G(B_{i-1}(G), M) & \xrightarrow{d_j^*} & \mathrm{Hom}_G(B_i(G), M) \\
{\scriptstyle\beta_{i-1}}\uparrow & & \downarrow{\scriptstyle\alpha_i} \\
C^{i-1}(G, M) & \xrightarrow[d^j]{} & C^i(G, M)
\end{array}$$

Mas para $f \in C^{i-1}(G, M)$ e $(g_1, \ldots, g_i) \in G^i$ temos

$$\begin{aligned}
&(\alpha_i(d_j^*(\beta_{i-1}(f))))(g_1, \ldots, g_i) = (d_j^*(\beta_{i-1}(f)))(1_G, g_1, g_1g_2, \ldots, g_1 \cdots g_i) \\
&= (\beta_{i-1}(f))(d_j(1_G, g_1, g_1g_2, \ldots, g_1g_i)) \\
&= \begin{cases}
\beta_{i-1}(f)(g_1, g_1 \cdots g_i), & \text{se } j = 0; \\
\beta_{i-1}(f)(1_G, g_1, g_1g_2, \ldots, g_1 \cdots g_{j-1}, g_1 \cdots g_{j+1}, \ldots, g_1 \cdots g_i), & \text{se } 1 \leq j \leq i-1; \\
\beta_{i-1}(f)(1_G, g_1, g_1g_2, \ldots, g_1 \cdots g_{i-1}), & \text{se } j = i;
\end{cases} \\
&= \begin{cases}
g_1 f(g_2, \ldots, g_i), & \text{se } j = 0; \\
f(g_1, g_2, \ldots, g_{i-1}, g_ig_{i+1}, g_{i+2}, \ldots, g_i), & \text{se } 1 \leq j \leq i-1; \\
f(g_1, \ldots, g_{i-1}), & \text{se } j = i;
\end{cases} \\
&= d^j(f)(g_1, \ldots, g_i).
\end{aligned}$$

□

Observação 18. Para cada $i \in \mathbb{N}$, chamaremos os elementos de $C^i(G, M)$ de i-cocadeias, os elementos de $\mathrm{Ker}(\delta^{i+1}) \subseteq C^i(G, M)$ de i-cociclos e os elementos de $\mathrm{Img}(\delta^i) \subseteq C^i(G, M)$ de i-cobordos.

Definição 46. Para cada $i \in \mathbb{N}$, dizemos que um elemento $f \in C^i(G, M)$ é normal quando $f(g_1, \ldots, g_i) = 0$ sempre que $g_k - 1_G$ para algum $1 \leq k \leq i$.

Definindo $\overline{C}^i(G,M) \subseteq C^i(G,M)$ como o subgrupo formados pelos elementos normais, temos que $(\overline{C}^\bullet(G,M), \delta^\bullet)$ é um cocomplexo cujo i-ésimo grupo de cohomologia é isomorfo a $H^i(G,M)$. A demonstração é feita de maneira análoga ao teorema anterior, tomando a resolução livre padrão normalizada de $\mathbb{Z}$.

4.6 Cálculo de H_0 e H^0

Nesta seção, faremos uma breve discussão sobre a homologia e a cohomologia no nível zero, dando uma caracterização para as mesmas.

Teorema 16. Seja G um grupo escrito multiplicativamente e M um G-módulo. Então

$$H_0(G,M) \cong M_G = \frac{M}{M \cdot I_G} = \frac{M}{\{m(g-1) \in M; m \in M, g \in G, g \neq 1\}},$$
$$H^0(G,M) \cong M^G = \{m \in M; gm = m, \forall g \in G\}.$$

Demonstração. Para a cohomologia, por definição temos que $H^0(G,M) = \mathrm{Hom}_G(\mathbb{Z}, M)$. Lembre-se de que um homomorfismo de grupos $\varphi : \mathbb{Z} \to M$ está unicamente determinado por $\varphi(1) = n$, assim, se φ é um G-homomorfismo, então para todo $m \in M$ temos

$$gm = g\varphi(1) = \varphi(g \cdot 1) = \varphi(1) = m.$$

Reciprocamente, dado $m \in M$ tal que $gm = m$ para todo $g \in G$, então o homomorfismo de grupos $\psi : \mathbb{Z} \to M$ dado por $\psi(1) = m$ é também um G-homomorfismo, pois para $z \in \mathbb{Z}$ temos

$$\psi(gz) = \psi(z) = zm = g(zm) = g\psi(z).$$

Agora, para a homologia, por definição temos que $H_0(G,M) = M \otimes_G \mathbb{Z}$. Como $M \otimes \mathbb{Z} \cong M$, então $M \otimes_G \mathbb{Z}$ pode ser visto como o quociente do grupo abeliano M pelo subgrupo T dos elementos da forma $mg - m = m(g-1)$ para $m \in M$ e $g \in G$. Do lema provado na seção anterior temos que os elementos $g - 1 \in \mathbb{Z}[G]$ geram o grupo abeliano I_G, então denotaremos $T = M \cdot I_G$.

Em particular, se M é um G-módulo trivial, então

$$H^0(G,M) = M \quad \text{e} \quad H_0(G,M) = M.$$

Neste caso chamamos M^G de grupo dos invariantes de M pela ação de G e M_G de grupo dos coinvariantes de M pela ação de G. □

Observação 19. Note que pela descrição dada para os grupos de cohomologia na Seção 4.5, temos que

$$H^0(G,M) \cong \mathrm{Ker}(\delta^1).$$

Perceba que as duas descrições coincidem, pois $\delta^1 : M \cong C^0(G,M) \to C^1(G,M)$ e $\delta^1(m)(g) = gm - m$, logo

$$m \in \mathrm{Ker}(\delta^1) \iff gm - m = 0, \forall g \in G \iff m \in M^G.$$

4.7 Cálculo de H_1 e H^1 com módulos de coeficientes triviais

Nesta seção calcularemos a homologia e a cohomologia no nível um com módulos de coeficientes triviais.

