UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
LICENCIATURA EM MATEMÁTICA

ARY GUIMARÃES DE VASCONCELOS NETO

INTRODUÇÃO A ÁLGEBRA HOMOLÓGICA

TRABALHO DE CONCLUSÃO DE CURSO

CORNÉLIO PROCÓPIO

2020

ARY GUIMARÃES DE VASCONCELOS NETO

INTRODUÇÃO A ÁLGEBRA HOMOLÓGICA

Trabalho de Conclusão de Curso de Graduação, apresentado à disciplina Trabalho de conclusão de curso, do curso de Licenciatura em Matemática da Universidade Tecnológica Federal do Paraná — UTFPR, como requisito parcial para a obtenção do título de Licenciado em Matemática.

Orientador: Prof. Anderson Paião dos Santos

CORNÉLIO PROCÓPIO
2020

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Cornélio Procópio
Diretoria de Graduação
Departamento de Matemática
Curso de Licenciatura em Matemática

FOLHA DE APROVAÇÃO

Ary Guimarães de Vasconcelos Neto

Introdução a Álgebra Homológica

Trabalho de Conclusão de Curso de Graduação apresentado às 14:00 no dia 23/10/2020, do curso de Licenciatura em Matemática da Universidade Tecnológica Federal do Paraná — UTFPR, como requisito parcial para a obtenção do título de Licenciado em Matemática. O candidato foi arguido pela Banca Avaliadora composta pelos professores abaixo assinados. Após deliberação a Banca Avaliadora considerou o trabalho aprovado.

Prof. Anderson Paião dos Santos
(Orientador)

Prof. Débora Aparecida Francisco Albanez

Prof. Matheus Henrique Pimenta Zanon

“A Folha de Aprovação assinada encontra-se na Coordenação do Curso”

AGRADECIMENTOS

Agradeço ao meu orientador Prof. Dr. Anderson Paião dos Santos, pela sabedoria e paciência com que me guiou nesta trajetória.

Aos meus colegas de sala e curso, que sempre estiveram ao meu lado nos momentos difíceis

A Secretaria do Curso, pela cooperação.

Gostaria de agradecer também ao meu pai, Junior, que sempre esteve ao meu lado e torce por mim em todos os caminhos pelos quais escolho trilhar. Ao meu irmão, Wagner, que me incentiva a ser uma pessoa melhor e um bom profissional. E a minha cunhada, Neide, que está sempre ao meu lado.

Enfim, a todos os que por algum motivo contribuíram para a realização desta pesquisa.

"A mente que se abre à uma nova ideia jamais voltará ao seu tamanho original".

Albert Enstein

RESUMO

Guimarães de Vasconcelos Neto, Ary. **Introdução a Álgebra Homológica**. 2020. 51 f. Trabalho de Conclusão de Curso (Graduação) – Licenciatura em Matemática. Universidade Tecnológica Federal do Paraná. Cornélio Procópio, 2020

O trabalho em questão tem como objetivo principal ser um material alternativo para o leitor que busca iniciar seus estudos em Álgebra Homológica. Faremos aqui o estudo de estruturas sobre conjuntos denominadas módulos, uma estrutura algébrica que generaliza o conceito de espaço vetorial. Para o desenvolvimento deste material, foi feita uma análise de diversas referências sobre o assunto, buscando obter um conjunto de resultados, exemplos e demonstrações consistentes.

Palavras-chave: Grupos. Anéis. Módulos. Homomorfismo de módulos. Sequências exatas.

ABSTRACT

Guimarães de Vasconcelos Neto, Ary. **Introduction to Homological Álgebra**. 2020. 51 f. Trabalho de Conclusão de Curso (Graduação) – Licenciatura em Matemática. Universidade Tecnológica Federal do Paraná. Cornélio Procópio, 2020

The work in question has as main objective to be an alternative material for the reader who seeks to start his studies in Homological Algebra. Here we will study the structures on sets called modules, an algebraic structure that generalizes the concept of vector space. For the development of this material, an analysis was made of several references on the subject, seeking to obtain a set of results, examples and consistent statements.

Keywords: Groups. Rings. Modules. Modules homomorphisms. Exact sequences.

SUMÁRIO

1 INTRODUÇÃO

A álgebra moderna é uma das áreas mais rigorosas da matemática, e fundamental em diversos ramos desta ciência. Dentre os conceitos algébricos, são destacados aqueles abordados em Álgebra Homológica, uma ferramenta muito importante para cálculos em Topologia Algébrica, área esta que por sua vez tem por objetivo resolver problemas topológicos através da Álgebra. Em Álgebra Homológica é estudada uma estrutura sobre um conjunto chamada de módulo sobre um anel, que é uma generalização do conceito de espaço vetorial. Posteriormente, serão exibidos conceitos relacionados à sequências exatas sobre módulos, que serão úteis para definir alguns grupos importantes em Topologia Algébrica, tais como: grupos de homologia e cohomologia.

O objetivo deste trabalho consiste em fazer um estudo inicial da teoria de módulos. Inicialmente, será feito o estudo conceitual de módulos sobre anéis, bem como as demonstrações de suas propriedades. Posteriormente, a teoria de sequências exatas de módulos é abordada, onde o leitor terá acesso a definições e teoremas fundamentais para esta área. O propósito de tal estudo é avançar em temas avançados da Álgebra, que não são abordados no curso de Licenciatura em Matemática da UTFPR-CP.

Este texto está dividido em três capítulos além desta introdução, os quais serão descritos um pouco melhor nos próximos parágrafos.

No Capítulo 2 é feita uma breve revisão de alguns conceitos de Álgebra, tais como: grupos, anéis e ideais dentre outros, que serão importantes para a fundamentação teórica de módulos sobre anéis. As principais referências utilizadas neste capítulo foram: (MILIES, 1972) e (DOMINGUES; IEZZI, 2018). Caso o leitor tenha curiosidade, é sugerido tais referências para maiores detalhes.

No Capítulo 3 é dado início ao estudo da teoria de módulos, a que se propõe este Trabalho de Conclusão de Curso. Neste capítulo, é apresentada a definição de módulos sobre anéis, demonstradas diversas propriedades, e feito também o estudo do conceito de homomorfismo de módulos, que será importante para o estudo de sequências exatas de módulos. Finalizamos com a demonstração de diversas versões do Teorema do Isomorfismo, para módulos. Para este estudo são usadas (MILIES, 1972) e (HU, 1968) como referências, as quais indicamos ao leitor que esteja interessado nos assuntos aqui abordados.

Já no Capítulo 4 o leitor é apresentado às sequências exatas, conteúdo final deste trabalho. Neste capítulo, são apresentadas as definições de sequências exatas sobre módulos, comutatividade entre sequências, e demonstrações de diversas proposições. Dentre os resultados demonstrados, cabe citar o Lema dos Três, Lema dos Quatro e Lema dos Cinco, que são juntos os principais resultados apresentados neste trabalho. Para tal estudo e demonstrações, são usadas (HU, 1968) e (MILIES, 1972) como referências, caso o leitor tenha interesse.

Este trabalho é finalizado com algumas considerações finais.

2 PRELIMINARES

Neste capítulo faremos uma revisão de alguns conceitos e resultados de Álgebra, mais precisamente da teoria de grupos e anéis. Para mais detalhes sugerimos ao leitor as referências (MILIES, 1972) e (DOMINGUES; IEZZI, 2018).