Teorema 17. Sejam G um grupo escrito multiplicativamente e M um G-módulo trivial. Então

$$H_1(G,M) \cong M \otimes I_G/(I_G)^2 \quad \text{e} \quad H^1(G,M) \cong \operatorname{Hom}\left(I_G/(I_G)^2, M\right).$$

Demonstração. Considere a sequência exata curta abaixo

$$0 \longrightarrow I_G \xrightarrow{\iota} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

Aplicando os funtores $\operatorname{Tor}_G^i(M,-)$ para $i = 0, 1$ obtemos a sequência exata longa abaixo

$$\begin{array}{c} \cdots \longrightarrow \operatorname{Tor}_G^1(M,\mathbb{Z}[G]) \xrightarrow{\varepsilon_*} \operatorname{Tor}_G^1(M,\mathbb{Z}) \\ \qquad\qquad\qquad\qquad\qquad\qquad \searrow^{\omega} \\ \operatorname{Tor}_G^0(M,I_G) \xrightarrow{\iota_*} \operatorname{Tor}_G^0(M,\mathbb{Z}[G]) \xrightarrow{\varepsilon_*} \operatorname{Tor}_G^0(M,\mathbb{Z}) \longrightarrow 0. \end{array}$$

Substituindo os isomorfismos adequados temos a sequência exata abaixo

$$0 \longrightarrow H_1(G,M) \longrightarrow M \otimes_G I_G \xrightarrow{\iota_*} M \longrightarrow H_0(G,M) \longrightarrow 0.$$

Logo temos que $H_1(G,M) \cong \operatorname{Ker}(\iota_* : M \otimes_G I_G \to M)$ com ι_* dada por $m \otimes (g-1) \mapsto m(g-1)$. Se M for um G-módulo trivial, então $mg = g$ para todo $m \in M$ e todo $g \in G$, logo $\iota_* = 0$ e $H_1(G,M) \cong M \otimes_G I_G$.

Notemos que $M \otimes_G I_G$ pode ser visto como o quociente do grupo abeliano $M \otimes I_G$ pelo subgrupo T gerado pelos elementos da forma $m \otimes h(g-1) - mh \otimes (g-1)$, mas por hipótese temos $mh \otimes (g-1) = m \otimes (g-1)$ para todo $m \in M$ e todo $h \in G$, logo T é gerado pelos elementos da forma $m \otimes (h-1)(g-1)$, assim

$$M \otimes_G I_G \cong M \otimes I_G/(I_G)^2.$$

Novamente consideramos a sequência exata curta

$$0 \longrightarrow I_G \xrightarrow{\iota} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

Aplicando os funtores $\operatorname{Ext}_i^G(-,M)$ para $i = 0, 1$ obtemos a sequência exata longa abaixo

$$\begin{array}{c} 0 \longrightarrow \operatorname{Ext}_0^G(\mathbb{Z},M) \xrightarrow{\varepsilon^*} \operatorname{Ext}_0^G(\mathbb{Z}[G],M) \xrightarrow{\iota^*} \operatorname{Ext}_0^G(I_G,M) \\ \qquad\qquad\qquad\qquad\qquad\qquad \searrow^{\omega} \\ \operatorname{Ext}_1^G(\mathbb{Z},M) \xrightarrow{\varepsilon^*} \operatorname{Ext}_1^G(\mathbb{Z},M) \longrightarrow \cdots. \end{array}$$

Substituindo os isomorfismos adequados temos a sequência exata abaixo

$$0 \longrightarrow H^0(G,M) \longrightarrow M \xrightarrow{\iota^*} \mathrm{Hom}_G(I_G,M) \longrightarrow H^1(G,M) \longrightarrow 0.$$

Logo temos que $H^1(G,M) \cong \mathrm{Coker}(\iota^* : M \to \mathrm{Hom}_G(I_G,M))$ com ι^* dada por $m \mapsto (\varphi_m : I_G \to M)$ e $\varphi_m(g-1) = m(g-1)$. Se M for um G-módulo trivial, então $mg = 1$ para todo $m \in M$ e todo $g \in G$, logo $i^* = 0$ e $H^1(G,M) \cong \mathrm{Hom}_G(I_G,M)$.

Notemos que $\mathrm{Hom}_G(I_G,M)$ é o subgrupo de $\mathrm{Hom}(I_G,M)$ composto pelos homomorfismos de grupo $\varphi : I_G \to M$ tais que $\varphi(h(g-1)) = h\varphi(g-1) = \varphi(g-1)$ para todo $g,h \in G$, ou seja, $\varphi((h-1)(g-1)) = 0$, mas homomorfismos de grupo com esta propriedade induzem homomorfismos de grupo de $\dfrac{I_G}{(I_G)^2}$ em M, assim

$$\mathrm{Hom}_G(I_G,M) \cong \mathrm{Hom}\left(I_G/(I_G)^2, M\right).$$

□

Para finalizar esta seção lembraremos o conceito de abelianização de um grupo e o relacionaremos com o que fizemos até agora.

Definição 47. Seja G um grupo escrito multiplicativamente. Então o subgrupo dos comutadores de G denotado por G' é aquele gerado pelo conjunto $\{g_1^{-1}g_2^{-1}g_1g_2; g_1, g_2 \in G\}$. A abelianização de G é o grupo $G_{ab} = G/G'$.

Lema 6. Seja G um grupo escrito multiplicativamente. Então

$$I_G/(I_G)^2 \cong G_{ab}.$$

Demonstração. Considere o diagrama comutativo abaixo no qual i e j são as injeções canônicas e p é a projeção canônica.

$$\begin{array}{ccccc} & & W & \xrightarrow{\psi} & G_{ab} \\ & & \downarrow{\scriptstyle i} & \nearrow{\scriptstyle \psi'} & \uparrow{\scriptstyle \psi''} \\ (I_G)^2 & \xrightarrow[j]{} & I_G & \xrightarrow[p]{} & I_G/(I_G)^2 \end{array}$$

Como I_G é um grupo abeliano livre com base $W = \{g-1; g \in G, g \neq 1\}$, então $\psi : W \to G_{ab}$ dado por $\psi(g-1) = gG'$ induz um único homomorfismo de grupos $\psi' : I_G \to G_{ab}$ tal que $\psi' i = \psi$.

Como $(g-1)(h-1) = (gh-1) - (g-1) - (h-1)$, então

$$\begin{aligned}\psi'((g-1)(h-1)) &= \psi'((gh-1) - (g-1) - (h-1)) \\ &= \psi'(gh-1) \cdot \psi'(g-1)^{-1} \cdot \psi'(h-1)^{-1} \\ &= ghG' \cdot g^{-1}G' \cdot h^{-1}G' \\ &= ghg^{-1}h^{-1}G' \\ &= G',\end{aligned}$$

logo $(I_G)^2 \subseteq \mathrm{Ker}(\psi')$ e portanto ψ' induz um único homomorfismo de grupos $\psi'' : I_G/(I_G)^2 \to G_{ab}$ tal que $\psi'' p = \psi'$.

Para o outro lado do isomorfismo considere o diagrama comutativo abaixo no qual π é a projeção canônica.

$$\begin{array}{ccc} G & \xrightarrow{\ \pi\ } & G_{ab} \\ \downarrow{\scriptstyle \varphi} & \nearrow_{\varphi'} & \\ I_G/(I_G)^2 & & \end{array}$$

Seja $\varphi : G \to I_G/(I_G)^2$ dado por $\varphi(g) = (g-1) + (I_G)^2$, então φ é um homomorfismo de grupos, pois

$$\begin{aligned}\varphi(gh) &= (gh-1) + (I_G)^2 \\ &= ((g-1)(h-1) + (g-1) + (h-1)) + (I_G)^2 \\ &= (g-1)(h-1) + (I_G)^2 + (g-1) + (I_G)^2 + (h-1) + (I_G)^2 \\ &= (g-1) + (I_G)^2 + (h-1) + (I_G)^2 \\ &= \varphi(g) + \varphi(h).\end{aligned}$$

Como $I_G/(I_G)^2$ é abeliano, então φ induz um único homomorfismo de grupos $\varphi' : G_{ab} \to I_G/(I_G)^2$ tal que $\varphi'\pi = \varphi$.

Verificar que φ' e ψ'' são inversos um do outro é um exercício de rotina e será omitido aqui. □

O lema acima nos dá o seguinte corolário.

Corolário 3. Sejam G um grupo escrito multiplicativamente e M um G-módulo trivial. Então

$$H_1(G, M) \cong M \otimes G_{ab} \quad \text{e} \quad H^1(G, M) \cong \mathrm{Hom}\,(G_{ab}, M)\,.$$

4.8 Relação entre H^1, derivações e extensões com cisão

Nesta seção e na seguinte atacaremos o problema da extensão de grupos dando algumas respostas através da cohomologia de grupos. Estamos interessados em, dados dois grupos K e Q,

encontrar todos os grupos E, tais que K é isomorfo a um subgrupo normal de E com o quociente associado isomorfo a Q. Com isso temos a seguinte definição.

Definição 48. Uma extensão de um grupo K por um grupo Q é uma sequência exata curta de grupos

$$1 \longrightarrow K \xrightarrow{i} E \xrightarrow{p} Q \longrightarrow 1.$$

Vale ressaltar que alguns autores chamam a sequência exata curta acima de uma extensão de Q por K.

Exemplo 26. Tomando $K = \mathbb{Z}/3\mathbb{Z}$ e $Q = \mathbb{Z}/2\mathbb{Z}$, podemos encontrar dois exemplos de extensões de K por Q: o grupo simétrico em três elementos, $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, e o grupo cíclico de ordem seis, $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$.

$$0 \longrightarrow \mathbb{Z}/3\mathbb{Z} \xrightarrow{i} S_3 \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

$$0 \longrightarrow \mathbb{Z}/3\mathbb{Z} \xrightarrow{j} \mathbb{Z}/6\mathbb{Z} \xrightarrow{q} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

com $i(\overline{1}) = (123)$, $p(1) = p(123) = p(132) = \overline{0}$, $p(12) = p(13) = p(23) = \overline{1}$, $j(\overline{1}) = \overline{2}$ e $q(\overline{1}) = \overline{1}$.

Naturalmente, dadas duas extensões de K por Q, gostaríamos de decidir quando estas são essencialmente a mesma extensão, por isto definimos o conceito de equivalência de extensões abaixo.

Definição 49. Dizemos que duas extensões de K por Q

$$1 \longrightarrow K \xrightarrow{i} E \xrightarrow{p} Q \longrightarrow 1$$
$$1 \longrightarrow K \xrightarrow{i'} E' \xrightarrow{p'} Q \longrightarrow 1$$

são equivalentes quando existe um homomorfismo de grupos $\varphi : E \to E'$ tal que o diagrama abaixo é comutativo

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \overset{i}{\nearrow} & E & \overset{p}{\searrow} & & & \\ & & & & \downarrow{\scriptstyle \varphi} & & Q & \longrightarrow & 1. \\ & & & \underset{i'}{\searrow} & E' & \underset{p'}{\nearrow} & & & \end{array}$$

Perceba que uma extensão é sempre equivalente a si mesma via φ igual à identidade, além disso, tomando a composição adequada temos que equivalência de extensões é uma relação transitiva, por fim, o Lema dos cinco nos garante que φ é um isomorfismo, ou seja, equivalência de extensões é também uma relação simétrica e, portanto, é realmente uma relação de equivalência.

Definição 50. Dizemos que uma extensão de K por Q

$$1 \longrightarrow K \xrightarrow{i} E \xrightarrow{p} Q \longrightarrow 1$$

cinde, é cindida, ou possui cisão, quando existe uma seção de p, isto é, quando existe um homomorfismo de grupos $s : Q \to E$ tal que $ps = Id_Q$.

Exemplo 27. As extensões do exemplo anterior são cindidas, já que existem os homomorfismos de grupo $s_1, s_2, s_3 : \mathbb{Z}/2\mathbb{Z} \to S_3$ e $t : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ tais que $ps_1 = ps_2 = ps_3 = Id_{\mathbb{Z}/2\mathbb{Z}} = qt$, dadas por $s_1(\overline{1}) = (23)$, $s_2(\overline{1}) = (13)$, $s_3(\overline{1}) = (12)$ e $t(\overline{1}) = \overline{3}$.

$$0 \longrightarrow \mathbb{Z}/3\mathbb{Z} \xrightarrow{\ i\ } S_3 \underset{s_1 \text{ ou } s_2 \text{ ou } s_3}{\overset{p}{\rightleftarrows}} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

$$0 \longrightarrow \mathbb{Z}/3\mathbb{Z} \xrightarrow{\ j\ } \mathbb{Z}/6\mathbb{Z} \underset{t}{\overset{q}{\rightleftarrows}} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

Note que neste exemplo, a primeira extensão cinde de três maneiras diferentes, enquanto que a segunda cinde de apenas uma maneira.