2.1 GRUPOS

O conceito de Grupo como conhecemos hoje teve início na primeira metade do século XIX, com um jovem matemático chamado Evariste Galois $(1811 - 1832)$. Galois buscava provar que não é possível resolver equações de grau maior que 4 por radicais, algo que outros matemáticos já haviam tentado antes dele, mas sem sucesso. Para tal feito, criou conceitos de estruturação de conjuntos chamados grupos, onde dentro destes algumas leis deveriam ser respeitadas, e com isso provou posteriormente que as equações de grau maior que 4 não são resolúveis por radicais. Uma de suas usualidades é a de ser um conceito necessário para definir o que é um módulo, portanto cabe definir aqui:

Definição 2.1. *Um par $(G, *)$, constituído de um conjunto não vazio G e uma operação $*$ sobre G é chamado de* **grupo** *se valem os axiomas a seguir:*

a) Associatividade

$$(a * b) * c = a * (b * c), \text{ para quaisquer } a, b, c \in G;$$

b) Existência do elemento neutro

Existe um único elemento $e \in G$, chamado elemento neutro, tal que

$$e * a = a * e = a, \text{ para todo } a \in G;$$

c) Existência dos simétricos

Para todo $a \in G$, existe um elemento em G, chamado de inverso de a, e denotado por a', tal que

$$a * a' = a' * a = e.$$

Se além disso, valer o axioma

d) Comutatividade

$$a * b = b * a, \text{ para quaisquer } a, b \in G$$

dizemos que $(G, *)$ é um **grupo abeliano**.

Exemplo 2.2. *O conjunto dos números inteiros é um grupo em relação a operação adição* $+$*, denotado por* $(\mathbb{Z}, +)$*, onde o elemento neutro é* 0 *e se* $z \in \mathbb{Z}$*, então* $z' = -z$ *é seu simétrico.*

Definição 2.3. *Dado um grupo* $(G, *)$*, dizemos que um subconjunto* $H \subset G$ *não vazio é um* **subgrupo** *de* G *se:*

a) H *é fechado para a operação* $*$*, ou seja, dados* $a, b \in H$*, então* $a * b \in H$*;*

b) $(H, *)$ *é um grupo.*

Exemplo 2.4. *O conjunto* $(2\mathbb{Z}, +)$ *definido por* $2\mathbb{Z} = \{2z \mid z \in \mathbb{Z}\}$*, dos inteiros pares, é um subgrupo do grupo aditivo* $\mathbb{Z}$*.*

De fato, note que $2\mathbb{Z}$ *é não vazio, pois* $0 = 2 \cdot 0 \in 2\mathbb{Z}$*.*

Agora, dados $k_1 = 2z_1$*,* $k_2 = 2z_2$ *e* $k_3 = 2z_3$ *elementos de* $2\mathbb{Z}$*, temos:*

$$k_1 + k_2 = 2z_1 + 2z_2 = 2(z_1 + z_2) \in 2\mathbb{Z},$$

ou seja, $2\mathbb{Z}$ *é fechado om relação à operação de adição.*

Vale também a propriedade associativa:

$$\begin{aligned}(k_1 + k_2) + k_3 &= (2z_1 + 2z_2) + 2z_3 \\ &= [2(z_1 + z_2)] + 2z_3 = 2(z_1 + z_2 + z_2) \\ &= 2z_1 + [2(z_2 + z_3)] = 2z_1 + (2z_2 + 2z_3) \\ &= k_1 + (k_2 + k_3).\end{aligned}$$

O elemento neutro é $0 = 2 \cdot 0 \in 2\mathbb{Z}$*, e o simétrico de um elemento* $2z \in 2\mathbb{Z}$*, é* $-(2z) = 2(-z)$*.*

Para ser provada a próxima proposição, é necessário o conceito de regularidade (ou lei do cancelamento) para um elemento de um conjunto, que será definido como:

Definição 2.5. *Seja* $*$ *uma operação sobre um conjunto* A*. Dizemos que um elemento* $a \in A$ *é* **regular à esquerda** *(à direita) em relação à operação* $*$ *se, para quaisquer* $x, y \in A$ *tais que* $a * x = a * y$ *(*$x * a = y * b$*), segue que* $x = y$*.*

Proposição 2.6. *Se uma operação* $*$ *sobre um conjunto* A *é associativa, tem elemento neutro* e *e* $a \in A$ *é simetrizável, então* a *é um elemento regular.*

Demonstração: Sejam $x, y \in A$ tais que

$$a * x = a * y.$$

como a é simetrizável, segue que

$$a' * (a * x) = a' * (a * y).$$

Daí, utilizando a associatividade

$$(a' * a) * x = (a' * a) * y \Rightarrow e * x = e * y \Rightarrow x = y.$$

Com isso, é demonstrado a regularidade à esquerda. A demonstração da regularidade à direita é análoga. □

Observação 2.7. *Da proposição anterior concluímos que todo elemento de um grupo é regular para sua operação.*

Proposição 2.8. *Seja $(G, *)$ um grupo. Um subconjunto não vazio $H \subset G$ é um subgrupo de G, se e somente se, dados $a, b \in H$, $a * b' \in H$.*

Demonstração: Sejam e_h, e os respectivos elementos neutros de H e G. Como

$$e_h * e_h = e_h = e_h * e,$$

e pela proposição anterior em um grupo vale a lei do cancelamento, tem-se que $e_h = e$. Tome agora $b \in H$ e seus respectivos simétricos b' e b'_h nos grupos G e H. Então,

$$b'_h * b = e_h = e = b' * b,$$

Novamente pela regularidade,

$$b'_h = b'.$$

Por fim, se $a, b \in H$, então, como H é um grupo fechado para a operação de seus elementos,

$$a * b'_h \in H,$$

mas $b'_h = b'$, logo $a * b' \in H$.

Reciprocamente, como H é não vazio, pode ser escolhido um elemento $k \in H$ de modo que pela hipótese

$$k * k' \in H \Rightarrow e \in H.$$

Seja agora um elemento $b \in H$, que novamente pela hipótese, tem-se que

$$e * b' \in H \Rightarrow b' \in H.$$

Além disso, dados $a, b \in H$

$$a * b' \in H \Rightarrow a * (b')' = a * b \in H$$

Como mostramos que H é fechado para a operação $*$ e $H \subset G$, a associatividade de G vale também em H. Logo, H é um grupo. □

2.2 ANÉIS

O conceito de anel como definido à seguir é essencial para o estudo dos próximos conceitos deste trabalho. O próprio módulo, principal estrutura da Álgebra Homológica, depende estritamente dos conceitos de grupo e anel para ser definido. Com isso, a definição formal de anel como usaremos à seguir é dada por:

Definição 2.9. *Um conjunto não vazio A é um* **anel** *se em A estão definidas duas operações, que serão indicadas por $+$ e $\cdot$, tais que para todos $a, b, c \in A$ verificam-se:*

a) Associatividade da soma:

$$(a+b)+c = a+(b+c);$$

b) Comutatividade da soma:

$$a+b = b+a;$$

c) Elemento nulo:

existe elemento em A, denotado por 0, de modo que $a+0 = 0+a = a$;

d) Existência do oposto:

existe elemento, denotado por $-a$ tal que $a+(-a) = (-a)+a = 0$;

e) Associatividade multiplicativa:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c);$$

f) Distributividade da multiplicação em relação a soma:

$$a \cdot (b+c) = a \cdot b + a \cdot c \text{ e } (b+c) \cdot a = b \cdot a + c \cdot a$$

Usaremos a notação $(A, +, \cdot)$ para representar um anel com operações $+$ e $\cdot$.