Nesta seção veremos que certos tipos de extensões com cisão podem ser caracterizadas com uma ferramenta da teoria de grupos chamada de produto semidireto.

Definição 51. Sejam K e Q dois grupos e $\sigma : Q \to \mathrm{Aut}(K)$ um homomorfismo de grupos. Então o produto semidireto de K por Q em relação a σ é o grupo denotado por $K \rtimes_\sigma Q$ cujo conjunto de elementos é o produto cartesiano $K \times Q = \{(k, q); k \in K, q \in Q\}$ e cuja operação é dada por

$$(k_1, q_1) \cdot (k_2, q_2) = (k_1 \cdot \sigma_{q_1}(k_2), q_1 \cdot q_2), \qquad \text{para } k_1, k_2 \in K, q_1, q_2 \in Q.$$

São exercícios de rotina verificar que $K \rtimes_\sigma Q$ realmente possui estrutura de grupo com elemento neutro $(1_K, 1_Q)$ para $1_K \in K$ e $1_Q \in Q$ os respectivos elementos neutros de cada grupo, e $(k, q)^{-1} = (\sigma_{q^{-1}}(k^{-1}), q^{-1})$. Além disso, $\overline{K} = \{(k, 1_Q); k \in K\}$ é um subgrupo normal de $K \rtimes_\sigma Q$ isomorfo a K e $\overline{Q} = \{(1_K, q); q \in Q\}$ é um subgrupo de $K \rtimes_\sigma Q$ isomorfo a Q. Por fim, temos um homomorfismo de grupos de inclusão canônico $i : K \to K \times_\sigma Q$ dado por $k \mapsto (k, 1_Q)$ e um homomorfismo de grupos de projeção canônico $p : K \times_\sigma Q \to Q$ dado por $(k, q) \mapsto q$.

Quando K for um Q-módulo, o produto semidireto de K e Q relativo ao homomorfismo de estrutura de K como Q-módulo será denotado por $K \rtimes Q$, sempre que isso não gerar ambiguidade.

A partir de agora estaremos interessados em procurar extensões de um grupo abeliano M (escrito aditivamente) por um grupo qualquer G (escrito multiplicativamente), por essa razão, alteraremos ligeiramente a notação empregada até aqui.

Lema 7. Considere a extensão de um grupo abeliano M por um grupo G qualquer abaixo

$$0 \longrightarrow M \xrightarrow{\ i\ } E \xrightarrow{\ p\ } G \longrightarrow 1.$$

Então M é um G-módulo.

Demonstração. Dados $m \in M$ e $g \in G$, definimos $g \cdot m \in M$ como sendo o único elemento tal que

$$i(g \cdot m) = \overline{g} \cdot i(m) \cdot \overline{g}^{-1}, \qquad \text{com } \overline{g} \in H \text{ tal que } p(\overline{g}) = g.$$

Devemos mostrar que esta definição faz sentido. Como $i(M)$ é um subgrupo normal de H, então $\overline{g} \cdot i(m) \cdot \overline{g}^{-1} \in i(M)$ para todo $m \in M$ e todo $\overline{g} \in H$. Agora, sejam $\overline{g_1}, \overline{g_2} \in H$ tais que $p(\overline{g_1}) = p(\overline{g_2})$, então $\overline{g_1} = \overline{g_2} \cdot i(\overline{m})$ para algum $\overline{m} \in M$, assim, para qualquer $m \in M$ temos que

$$\begin{aligned}
\overline{g_1} \cdot i(m) \cdot \overline{g_1}^{-1} &= (\overline{g_2} \cdot i(\overline{m})) \cdot i(m) \cdot (\overline{g_2} \cdot i(\overline{m}))^{-1} \\
&= \overline{g_2} \cdot i(\overline{m}) \cdot i(m) \cdot i(\overline{m})^{-1} \cdot \overline{g_2}^{-1} \\
&= \overline{g_2} \cdot i(\overline{m} + m - \overline{m}) \cdot \overline{g_2}^{-1} \\
&= \overline{g_2} \cdot i(m) \cdot \overline{g_2}^{-1},
\end{aligned}$$

isto é, a operação definida acima não depende da escolha da pré-imagem $\overline{g} \in H$ de $g \in G$ por $p : E \to G$.

Claramente temos que

$$\begin{aligned}
1_G \cdot m &= m, \\
g_1 \cdot (g_2 \cdot m) &= (g_1 \cdot g_2) \cdot m, \\
g \cdot (m_1 + m_2) &= g_1 \cdot m_1 + g_2 \cdot m_2,
\end{aligned}$$

para $g, g_1, g_2 \in G$ e $m, m_1, m_2 \in M$. Portanto segue o resultado desejado. □

Observação 20. Dado um G-módulo M. Diremos que uma sequência exata curta como abaixo

$$0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$$

é uma extensão de M por G, ou que realiza a estrutura de G-módulo de M, quando a estrutura de G-módulo induzida, descrita pelo lema anterior, coincidir com a estrutura de G-módulo já presente em M.

Observação 21. O lema anterior está de acordo com o que vimos até agora nos exemplos envolvendo $M = \mathbb{Z}/3\mathbb{Z}$ e $G = \mathbb{Z}/2\mathbb{Z}$, isto é, S_3 e $\mathbb{Z}/6\mathbb{Z}$ realizam as duas estruturas de M como G-módulo.

Lema 8. Considere as extensões de um G-módulo M por G abaixo, com i' e p' a injeção e a projeção canônicas:

$$0 \longrightarrow M \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1. \tag{4.1}$$

$$0 \longrightarrow M \xrightarrow{i'} M \rtimes G \xrightarrow{p'} G \longrightarrow 1, \tag{4.2}$$

Então Equação 4.1 cinde se, e somente se, Equação 4.1 é equivalente a Equação 4.2.

Demonstração. Suponha que Equação 4.1 cinde. Sejam $e \in E$, $g = p(e) \in G$ e $\overline{g} = s(g) = s(p(e)) \in E$, então $p(\overline{g}) = p(s(p(e))) = p(e)$, logo $e \cdot \overline{g}^{-1} \in \mathrm{Ker}(p) = \mathrm{Img}(i)$, assim $e = i(m) \cdot \overline{g} = i(m) \cdot s(g)$ para algum $m \in M$.

Agora, se $m_1, m_2 \in M$ e $g_1, g_2 \in G$ são tais que $i(m_1) \cdot s(g_1) = i(m_2) \cdot s(g_2)$, então

$$p(i(m_1) \cdot s(g_1)) = p(i(m_2) \cdot s(g_2)) \Rightarrow$$

$$p(i(m_1)) \cdot p(s(g_1)) = p(i(m_2)) \cdot p(s(g_2)) \Rightarrow$$

$$g_1 = g_2,$$

e assim temos que $i(m_1) = i(m_2)$, mas da injetividade de i segue que $m_1 = m_2$. Desta maneira mostramos que todo elemento $e \in E$ pode ser escrito de maneira única como um produto $i(m) \cdot s(g)$ para algum $m \in N$ e algum $g \in G$. Note que até aqui não usamos o fato de s ser um homomorfismo de grupos, isto será importante na próxima seção do texto.

Por fim, a operação de E pode ser recuperada pela operação de G-módulo em M

$$i(g \cdot m) = s(g) \cdot i(m) \cdot s(g)^{-1}, \qquad \text{para } m \in m, g \in G,$$

pois se $e_1 = i(m_1) \cdot s(g_1)$ e $e_2 = i(m_2) \cdot s(g_2)$, então

$$\begin{aligned} e_1 \cdot e_2 &= (i(m_1) \cdot s(g_1)) \cdot (i(m_2) \cdot s(g_2)) \\ &= i(m_1) \cdot (s(g_1) \cdot i(m_2) \cdot s(g_1)^{-1}) \cdot s(g_1) \cdot s(g_2) \\ &= i(m_1) \cdot i(g_1 \cdot m_2) \cdot s(g_1) \cdot s(g_2) \\ &= i(m_1 + g_1 \cdot m_2) \cdot s(g_1 \cdot g_2). \end{aligned}$$

Obtemos assim um isomorfismo de grupos

$$\begin{aligned} \varphi : E &\to M \rtimes G \\ e = i(m) \cdot s(g) &\mapsto (m, g). \end{aligned}$$

Agora, se $m \in M$, então

$$\varphi(i(m)) = \varphi(i(m) \cdot s(1_G)) = (m, 1_G) = i'(m)$$

e se $e = i(m) \cdot s(g) \in E$, então

$$p'(\varphi(e)) = p'(\varphi(i(m) \cdot s(g))) = p'(m, g) = g = p(i(m) \cdot s(g)) = p(e).$$

Segue que Equação 4.1 é equivalente a Equação 4.2. A recíproca é trivial. □

Exemplo 28. Já vimos, no Exemplo 23 que $M = \mathbb{Z}/3\mathbb{Z}$ pode ser visto de duas maneiras diferentes como G-módulo, quando $G = \mathbb{Z}/2\mathbb{Z}$, ou seja, existem dois homomorfismos de grupo diferentes $\mathbb{Z}/2\mathbb{Z} = G \to G \cong \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ e, assim, podemos construir dois produtos semidiretos de M por G. Desta maneira, o lema anterior nos garante que $M \rtimes_{Id_G} G \cong S_3$ e $M \rtimes_0 G \cong \mathbb{Z}/6\mathbb{Z}$.

O lema acima nos diz que, a menos de equivalência, a única extensão com cisão de um G-módulo M por G é o produto semidireto $M \rtimes G$ relativo ao homomorfismo de estrutura de M como G-módulo, esta será chamada de extensão com cisão canônica de M por G. Passa a ser natural se perguntar quais são as possíveis maneiras de cindir a extensão acima, a menos de alguma noção de equivalência.

Definição 52. Sejam $s, s' : G \to E$ duas seções de uma mesma extensão com cisão. Dizemos que s e s' são seções conjugadas, denotando por $s \sim s'$, quando existe $m \in M$ tal que

$$s(g) = i(m) \cdot s'(g) \cdot i(m)^{-1}, \qquad \text{para todo } g \in G.$$

Claramente a conjugação de seções de uma mesma extensão de grupos com cisão é uma relação de equivalência.

Exemplo 29. Vimos no Exemplo 27 que a extensão abaixo tem três seções diferentes $s_1 : \overline{1} \mapsto (23)$, $s_2 : \overline{1} \mapsto (13)$ e $s_3 : \overline{1} \mapsto (12)$

$$0 \longrightarrow \mathbb{Z}/3\mathbb{Z} \xrightarrow{\ i\ } S_3 \xrightarrow{\ p\ } \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

note que estas seções são conjugadas duas a duas, pois

$$\begin{aligned} s_1(\overline{1}) = (23) &= (123)(12)(132) = i(\overline{1})s_3(\overline{1})i(\overline{1})^{-1} \\ s_2(\overline{1}) = (13) &= (123)(23)(132) = i(\overline{1})s_1(\overline{1})i(\overline{1})^{-1} \\ s_3(\overline{1}) = (12) &= (123)(13)(132) = i(\overline{1})s_2(\overline{1})i(\overline{1})^{-1} \end{aligned}$$

Definição 53. Seja M um G-módulo. Uma derivação (ou um homomorfismo cruzado) de G em M é uma função $d : G \to M$ tal que

$$d(g_1 \cdot g_2) = d(g_1) + g_1 \cdot d(g_2), \qquad \text{para todo } g_1, g_2 \in G.$$

O conjunto das derivações de G em M possui estrutura de grupo abeliano com adição dada pontualmente e será denotado por $\mathrm{Der}(G, M)$.

Definição 54. Seja M um G-módulo à esquerda. Uma derivação $d : G \to M$ é dita interna (ou principal) quando existe $m \in M$ tal que

$$d(g) = g \cdot m - m, \qquad \text{para todo } g \in G.$$

O conjunto das derivações internas (ou principais) de G em M é um subgrupo de $\mathrm{Der}(G, M)$ e será denotado por $\mathrm{IDer}(G, M)$.

Observação 22. Note que as derivações de G em M são justamente os elementos de $\mathrm{Ker}(\delta^2)$, que chamamos de 1-cociclos, e as derivações internas de G em M são justamente os elementos de $\mathrm{Img}(\delta^1)$, que chamamos de 1-cobordos, como descrito na Seção 4.5. Portanto temos o seguinte isomorfismo de grupos

$$H^1(G, M) \cong \frac{\mathrm{Der}(G, M)}{\mathrm{IDer}(G, M)}.$$

Finalmente temos tudo o que é necessário para enunciar e demonstrar o teorema abaixo relacionando o grupo de cohomologia $H^1(G, M)$ e seções da extensão $M \rtimes G$.