Observação 2.10. *As quatro primeiras propriedades dizem que um anel A, com respeito à operação $+$, é um grupo abeliano.*

Um anel A será chamado de **anel comutativo** *se é válido o seguinte axioma:*

g) Comutatividade da multiplicação:

para todos $a, b \in A$, temos

$$a \cdot b = b \cdot a;$$

Um anel será chamado com **unidade** *se verifica-se:*

h) *Existência do elemento neutro multiplicativo:*

Existe elemento em A, denotado por 1, $1 \neq 0$, tal que

$$1 \cdot a = a \cdot 1 = a,$$

para todo $a \in A$.

Por fim, um anel será chamado de **anel de integridade** *ou* **domínio de integridade** *se é um anel comutativo com unidade, e além disso verifica-se:*

i) *Lei do anulamento do produto:*

dados $a, b \in A$,

$$\text{se } a \cdot b = 0, \text{ então } a = 0 \text{ ou } b = 0.$$

Exemplo 2.11. *O conjunto dos números inteiros é um anel de integridade em relação as operações usuais de soma e multiplicação de números inteiros.*

Definição 2.12. *Sejam A e B anéis. Definimos o* **produto direto** *de A por B como o conjunto $A \times B = \{(a, b) \mid a \in A, b \in B\}$, onde são definidas em $A \times B$ as seguintes operações:*

$$\begin{aligned} (a_1, b_1) + (a_2, b_2) &= (a_1 + a_2, b_1 + b_2); \\ (a_1, b_1) \cdot (a_2, b_2) &= (a_1 \cdot a_2, b_1 \cdot b_2). \end{aligned}$$

Podemos provar que $A \times B$ com as operaões definidas anteriormente é um anel.

De maneira análoga, dada uma família $A_1, A_2, \ldots, A_n$ de anéis, podemos definir o anel produto direto desta família como:

$$A = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i\},$$

onde a adição e multiplicação de elementos de A é feita termo a termo.

Definição 2.13. *Sejam A um anel e B um subconjunto não vazio de A. É dito que B é um* **subanel** *de A se*

a) *B é fechado para as operações $+$ e $\cdot$ do anel A, ou seja, dados $a, b \in B$, então $a + b \in B$ e $a \cdot b \in B$;*

b) *B admite uma estrutura de anel em relação as operações do anel A.*

Proposição 2.14. *Seja A um anel. Um subconjunto não vazio B de A é um subanel de A se, e somente se, dados $a, b \in B$,*

$$a - b \in B \text{ e } a \cdot b \in B.$$

Demonstração: Com efeito, seja B subanel de A. Então o grupo B é subgrupo do grupo abeliano A. Logo, pela Proposição 2.8

$$a + (-b) = a - b \in B.$$

Além disso, como B é um anel e $a, b \in B$, vale também que $a \cdot b \in B$.

Por outro lado, se dados $a, b \in B$ temos $a - b \in B$, então B é subgrupo de A pela Proposição 2.8. Como B é fechado para a multiplicação por hipótese, e $B \subset A$, onde A é um anel, então valem as propriedades associativas e distributivas em relação a multiplicação. □

Definição 2.15. *Um elemento a de um anel com unidade A é* **invertível** *se existe um elemento em A, denotado por a^{-1}, de modo que*

$$a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

A definição acima é de extrema importância, pois com ela pode ser definido um tipo de anel bastante utilizado:

Definição 2.16. *Seja A um anel. Dizemos que A é um* **corpo** *se A é um domínio de integridade, ou seja, é um anel comutativo com unidade onde vale a lei do anulamento, e além disso, para cada $a \in A$, $a \neq 0$, existe $a^{-1} \in A$, ou seja, todos os seus elementos não nulos são invertíveis.*

Exemplo 2.17. *O conjunto dos números reais $\mathbb{R}$, com as operações usuais de adição e multiplicação, é um corpo.*

2.3 HOMOMORFISMOS DE ANÉIS

Definição 2.18. *Sejam $(A, +, \cdot)$ e $(B, +, \cdot)$ anéis. Uma função $f : A \to B$ é um* **homomorfismo de anéis** *se dados $a, b \in A$,*

a) $f(a + b) = f(a) + f(b)$;

b) $f(a \cdot b) = f(a) \cdot f(b)$.

Exemplo 2.19. *Sejam $(A, +, \cdot)$ e $(B, +, \cdot)$ anéis. A função definida por:*

$$\begin{array}{rcl} f : A & \longrightarrow & B \\ a & \longmapsto & f(a) = 0 \end{array}$$

é um homomorfismo, pois dados $a, b \in A$,

i) $f(a + b) = 0 = 0 + 0 = f(a) + f(b)$;

ii) $f(a \cdot b) = 0 = 0 \cdot 0 = f(a) \cdot f(b)$.

Tal homomorfismo é denominado **Homomorfismo nulo**.

Exemplo 2.20. *Considere* $A = \mathbb{Z}$ *e* $B = \mathbb{Z} \times \mathbb{Z}$ *(produto direto) e* $f : A \to B$ *a função definida por* $f(z) = (z, 0)$*, temos que* f *é um homomorfismo, pois dados* $z_1, z_2 \in \mathbb{Z}$*,*

a) $f(z_1 + z_2) = (z_1 + z_2, 0) = (z_1, 0) + (z_2, 0) = f(z_1) + f(z_2)$*;*

b) $f(z_1 \cdot z_2) = (z_1 \cdot z_2, 0) = (z_1, 0) \cdot (z_2, 0) = f(z_1) \cdot f(z_2)$*.*

Serão destacadas agora algumas propriedades referentes aos homomorfismos que serão importantes para os estudos seguintes.

Proposição 2.21. *Se* $f : A \to B$ *é um homomorfismo de anéis, então:*

i) $f(0) = 0$*;*

ii) $f(-a) = -f(a)$*;*

iii) $f(a - b) = f(a) - f(b)$*.*

Demonstração:

i) Note que

$$f(0) + f(0) = f(0 + 0) = f(0) = f(0) + 0,$$

como vale a propriedade do cancelamento para a soma no anel, concluímos que

$$f(0) = 0.$$

ii) Como

$$f(a) + f(-a) = f[a + (-a)] = f(0) = 0 = f(a) - f(a)$$

novamente, pela regularidade dos elementos de um anel com respeito a adição, concluímos que

$$f(-a) = -f(a).$$

iii) Por último,

$$f(a - b) = f[a + (-b)] = f(a) + f(-b) = f(a) - f(b). \quad \square$$

Exemplo 2.22. *Sejam* $A = M_2(\mathbb{Q})$ *e* $A' = M_3(\mathbb{Q})$ *e defina* $f : A \to A'$ *um homomorfismo tal que*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Q}) \longrightarrow \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{bmatrix} \in M_3(\mathbb{Q})$$

Note que neste exemplo a identidade de A *não levará a identidade de* A'*, portanto, nem sempre* $f(1) = 1$*. Os resultados a seguir irão assegurar em quais momentos podemos garantir esta propriedade.*

Proposição 2.23. *Sejam A e A' anéis com unidade e $f : A \to A'$ um homomorfismo de anéis. Sob estas condições:*

i) Se A é um domínio de integridade, então $f(1) = 1$.

ii) Se f é um homomorfismo sobrejetor, então, $f(1) = 1$.