Teorema 18. Seja M um G-módulo. Então existe uma bijeção entre o conjunto das classes de equivalência das seções da extensão com cisão canônica de M por G e $H^1(G, M)$.

Demonstração. Considere a extensão com cisão canônica de M por G

$$0 \longrightarrow M \xrightarrow{i} M \rtimes G \xrightarrow{p} G \longrightarrow 1.$$

Suponha que $s : G \to M \rtimes G$ é um função tal que $ps = 1_G$, então existe uma função $d : G \to M$ tal que $s(g) = (d(g), g)$. Mostraremos que s é um homomorfismo de grupos se, e somente se, d é um derivação. De fato, para $g_1, g_2 \in G$ temos que

$$s(g_1 \cdot g_2) = s(g_1) \cdot s(g_2) \iff$$

$$(d(g_1 \cdot g_2), g_1 \cdot g_2) = (d(g_1), g_1) \cdot (d(g_2), g_2) = (d(g_1) + g_1 \cdot d(g_2), g_1 \cdot g_2) \iff$$

$$d(g_1 \cdot g_2) = d(g_1) + g_2 \cdot d(g_2).$$

Isto mostra que o conjunto das seções $s : G \to M \rtimes G$ está em bijeção com o conjunto das derivações $d : G \to M$.

Suponha agora que $s, s' : G \to M \rtimes G$ são duas seções de p correspondentes, respectivamente, às derivações $d, d' : G \to N$. Como para todo $m \in M$ e todo $g \in G$ temos que

$$\begin{aligned} i(m) \cdot s'(g) \cdot i(m)^{-1} &= (m, 1) \cdot (d'(g), g) \cdot (-m, 1) \\ &= (m + d'(g), g) \cdot (-m, 1) \\ &= (m + d'(g) - g \cdot m, g) \\ &= (d'(g) + (g - 1) \cdot m, g), \end{aligned}$$

então

$$s \sim s' \iff \exists m \in M \text{ tal que } \forall g \in G \text{ vale } s(g) = i(m) \cdot s'(g) \cdot i(m)^{-1} \iff$$

$$\exists m \in M \text{ tal que } \forall g \in G \text{ vale } (d(g), g) = (d'(g) + (g - 1) \cdot m, g) \iff$$

$$\exists m \in M \text{ tal que } \forall g \in G \text{ vale } d(g) = d'(g) + (g - 1) \cdot m \iff d - d' \in \mathrm{IDer}(G, M).$$

□

4.9 Relação entre H^2 e extensões

Nesta seção daremos uma caracterização do conjunto das classes de equivalência de extensões de M por G em termos do grupo de cohomologia $H^2(G, M)$. Mais precisamente, temos o teorema abaixo.

Teorema 19. Seja M um G-módulo. Então existe uma bijeção entre o conjunto das classes de equivalência das extensões de M por G e $H^2(G, M)$.

Demonstração. Suponha a extensão do G-módulo M por G

$$0 \longrightarrow M \xrightarrow{i} E \underset{s}{\overset{p}{\rightleftarrows}} G \longrightarrow 1 \tag{4.3}$$

e seja $s : G \to E$ uma função tal que $ps = Id_G$, assumimos que s é tal que $s(1) = 1$ mas não exigimos que s seja necessariamente um homomorfismo de grupos.

De maneira similar ao que fizemos na seção anterior, temos que todo $e \in E$ é escrito de maneira única como $e = i(m) \cdot s(g)$ para algum $m \in M$ e $g \in G$. Temos ainda que para $m \in M$ e $g \in G$, a estrutura de G-módulo de M é dada por

$$i(g \cdot m) = s(g) \cdot i(m) \cdot s(g)^{-1}.$$

Note que podemos mensurar o quanto s falha em ser um homomorfismo de grupos, pois para $g_1, g_2 \in G$ temos que

$$p(s(g_1) \cdot s(g_2)) = p(s(g_1)) \cdot p(s(g_2)) = g_1 \cdot g_2 = p(s(g_1 \cdot g_2)),$$

logo $s(g_1) \cdot s(g_2) \cdot s(g_1 \cdot g_2)^{-1} \in \mathrm{Ker}(p) = \mathrm{Img}(i)$, escolhemos assim a 2-cocadeia $f : G \times G \to M$ dada por

$$s(g_1) \cdot s(g_2) = i(f(g_1, g_2)) \cdot s(g_1 \cdot g_2).$$

Note que de $s(1) = 1$ segue que f é uma 2-cocadeia normal, pois

$$i(f(g_1, 1)) = s(g_1) \cdot s(1) \cdot s(g_1 \cdot 1)^{-1} = s(g_1) \cdot s(g_1)^{-1} = 1 \Rightarrow f(g_1, 1) = 0,$$

$$i(f(1, g_2)) = s(1) \cdot s(g_2) \cdot s(1 \cdot g_2)^{-1} = s(g_2) \cdot s(g_2)^{-1} = 1 \Rightarrow f(1, g_2) = 0.$$

Agora, se $e_1 = i(m_1) \cdot s(g_1), e_2 = i(m_2) \cdot s(g_2) \in E$, então

$$\begin{aligned} e_1 \cdot e_2 &= i(m_1) \cdot s(g_1) \cdot i(m_2) \cdot s(g_2) \\ &= i(m_1) \cdot s(g_1) \cdot i(m_2) \cdot s(g_1)^{-1} \cdot s(g_1) \cdot s(g_2) \\ &= i(m_1) \cdot i(g_1 \cdot m_2) \cdot i(f(g_1, g_2)) \cdot s(g_1 \cdot g_2) \\ &= i(m_1 + g_1 \cdot m_2 + f(g_1, g_2)) \cdot s(g_1 \cdot g_2). \end{aligned}$$

Logo, da associatividade em E, temos que f é um 2-cociclo, pois se $e_1 = i(m_1)s(g_1), e_2 = i(m_2)s(g_2), e_3 = i(m_3)s(g_3) \in E$, então

$$\begin{aligned} e_1(e_2e_3) &= i(m_1)s(g_1)(i(m_2)s(g_2)i(m_3)s(g_3)) \\ &= i(m_1)s(g_1)(i(m_2 + g_2m_3 + f(g_2, g_3))s(g_2g_3)) \\ &= i(m_1 + g_1m_2 + g_1g_2m_3 + g_1f(g_2, g_3) + f(g_1, g_2g_3))s(g_1g_2g_3), \\ (e_1e_2)e_3 &= (i(m_1)s(g_1)i(m_2)s(g_2))i(m_3)s(g_3) \\ &= (i(m_1 + g_1m_2 + f(g_1, g_2))s(g_1g_2))i(m_3)s(g_3) \\ &= i(m_1 + g_1m_2 + f(g_1, g_2) + g_1g_2m_3 + f(g_1g_2, g_3))s(g_1g_2g_3), \end{aligned}$$

o que implica que para todo $g_1, g_2, g_3 \in G$ vale

$$g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2) = 0.$$

Suponha agora que $s' : G \to E$ é outra função tal que $ps' = Id_G$ e $s(1) = 1$ com $f' : G \times G \to M$ o 2-cociclo normal associado, isto é,

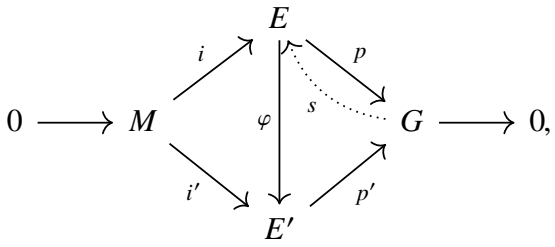
$$s'(g_1)s'(g_2) = i(f'(g_1, g_2))s(g_1 g_2).$$

Tome $d : G \to M$ a 1-cocadeia dada por $i(d(g)) = s'(g)s(g)^{-1}$. De $s(1) = 1 = s'(1)$ segue que d é normal. Vamos provar que $f' = f + \delta^2(d)$, isto é, $f + \mathrm{Img}(\delta^2) = f' + \mathrm{Img}(\delta^2)$ em $H^2(G, M)$. Isto de fato ocorre, pois para todo $g_1, g_2 \in G$ temos que

$$\begin{aligned}
i(f'(g_1, g_2)) &= s'(g_1)s'(g_2)s'(g_1 g_2)^{-1} \\
&= i(d(g_1))s(g_1)i(d(g_2))s(g_2)s(g_1 g_2)^{-1}i(d(g_1 g_2))^{-1} \\
&= i(d(g_1))s(g_1)i(d(g_2))s(g_1)^{-1}s(g_1)s(g_2)s(g_1 g_2)^{-1}i(d(g_1 g_2))^{-1} \\
&= i(d(g_1))i(g_1 d(g_2))i(f(g_1, g_2))i(d(g_1 g_2))^{-1} \\
&= i(d(g_1) + g_1 d(g_2) + f(g_1, g_2) - d(g_1, g_2)) \\
&= i(f(g_1, g_2) + \delta^2(d)(g_1, g_2),
\end{aligned}$$

e da injetividade de i segue a igualdade desejada.

Agora, se temos outra extensão de M por G equivalente a Equação 4.3 via $\varphi : E \to E'$,



então tomando $s' = \varphi s : G \to E'$ temos que $p's' = p'\varphi s = ps = Id_G$ e $s'(1) = \varphi(s(1)) = \varphi(1) = 1$. Denotando por $f : G \times G \to M$ o 2-cociclo normal induzido por s e por $f' : G \times G \to M$ o 2-cociclo normal induzido por s' concluímos que para todo $g_1, g_2 \in G$ vale que

$$\begin{aligned}
i'(f'(g_1, g_2)) &= s'(g_1)s'(g_2)s'(g_1 g_2)^{-1} \Rightarrow \\
\varphi(i(f'(g_1, g_2))) &= \varphi(s(g_1))\varphi(s(g_2))\varphi(s(g_1 g_2))^{-1} \Rightarrow \\
\varphi(i(f'(g_1, g_2))) &= \varphi(s(g_1)s(g_2)s(g_1 g_2)^{-1}) = \varphi(i(f(g_1, g_2)) \Rightarrow \\
i(f'(g_1, g_2)) &= i(f(g_1, g_2)) \Rightarrow \\
f'(g_1, g_2) &= f(g_1, g_2).
\end{aligned}$$

Até aqui provamos que extensões equivalentes de M por G dão origem ao mesmo elemento em $H^2(G, M)$, isto é, para cada classe de equivalência de extensões de M por G corresponde um único elemento de $H^2(G, M)$.

Reciprocamente, dado um 2-cociclo $f : G \times G \to M$ normal, construímos o grupo E_f cujos elementos são pares ordenados (m, g) com $m \in M$ e $g \in G$ e cuja multiplicação é dada por

$$(m_1, g_1)(m_2, g_2) = (m_1 + g_1 m_2 + f(g_1, g_2), g_1 g_2).$$

Realizando cálculos de rotina mostra-se, usando que f é um 2-cociclo normal, que a operação definida acima é associativa, que $(0, 1)$ é o elemento neutro da operação e que os inversos são da forma $(m, g)^{-1} = (-g^{-1}m - f(g^{-1}, g), g^{-1}) = (-g^{-1}m - g^{-1}f(g, g^{-1}), g^{-1})$. Além disso, as aplicações $i_f : M \to E_f$ dada por $i_f(m) = (m, 1)$ e $p_f : E_f \to G$ dada por $p_f(m, g) = g$ fazem de E_f uma extensão de M por G, já que a sequência curta abaixo é exata e recupera a ação de G sobre M como G-módulo

$$0 \longrightarrow M \xrightarrow{i_f} E_f \xrightarrow{p_f} G \longrightarrow 1.$$