Demonstração:

i) Temos que

$$f(1) \cdot f(1) = f(1 \cdot 1) = f(1) = f(1) \cdot 1.$$

Assim, como um anel é domínio de integridade se, e somente se todos seus elementos não-nulos obedecem a lei do cancelamento, obtêm-se que

$$f(1) = 1.$$

ii) Seja $b \in A'$. Logo, existe $a \in A$ tal que $b = f(a)$, e daí

$$b \cdot f(1) = f(a) \cdot f(1) = f(a \cdot 1) = f(a) = b.$$

Analogamente,

$$f(1) \cdot b = f(1) \cdot f(a) = f(1 \cdot a) = f(a) = b.$$

Logo, $f(1)$ é a unidade de A'. □

Definição 2.24. *Seja $f : A \to A'$ um homomorfismo de anéis, onde A e A' são anéis com unidade. Dizemos que f é um homomorfismo de anéis com unidade se $f(1) = 1$.*

A seguir serão introduzidas algumas terminologias de uso frequente no estudo de homomorfismos de anéis.

Definição 2.25. *Um homomorfismo de anéis é denominado um* **epimorfismo** *se é um homomorfismo sobrejetor; um* **monomorfismo** *se for injetor e um* **isomorfismo** *se for injetor e sobrejetor. Finalmente, um homomorfismo de um anel em sí próprio é chamado* **automorfismo**, *e um isomorfismo nestas condições é chamado* **endomorfismo**.

Proposição 2.26. *Se $f : A \to B$ é um homomorfismo de anéis, e L é um subanel de A, então $f(L)$ é um subanel de B.*

Demonstração: Se $c, d \in f(L)$, então existem $a, b \in L \subset A$ de modo que $f(a) = c$ e $f(b) = d$. Logo,

$$c - d = f(a) - f(b) = f(a - b).$$

Como L é um subanel, $a - b \in L$, portanto $c - d \in f(L)$. Além disso,

$$c \cdot d = f(a) \cdot f(b) = f(a \cdot b)$$

onde $a \cdot b \in L$, e portanto $f(L)$ é fechado para a multiplicação, e pela Proposição 2.14, $f(L)$ é subanel de B. □

Definição 2.27. *Seja $f : A \to B$ um homomorfismo de anéis. A* **imagem** *de f é o conjunto definido por*

$$Im(f) = \{b \in B \mid \exists a \in A, f(a) = b\}.$$

O **núcleo** *de f é o conjunto*

$$Ker(f) = \{a \in A \mid f(a) = 0\}.$$

Proposição 2.28. *Sejam A e B anéis e $f : A \to B$ homomorfismo. Então, $Ker(f)$ é subanel de A e $Im(f)$ é subanel de B.*

Demonstração: De fato, $Ker(f) \subset A$, e sendo assim, dados $a, b \in Ker(f)$

$$f(a - b) = f(a) - f(b) = 0 - 0 = 0,$$

isto é, $a - b \in Ker(f)$. Além disso,

$$f(a \cdot b) = f(a) \cdot f(b) = 0 \cdot 0 = 0,$$

ou seja, $a \cdot b \in Ker(f)$.

Logo, da Proposição 2.14, segue que $Ker(f)$ é subanel de A.

Agora, dados $c, d \in Im(f)$ existem $a, b \in A$ de modo que $c = f(a)$ e $d = f(b)$. Logo,

$$c - d = f(a) - f(b) = f(a - b) \in Im(f)$$

e

$$c \cdot d = f(a) \cdot f(b) = f(a \cdot b) \in Im(f),$$

o que conclui nossa demonstração. □

2.4 IDEAIS

O conceito de ideal como será apresentado aqui nada mais é do que um caso específico de subanel. Porém, é importante destacarmos os ideais como estruturas fundamentais para o desenvolvimento de nossos estudos, pois apenas com ele podemos definir outros conceitos muito usados na Álgebra Homológica, como por exemplo as classes de equivalência e o módulo quociente.

Definição 2.29. *Um subconjunto I de um anel A é chamado* **ideal à esquerda de** *A se verifica:*

a) I é um subgrupo do grupo aditivo A;

b) *Para todo $a \in I$ e $\alpha \in A$, tem-se que $\alpha \cdot a \in I$.*

Observação 2.30. *O nome ideal à esquerda provém do fato da segunda propriedade se referir a multiplicação de elementos do anel à esquerda. De maneira análoga, é possível definir um ideal à direita. Caso um subconjunto de A seja simultaneamente ideal à direita e à esquerda, dizemos que o mesmo é um* **ideal bilateral** *de A. Para facilitar a escrita, quando o nome ideal for usado, considere o mesmo como um ideal bilateral em A.*

Exemplo 2.31. *O subanel $2\mathbb{Z}$ dos inteiros pares é um ideal do anel $\mathbb{Z}$.*

Proposição 2.32. *Seja $f : A \to A'$ um homomorfismo de anéis. Então, $Ker(f)$ é um ideal de A.*

Demonstração: De fato, pela Proposição 2.28, $Ker(f)$ é subgrupo aditivo de A, e além disso, dados $a \in Ker(f)$ e $\alpha \in A$,

$$f(\alpha \cdot a) = f(\alpha) \cdot f(a) = f(\alpha) \cdot 0 = 0,$$

o que implica em $\alpha \cdot a \in Ker(f)$, e

$$f(a \cdot \alpha) = f(a) \cdot f(\alpha) = 0 \cdot f(\alpha) = 0,$$

isto é, $a \cdot \alpha \in Ker(f)$. Portanto, concluímos que $Ker(f)$ é um ideal de A. □

Exemplo 2.33. *Se A é um anel e $a \in A$, será denotado por $A \cdot a$ o conjunto de todos os múltiplos de a, isto é,*

$$A \cdot a = \{\alpha \cdot a \mid \alpha \in A\}.$$

Temos que $A \cdot a$ é um ideal de A.

De fato, note que dados $k_1, k_2 \in A \cdot a$, então $k_1 = \alpha_1 \cdot a$ e $k_2 = \alpha_2 \cdot a$; Logo

$$k_1 - k_2 = \alpha_1 \cdot a - \alpha_2 \cdot a = (\alpha_1 - \alpha_2) \cdot a$$

Como $\alpha = \alpha_1 - \alpha_2 \in A$, então $\alpha \cdot a \in A \cdot a$. Além disso, dado $k = \alpha \cdot a \in A \cdot a$ e $\beta \in A$,

$$\beta \cdot k = \beta \cdot (\alpha a) = (\beta\alpha) \cdot a.$$

Como $\beta\alpha \in A$, então $(\beta\alpha) \cdot a \in A \cdot a$. Portanto, $A \cdot a$ é um ideal.

Sejam agora A um anel e I um ideal de A. Será definida em A a seguinte relação:

Dados $a, b \in A$, dizemos $a \sim b$ se, e somente se, $a - b \in I$. Esta relação é uma relação de equivalência em A, pois:

1) Temos que $a - a = 0 \in I$, isto é, $a \sim a$. Logo, a relação é reflexiva.

2) Se $a \sim b$, então $a - b \in I$, logo, $-(a - b) = b - a \in I$, ou seja, $b \sim a$. A relação é portanto simétrica.