Por fim, dado outro 2-cociclo normal $f' : G \times G \to M$ tal que $f' = f + \delta^2(d)$ para alguma 1-cocadeia $d : G \to M$ normal, construímos a extensão $E_{f'}$ como feito acima para f. Definindo $\varphi : E_{f'} \to E_f$ dado por $\varphi(m, g) = (m + d(g), g)$ temos que para todo $(m_1, g_1), (m_2, g_2) \in H_f$ vale

$$\begin{aligned}
\varphi((m_1, g_1)(m_2, g_2)) &= \varphi(m_1 + g_1 m_2 + f'(g_1, g_2), g_1 g_2) \\
&= (m_1 + g_1 m_2 + f'(g_1, g_2) + d(g_1 g_2), g_1 g_2) \\
&= (m_1 + g_1 m_2 + f(g_1, g_2) + g_1 d(g_2) - d(g_1 g_2) + d(g_1) + d(g_1 g_2), g_1 g_2) \\
&= (m_1 + g_1 m_2 + f(g_1, g_2) + g_1 d(g_2) + d(g_1), g_1 g_2) \\
&= (m_1 + d(g_1), g_1)(m_2 + d(g_2), g_2) \\
&= \varphi(m_1, g_1)\varphi(m_2, g_2),
\end{aligned}$$

logo φ é um homomorfismo de grupos. Além disso, para todo (m, g) vale

$$\begin{aligned}
\varphi(i_f(m)) &= \varphi(m, 1) = (m + d(1), 1) = (m, 1) = i_{f'}(m) \\
p_{f'}(\varphi(m, g)) &= p_{f'}(m + d(g), g) = g = p_f(m, g),
\end{aligned}$$

portanto φ é uma equivalência entre as extensões de M por G dadas por f e f'

$$\begin{array}{ccccccccc}
 & & & & E_{f'} & & & & \\
 & & & \overset{i_{f'}}{\nearrow} & \downarrow{\scriptstyle \varphi} & \overset{p_{f'}}{\searrow} & & & \\
0 & \longrightarrow & M & & & & G & \longrightarrow & 1. \\
 & & & \underset{i_f}{\searrow} & & \underset{p_f}{\nearrow} & & & \\
 & & & & E_f & & & &
\end{array}$$

Fica provado então que a cada elemento de $H^2(G, M)$ corresponde uma extensão de M por G. Só nos resta mostrar que estas construções são inversas uma da outra, para que enfim tenhamos a bijeção desejada.

Para um 2-cociclo normal $f : G\times G \to NM$ representando uma classe de cohomologia em $H^2(G, M)$, escolha a função $s : G \to E_f$ óbvia dada por $s(g) = (0, g)$ da extensão correspondente

$$0 \longrightarrow M \xrightarrow{i_f} E_f \underset{s}{\overset{p_f}{\rightleftarrows}} G \longrightarrow 1.$$

Assim, s determina um 2-cociclo normal $f' : G \times G \to M$ dado por $i_f(f'(g_1, g_2)) = s(g_1)s(g_2)s(g_1g_2)^{-1}$. Então temos que

$$\begin{aligned} i_f(f'(g_1, g_2)) &= s(g_1)s(g_2)s(g_1g_2)^{-1} \\ &= (0, g_1)(0, g_2)(0, g_1g_2)^{-1} \\ &= (f(g_1, g_2), g_1g_2)(-(g_1g_2)^{-1}f(g_1g_2, (g_1g_2)^{-1}), (g_1g_2)^{-1}) \\ &= (f(g_1, g_2) - f(g_1g_2, (g_1g_2)^{-1}) + f(g_1g_2, (g_1g_2)^{-1}), 1) \\ &= (f(g_1, g_2), 1) \\ &= i_f(f(g_1, g_2), \end{aligned}$$

logo $f(g_1, g_2) = f'(g_1, g_2)$ para todo $g_1, g_2 \in G$ e, portanto, $f = f'$.

Finalmente, para uma extensão

$$0 \longrightarrow M \xrightarrow{i} E \underset{s}{\overset{p}{\rightleftarrows}} G \longrightarrow 1,$$

juntamente com uma função $s : G \to E$ tal que $s(1) = 1$ e $ps = Id_G$, obtemos um 2-cociclo normal $f : G \times G \to M$ dado pela igualdade $i(f(g_1, g_2)) = s(g_1)s(g_2)s(g_1g_2)^{-1}$. Para este 2-cociclo f construímos a extensão

$$0 \longrightarrow M \xrightarrow{i_f} E_f \xrightarrow{p_f} G \longrightarrow 1,$$

com $i_f(m) = (m, 1)$ e $p_f(m, g) = g$. Para mostrar que estas duas extensões são equivalentes definimos a aplicação $\varphi : E_f \to E$ dada por $\varphi(m, g) = i(m)s(g)$. Claramente temos que

$$\begin{aligned} \varphi((m_1, g_1)(m_2, g_2)) &= \varphi(m_1 + g_1m_2 + f(g_1, g_2), g_1g_2) \\ &= i(m_1)i(g_1m_2)i(f(g_1, g_2))s(g_1g_2) \\ &= i(m_1)s(g_1)i(m_2)s(g_1)^{-1}s(g_1)s(g_2)s(g_1g_2)^{-1}s(g_1g_2) \\ &= i(m_1)s(g_1)i(m_2)s(g_2) \\ &= \varphi(m_1, g_1)\varphi(m_2, g_2), \end{aligned}$$

provando que φ é um homomorfismo de grupos. Além disso, vale que $p(\varphi(m, g)) = p(i(m)s(g)) = g = p_f(m, g)$ e $\varphi(i_f(m)) = \varphi(m, 1) = i(m)s(1) = i(m)$ para todo $m \in M$ e $g \in G$, isto mostra que φ é uma equivalência de extensões e com isso concluímos a demonstração do teorema. □

REFERÊNCIAS

ATIYAH, M. F.; MACDONALD, I. G. **Introduction to Commutative Algebra**. [S.l.]: Addison-Wesley Publishing Company, 1969. Citado na página 46.

BROWN, K. S. **Cohomology of Groups**. [S.l.]: Springer, 1982. Citado na página 71.

HILTON, P. J.; STAMMBACH, U. **A Course in Homological Algebra, 2nd ed.** [S.l.]: Springer, 1996. Citado nas páginas 52 e 71.

LEINSTER, T. **Basic Category Theory**. [S.l.]: Cambridge University Press, 2014. Citado na página 19.

LLUIS-PUEBLA, E. **Álgebra Homógica, Cohomología de Grupos y K-Teoría Algebraica Clásica**. [S.l.]: Sociedad Matemática Mexicana, 2005. Citado na página 71.

MACLANE, S. **Categories for the Working Mathematician, 2nd ed.** [S.l.]: Springer, 1978. Citado na página 19.

ROTMAN, J. J. **An Introduction to Homological Algebra, 2nd ed.** [S.l.]: Springer, 2009. Citado nas páginas 64, 66 e 71.

____. **An Introduction to the Theory of Groups, 4th ed.** [S.l.]: Springer, 2014. Citado na página 71.


ICMC
USP
SÃO CARLOS