3) Por fim, se $a \sim b$ e $b \sim c$, então $a - b \in I$ e $b - c \in I$. Logo, a soma

$$(a - b) + (b - c) = a - c \in I,$$

e portanto $a \sim c$. Assim a relação é transitiva.

Será denotado por A/I o conjunto das classes de equivalência, onde a classe de um elemento $a \in A$ é o subconjunto

$$\overline{a} = a + I = \{a + m \mid m \in I\}.$$

No conjunto A/I, é possível definir uma operação, a partir da adição de A da seguinte forma:

$$\overline{a} + \overline{b} = \overline{a + b},$$

isto é,

$$(a + I) + (b + I) = (a + b) + I.$$

Tal operação está bem definida, pois independe de representante, isto é, se a_1 é um representante de $\overline{a}$ e b_1 é um representante de $\overline{b}$, então

$$\overline{a_1} + \overline{b_1} = \overline{a_1 + b_1}.$$

Agora,

$$(a_1 + b_1) - (a + b) = (a_1 - a) + (b_1 - b)$$

onde por hipótese $(a_1 - a) \in I$ e $(b_1 - b) \in I$, de onde é possível concluir que

$$(a_1 + b_1) - (a + b) \in I,$$

e portanto $\overline{a_1 + b_1} = \overline{a + b}$.

Ainda, se I é um ideal bilateral, podemos definir um produto em A/I por:

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b},$$

isto é,

$$(a + I) \cdot (b + I) = (a \cdot b) + I$$

Esta operação também independe de representantes, pois se $a_1 \in \overline{a}$ e $b_1 \in \overline{b}$, então $a - a_1 \in I$ e $b - b_1 \in I$. Como I é um ideal,

$$b \cdot (a - a_1) \in I \text{ e } a_1 \cdot (b - b_1) \in I.$$

Assim, utilizando a propriedade distributiva e a propriedade associativa, temos que

$$\begin{aligned} b \cdot (a - a_1) - a_1 \cdot (b - b_1) &= (b \cdot a - b \cdot a_1) - (a_1 \cdot b - a_1 \cdot b_1) \\ &= b \cdot a - (b \cdot a_1 - a_1 \cdot b) + a_1 \cdot b_1 \\ &= b \cdot a + a_1 \cdot b_1 \\ &= a \cdot b + a_1 \cdot b_1 \in I. \end{aligned}$$

Logo, $\overline{a \cdot b} = \overline{a_1 \cdot b_1}$.

Definição 2.34. *Sejam A um anel e $I \subset A$ um ideal bilateral. O anel A/I construído acima é chamado* **anel quociente** *de A pelo ideal I.*

Exemplo 2.35. *O conjunto das classes de equivalência do anel quociente $\mathbb{Z}/2\mathbb{Z}$ é exatamente o conjunto*

$$\mathbb{Z}/2\mathbb{Z} = \{z + 2\mathbb{Z} \mid z \in \mathbb{Z}\}.$$

Considere agora a aplicação $j : A \to A/I$ definida por:

$$\begin{array}{rccc} j : & A & \longrightarrow & A/I \\ & a & \longmapsto & a + I \end{array}$$

isto é, a função que associa a cada elemento do anel à sua classe no anel quociente.

Esta função é um epimorfismo, pois tomando $a, b \in A$,

$$j(a + b) = (a + b) + I = (a + I) + (b + I) = j(a) + j(b)$$

$$j(a \cdot b) = (a \cdot b) + I = (a + I) \cdot (b + I) = j(a) + j(b)$$

o que implica j ser um homomorfismo.

Suponha então que j não seja sobrejetora, ou seja, $Im(j) \neq A/I$. Logo, existe $\overline{a} \in A/I$ tal que $\overline{a}$ não está em $Im(j)$. Portanto, não existe um elemento $a \in A$ de modo que $j(a) = a + I = \overline{a}$, o que gera uma contradição com o elemento a, pois $A/I = \{a + I \mid a \in A\}$. O que conclui a demonstração.

Tal homomorfismo terá um importante papel no estudo de homomorfismos de módulos no capítulo a seguir, o que torna interessante destacar algumas propriedades:

1) $j(0) = I$.

2) Se A tem unidade, então $j(1)$ é a unidade de A/I.

3) $Ker(j) = 0 + I = I$, onde I é o elemento neutro de A/I.

Isso mostra que para todo ideal $I \subset A$, existe ao menos um homomorfismo j tal que $I = Ker(j)$. O epimorfismo definido acima é denominado **epimorfismo canônico**.

3 MÓDULOS

Neste capítulo, o leitor será apresentado à base da Álgebra Homológica. Nele, serão definidos conceitos relacionados à Álgebra abstrata, Álgebra Homológica e Álgebra linear. As principais referências utilizadas neste capítulo são: (HU, 1968), (COELHO; LOURENÇO, 2005) e (MILIES, 1972).

Definição 3.1. *Seja A um anel com unidade. Dizemos que um conjunto não vazio M é um* **módulo à esquerda** *sobre A ou um A-módulo à esquerda se M é um grupo abeliano em relação a uma operação, que será indicado por $+$, e está bem definida uma lei de composição externa que a cada par $(\alpha, m) \in A \times M$ associa um elemento $\alpha m \in M$ e tal que, para todos $\alpha_1, \alpha_2 \in A$ e todos $m_1, m_2 \in M$, verifica-se:*

i) $\alpha_1(\alpha_2 m_1) = (\alpha_1 \alpha_2) m_1$;

ii) $\alpha_1(m_1 + m_2) = \alpha_1 m_1 + \alpha_1 m_2$;

iii) $(\alpha_1 + \alpha_2) m_1 = \alpha_1 m_1 + \alpha_2 m_1$;

iv) $1 \cdot m_1 = m_1$, *onde 1 é a unidade do anel A.*

Observação 3.2.
- *Da mesma forma que definido acima, também podemos definir um A-módulo à direita.*
- *Caso M seja um A-módulo à direita e à esquerda, diremos que M é um módulo bilateral.*

No que segue, a menos que se diga o contrário, os módulos serão bilaterais.

Exemplo 3.3. *Das propriedades de espaços vetoriais, segue que todo espaço vetorial sobre um corpo $\mathbb{K}$ é um $\mathbb{K}$-módulo. Ou seja, de certa forma, o módulo generaliza o conceito de espaço vetorial.*

Exemplo 3.4. *Todo grupo abeliano G aditivo pode ser considerado como um $\mathbb{Z}$-módulo definindo o produto de um inteiro n por um elemento $g \in G$ como:*

$$\begin{aligned} ng = g + g + g + \cdots + g \quad (n \text{ parcelas}), \quad \text{se } n > 0 \\ ng = (-g) + (-g) + \cdots + (-g) \quad (|n| \text{ parcelas}), \quad \text{se } n < 0 \\ 0g = 0. \end{aligned}$$

Exemplo 3.5. *Seja A um anel e X um conjunto qualquer. Será indicado por A^X o conjunto de todas as funções de domínio em X que assumem valores em A. Com isso, o conjunto $A^X = \{\varphi \in A^X; \varphi : X \to A\}$ admite uma estrutura de A-módulo em relação a soma usual de funções e a multiplicação de um escalar à esquerda por uma função como definido abaixo.*

A multiplicação de elementos de A (escalar) por elementos de A^X será feita associando a cada par $(a, \varphi) \in A \times A^X$ a função $a \cdot \varphi \in A^X$ e definida por

$$(a\varphi)(x) = a \cdot \varphi(x), \text{ para todo } x \in X.$$

Exemplo 3.6. *Sejam V um $\mathbb{K}$-espaço vetorial e $T : V \to V$ uma transformação linear. Dado um polinômio $f \in \mathbb{K}[X]$ da forma*

$$f = a_0 + a_1X + a_2X^2 + ... + a_nX^n,$$

será indicada por $f(T)$ a transformação linear

$$f(T) = a_0I + a_1T + ... + a_nT^n,$$

onde I representa a transformação identidade de V em V e $T^n = T \circ T^{n-1}$, ou seja, a n-ésima composta de T, onde $T^1 = T$.

Assim, pode ser estabelecida uma estrutura de $\mathbb{K}[X]$-módulo em V, conservando a soma e associando a cada par $(f, v) \in \mathbb{K}[X] \times V$ o elemento $f(T)(v) \in V$, onde a última indica a função $f(T)$ aplicada no vetor v.

Definição 3.7. *Seja M um A-módulo. Um subconjunto $N \subset M$ será um* **A-submódulo** *de M, ou* **submódulo** *se:*

a) N é um subgrupo aditivo de M.

b) N é fechado em relação à multiplicação por escalares, isto é, para todo $a \in A$ e $n \in N$, obtêm-se que $a \cdot n \in N$.

Proposição 3.8. *Seja M um A-módulo. Um subconjunto não vazio $N \subset M$ é um submódulo se, e somente se,*

i) dados $n, n' \in N$, então $n + n' \in N$, onde n' é o oposto aditivo de n, e

ii) dado $a \in A$, para todo $n \in N$, $a \cdot n \in N$.

Demonstração: Seja M um A-módulo e $N \subset M$ um submódulo. Temos que N é um subgrupo aditivo de M, portanto, pela definição de subgrupo, dados $n, n' \in N$, temos que $n + n' \in N$ e além disso, segue da definição de submódulo que N é fechado para a multiplicação por escalares de A, portanto é um submódulo. Por outro lado, se M é A-módulo, então em particular M é grupo. Sendo assim, dado $N \subset M$ tal que vale i), pela Proposição 2.8, N é subgrupo aditivo de M. Além disso, pela hipótese de que N é fechado para a multiplicação de escalares de A, N é um A-submódulo e está concluída a demonstração. $\square$

Exemplo 3.9. *Se N_1 e N_2 são submódulos de um A-módulo M, o conjunto*

$$N_1 + N_2 = \{n_1 + n_2; n_1 \in N_1, n_2 \in N_2\}$$

também é um submódulo de M, chamado submódulo da soma. De fato, o conjunto é não vazio, pois

$$0 + 0 = 0 \in N_1 + N_2.$$

Agora, sejam $n_1 + n_2, n_1' + n_2' \in N_1 + N_2$, com $n_1, n_1' \in N_1$ e $n_2, n_2' \in N_2$. Então

$$\begin{aligned}(n_1 + n_2) + (n_1' + n_2') &= (n_1 + n_1') + (n_2 + n_2') \\ &= 0_{N_1} + 0_{N_2} \in N_1 + N_2.\end{aligned}$$

Além disso, dado $a \in A$ e $n_1 + n_2 \in N_1 + N_2$,

$$a(n_1 + n_2) = an_1 + an_2 \in N_1 + N_2.$$

Logo, pela Proposição 3.8, $N_1 + N_2$ é um submódulo de M.

Exemplo 3.10. *Se M é um A-módulo e $\{N_i\}_{i \in I}$ uma família de submódulos de M, então $\bigcap_{i \in I} N_i$ é um submódulo de M.*

Exemplo 3.11. *Se I é um ideal de um anel A e m um elemento fixado de um A-módulo M, então o conjunto*

$$I \cdot m = \{\alpha m; \alpha \in I\}$$

é um submódulo de M.

De fato, note primeiramente que $I \cdot m$ é não vazio, pois existe $0 \in I$ e $0 \cdot m = 0 \in I \cdot m$. Agora, dado um $k \in I \cdot m$, existe $i_k \in I$ tal que $i_k m = k$. Do mesmo modo, pela propriedade de ideal, deve existir $-i_k \in I$ de maneira que

$$(-i_k)m = -(i_k m) = -k \in I \cdot m.$$

Daí,

$$k + (-k) = (i_k m) + (-i_k m) = i_k m - i_k m = (i_k - i_k)m = 0 \in I \cdot m.$$

Tome agora $a \in A$ e $k \in I \cdot m$, logo

$$ak = a(i_k m) = (ai_k)m \in I \cdot m,$$

pois I é fechado para a multiplicação de escalares de A. Portanto, pela Proposição 3.8, $I \cdot m$ é um submódulo de M.

Definição 3.12. *Sejam A um anel e M um A-módulo. O conjunto*

$$Anl(M) = \{a \in A; am = 0, \forall m \in M\}$$

é chamado **anulador do módulo** *M. Em particular, se $Anl(M) = \{0\}$, então M é chamado um A-***módulo fiel**.

Proposição 3.13. *Seja A um anel e M um A-módulo. Então, $Anl(M)$ é um ideal bilateral de A e M é um $A/Anl(M)$-módulo fiel.*

Demonstração: De fato, se $Anl(M) = \{0\}$, então $0 - 0 = 0 \in Anl(M)$ e $a \cdot 0 = 0 \in Anl(M), \forall a \in A$, o que conclui esta etapa. Porém, se existe $\alpha \in Anl(M)$ de modo que $\alpha \neq 0$, então fixado um $m \in M$, $\alpha m = 0$ e portanto,

$$0 = -(\alpha m) = (-\alpha)m,$$

daí $-\alpha \in Anl(M)$, logo

$$\alpha - \alpha = 0 \in Anl(M).$$

Se $\alpha \in Anl(M)$ e $k \in A$,

$$(k \cdot \alpha)m = k \cdot (\alpha m) = k \cdot 0 = 0,$$

logo $k\alpha \in Anl(M)$, e com isso, o anulador é um ideal de A. Seja agora M um $A/Anl(M)$-módulo e $Anl(M)^*$ seu anulador. Daí, o conjunto

$$Anl(M)^* = \{\overline{a} \in A/Anl(M); \overline{a}m = 0\}.$$

Com efeito, se $\overline{a}m = \overline{0}$, então $\overline{a} = \overline{0}/m$ e logo, $\overline{a} \equiv \overline{0}(modAnl(M))$, portanto $Anl(M)^* = \{0\}$. □

Seja M um A-módulo e N um submódulo de M. Considerando apenas a estrutura do grupo aditivo abeliano de M é possível definir o grupo quociente

$$M/N = \{m + N \mid m \in M\}$$

cuja lei de composição interna é definida por:

$$(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N.$$

Podemos definir uma multiplicação por escalares de A, associando ao par $(a, m+N) \in A \times M/N$ o elemento $am + N \in M/N$. Nestas condições, a construção acima dá uma estrutura de A-módulo para M/N.

Definição 3.14. *O A-módulo M/N construído acima é denominado* **módulo quociente** *do módulo M pelo submódulo N.*

3.1 HOMOMORFISMOS DE MÓDULOS

Definição 3.15. *Sejam M e N dois A-módulos. Uma função $f : M \to N$ diz-se um* **homomorfismo** *de A-módulos ou um A-homomorfismo se para todo $m_1, m_2 \in M$ e todo $a \in A$ se verifica:*

i) $f(m_1 + m_2) = f(m_1) + f(m_2)$

ii) $f(a \cdot m_1) = a \cdot f(m_1)$.

Exemplo 3.16. *Se $\mathbb{K}$ é um corpo, os $\mathbb{K}$-homomorfismos são as transformações lineares entre espaços vetoriais sobre $\mathbb{K}$.*

Exemplo 3.17. *Dados M e N dois A-módulos, a função trivial $f : M \to N$ definida por $f(m) = 0$, para todo $m \in M$ é um A-homomorfismo, chamado* **homomorfismo nulo**.

Um A-homomorfismo injetor é chamado **A-monomorfismo**, e um A-homomorfismo sobrejetor, **A-epimorfismo**.

Proposição 3.18. *Um A-homomorfismo $f : M \longrightarrow N$ será um epimorfismo se, e somente se, $Im(f) = N$. Da mesma forma, f será um monomorfismo se, e somente se, $Ker(f) = \{0\}$.*

Demonstração: Seja $f : M \longrightarrow N$ um A-epimorfismo. Suponha que $Im(f) \neq N$, então existe $c \in N$ tal que $c \in N - Im(f)$ e f não será sobrejetiva, o que contraria nossa hipótese. Por outro lado, se $Im(f) = N$), dado $c \in N$, existe um elemento $m \in M$ de modo que $c = f(m)$, logo é um epimorfismo. Do mesmo modo, suponha por absurdo f é um A-monomorfismo e $Ker(f) \neq \{0\}$, então existe $k \in ker(f)$ de modo que $f(k) = 0$, o que implica f não ser injetiva, pois $f(k) = 0$ e $f(0) = 0$. Por outro lado, se $f : M \longrightarrow N$ é um homomorfismo e $Ker(f) = 0$, então dados dois elementos quaisquer de M, denotados por m_1, m_2, de modo que $f(m_1) = f(m_2)$, tem-se que:

$$0 = f(m_1) - f(m_2) = f(m_1 - m_2),$$

o que implica $m_1 - m_2 \in Ker(f)$, ou seja, $m_1 = m_2$. Portanto fica provado que f é monomorfismo. $\square$

Exemplo 3.19. *Seja N um submódulo de um A-módulo M. Então a função inclusão $i : N \to M$, que associa o elemento $x \in N$ ao elemento $i(x) = x \in M$, é um A-homomorfismo. De fato, dados $n_1, n_2 \in N$, então*

$$i(n_1 + n_2) = n_1 + n_2 = i(n_1) + i(n_2),$$

e dado $\alpha \in A$, $n \in N$

$$i(\alpha n) = \alpha n = \alpha i(n).$$

Em particular, tomando o submódulo $M \subset M$, o A-homomorfismo inclusão é também o homomorfismo identidade.

Exemplo 3.20. *Seja N um submódulo de um A-módulo M. Definimos o homomorfismo canônico ou projeção canônica a aplicação $j : M \mapsto M/N$ dada por*

$$j(m) = m + N, \forall m \in M.$$

De fato, dados $m_1, m_2 \in M$ *e* $\alpha \in A$

$$\begin{aligned} j(m_1 + m_2) = (m_1 + m_2) + N &= (m_1 + N) + (m_2 + N) \\ &= j(m_1) + j(m_2). \end{aligned}$$

E ainda,

$$\begin{aligned} j(\alpha m) &= (\alpha m) + N \\ &= \alpha(m + N) \\ &= \alpha j(m). \end{aligned}$$

Definição 3.21. *Dado um* A*-homomorfismo* $f : M \to N$*, respectivamente, a* **imagem** *de* f *e o* **núcleo** *de* f *são definidos por:*

i) $Im(f) = \{n \in N \mid \exists m \in M; f(m) = n\}$*;*

ii) $Ker(f) = \{m \in M \mid f(m) = 0\}$.

Proposição 3.22. *Sejam* M *e* N A*-módulos, e* $f : M \mapsto N$ *um homomorfismo. Nestas condições, os subconjuntos* $Ker(f) \subset M$ *e* $Im(f) \subset N$ *admitem uma estrutura de* A*-submódulo.*

Demonstração: De fato, dados $a, b \in Ker(f)$,

$$f(a - b) = f(a) - f(b) = 0 + 0 = 0,$$

o que implica em $a - b \in Ker(f)$. Além disso, dado $\alpha \in A$ e $a \in Ker(f)$ temos que

$$f(\alpha \cdot a) = \alpha \cdot f(a) = \alpha \cdot 0 = 0,$$

isto é, $\alpha a \in Ker(f)$.

Portanto, obtêm-se que $Ker(f)$ admite uma estrutura de A-submódulo.

Agora, dados $c, d \in Im(f)$, existem $a, b \in M$ tais que $f(a) = c$ e $f(b) = d$. Assim

$$c - d = f(a) - f(b) = f(a + (-b)) = f(a - b),$$

o que implica em $c - d \in Im(f)$. Além disso, dado $\alpha \in A$ e $c \in Im(f)$,

$$\alpha \cdot c = \alpha \cdot f(a) = f(\alpha \cdot a) \in Im(f).$$

Portanto, $Im(f)$ também é A-submódulo. □

Exemplo 3.23. *Seja* M *um* A*-módulo. Para cada elemento* $\alpha \in A$*, podemos definir uma função* $f_\alpha : M \to M$ *por* $f_\alpha(m) = \alpha m$*, para todo* $m \in M$*. Tal função chama-se* **homotetia.** *Caso* A *seja um anel comutativo ou,* α *comuta com todo elemento de* A*, então a homotetia* f_α *é um* A*-homomorfismo.*

Proposição 3.24. *i) Sejam $f : M \to M', g : M' \to M''$ dois A-homomorfismos, então $g \circ f : M \to M''$ também é um A-homomorfismo.*

ii) Se $f : M \to M', g : M' \to M''$ e $h : M'' \to M'''$ são A-homomorfismos, então

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

iii) Sejam $f_1, f_2 : M \to M'$ e $g : M' \to M''$, então

$$g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2.$$

iv) Dado um A-homomorfismo $f : M \to N$, se $Id_M : M \to M$ é o homomorfismo identidade, então

$$Id \circ f = f \circ Id = f.$$

v) Dados A-homomorfismos $f : M \to M', g : M' \to M$, tais que $g \circ f = Id_M$, então f é um monomorfismos e g é um epimorfismo.

Definição 3.25. *Um A-homomorfismo $f : M \to N$ é um A-isomorfismo se existe um A-homomorfismo $g : N \to M$ de modo que*

$$g \circ f = Id_M \text{ e } f \circ g = Id_N$$

Proposição 3.26. *Um A-homomorfismo $f : M \to N$ é um isomorfismo, se e somente se, f é simultaneamente monomorfismo e epimorfismo.*

Demonstração: De fato, se $f : M \to N$ é um isomorfismo, então por definição existe uma $g : N \to M$ de modo que

$$g \circ f = Id_M \tag{3.1}$$

$$f \circ g = Id_N \tag{3.2}$$

Pela primeira igualdade, utilizando o resultado anterior, f é um monomorfismo e g um epimorfismo. Utilizando o mesmo raciocínio para a segunda igualdade, obtêm-se que f é um epimorfismo e g um monomorfismo. Logo, f é um monomorfismo e um epimorfismo. Reciprocamente, se f é um monomorfismo e um epimorfismo, existe $g : Im(f) = N \to M$ de modo que vale (3.1) e (3.2). Portanto, f é um isomorfismo. □

Teorema 3.27 (Teorema do homomorfismo para módulos). *Sejam M e N dois A-módulos, $f : M \to N$ um A-homomorfismo, $j : M \to M/Ker(f)$ a projeção canônica e $i : Im(f) \to N$ a inclusão. Existe uma única função $f^* : M/Ker(f) \to Im(f)$ tal que*

i) $f = i \circ f^* \circ j$;

ii) f^* é um A-isomorfismo.

Demonstração: Defina $f^* : M/Ker(f) \to Im(f)$ por

$$f^*(\overline{m}) = f(m), \text{ para todo } m \in M.$$

Note que f^* está bem definida, pois se $m_1, m_2 \in M$ são tais que para $\overline{m_1} = \overline{m_2}$, isto é, tais que $m_1 - m_2 \in Ker(f)$, por um lado, teremos que

$$f^*(\overline{m_1}) = f(m_1) \text{ e } f^*(\overline{m_2}) = f(m_2),$$

e por outro lado

$$f(m_1) - f(m_2) = f(m_1 - m_2) = 0 \Rightarrow f(m_1) = f(m_2),$$

donde segue que $f^*(\overline{m_1}) = f^*(\overline{m_2})$.

Será mostrado agora que f^* é um A-homomorfismo, e que ele é único nas condições do enunciado.

$$\begin{aligned} f^*(\overline{m_1} + \overline{m_2}) &= f^*((m_1 + m_2) + Ker(f)) \\ &= f(m_1 + m_2) \\ &= f(m_1) + f(m_2) \\ &= f^*(m_1 + Ker(f)) + f^*(m_2 + Ker(f)). \end{aligned}$$

Além disso, dado $\alpha \in A$,

$$\begin{aligned} f^*(\alpha\overline{m}) &= f^*(\alpha(m + Ker(f))) \\ &= f^*((\alpha m) + Ker(f)) \\ &= f(\alpha m) = \alpha f(m) \\ &= \alpha f^*(m + Ker(f)). \end{aligned}$$

Logo, f^* é um A-homomorfismo. Sendo assim, temos

$$\begin{aligned} [i \circ f^* \circ j](m) &= [i \circ f^*] \circ j(m) \\ &= [i \circ f^*](m + Ker(f)) \\ &= i[f^*(m + Ker(f)] \\ &= i(f(m)) = f(m) \in N, \end{aligned}$$

e portanto, $(i \circ f^* \circ j)(m) = f(m)$, para todo $m \in M$, isto é, $f = i \circ f^* \circ j$.

Além disso, dado $m \in M$ tal que $f(m) \in Im(f)$, existe $\overline{m} = m + Ker(f) \in M/Ker(f)$ de modo que $f(m) = f^*(\overline{m})$, pela construção de f^*, logo é um epimorfismo.

Por outro lado, tome $g : Im(f) \to M/Ker(f)$ de modo que $g(f(m)) = m + Ker(f)$. Note que g é um homomorfismo, pois dados $f(m_1), f(m_2) \in Im(f)$,

$$\begin{aligned} g(f(m_1) + f(m_2)) &= g(f(m_1 + m_2)) \\ &= \overline{m_1 + m_2} \\ &= \overline{m_1} + \overline{m_2} \\ &= g(f(m_1)) + g(f(m_2)). \end{aligned}$$

Dado $\alpha \in A$,

$$\begin{aligned} g(\alpha f(m)) &= g(f(\alpha m)) \\ &= \overline{\alpha m} \\ &= \alpha \overline{m} \\ &= \alpha g(f(m)) \end{aligned}$$

e g é um A-homomorfismo. Daí, dado $\overline{m} \in M/Ker(f)$

$$\begin{aligned} g \circ f^*(\overline{m}) &= g(f(m)) \\ &= m + Ker(f) \\ &= \overline{m}, \end{aligned}$$

logo

$$g \circ f : M/Ker(f) \to Im(f) \to M/Ker(f) = I_{M/Ker(f)}$$

e portanto, f^* é um monomorfismo, logo é também um A-isomorfismo. □

Corolário 3.28. *Se $f : M \to N$ é um A-epimorfismo, então $M/Ker(f) \cong N$.*

Demonstração: Como $f : M \to N$ é um A-epimorfismo, então $Im(f) = N$. Pelo teorema anterior segue que

$$M/Ker(f) \cong N.$$

□

Teorema 3.29 (Primeiro Teorema do Isomorfismo)**.** *Sejam M um A-módulo, P e N submódulos, tais que $P \subset N$. Então,*

$$M/N \cong \frac{M/P}{N/P}.$$

Demonstração: Definimos uma função $f : M/P \to M/N$ por

$$f(m + P) = m + N, \forall m \in M.$$

Como $P \subset N$ segue que, se $m_1, m_2 \in M$ são tais que $m_1 + P = m_2 + P$ então $m_1 + N = m_2 + N$, o que permite provar que a definição de f independe do representante.

Também é trivial verificar que f é um epimorfismo; logo, do Corolário 3.28, vem que

$$\frac{M/P}{Ker(f)} \cong M/N$$

Agora, uma classe $m+P$ pertence a $Ker(f)$ se, e somente se, $m+N=N$ o que implica em $m \in N$ e $m+P \in N/P$. Logo, $Ker(f) = N/P$ o que completa a demonstração. $\square$

Teorema 3.30 (Segundo Teorema do Isomorfismo)**.** *Sejam N, P submódulos de um A-módulo M. Então tem-se que*

$$\frac{N}{N \cap P} \cong \frac{N+P}{P}$$

Demonstração: Definimos $f : N \to \frac{N+P}{P}$ por $f(n) = n+P, \forall n \in N$.

Claramente f é um homomorfismo, e para verificar que é sobrejetor basta observar que todo elemento de $\frac{N+P}{P}$ é da forma $(n+p)+P$ com $n \in N, p \in P$. Mas $(n+p)+P = n+P$, logo $f(n) = n+P = (n+p)+P$ e portanto f é epimorfismo.

Temos então que

$$\frac{N}{Ker(f)} \cong \frac{N+P}{P}$$

Finalmente, observemos que dado $n \in N, n \in Ker(f)$ se, e somente se, $n+P = P$, ou seja, $n \in P$, o que implica $n \in N \cap P$, o que completa a demonstração. $\square$

Este resultado é por vezes chamado de **Isomorfismo de Noether**.

4 SEQUÊNCIAS EXATAS

O conceito de sequência exata, que é definido em álgebra homológica, nada mais é que uma forma de linguagem para representar certas relações entre homomorfismos por meio de diagramas. Neste capítulo iremos apresentar este conceito e mostrar alguns resultados relevantes.

Definição 4.1. *Sejam F, G e H três A-módulos, e $f : F \longrightarrow G$ e $g : G \longrightarrow H$ dois A-homomorfismos. Dizemos que o diagrama*

$$F \xrightarrow{f} G \xrightarrow{g} H$$

é uma **sequência de ordem 2** *em G se $Im(f) \subset Ker(g)$.*

Em particular, se $Im(f) = Ker(g)$ o diagrama é chamado de **sequência exata em** *G.*

Note que afirmar $Im(f) \subset Ker(g)$ é equivalente à dizer que $g \circ f = 0$. De fato, se $k \in F$ é tal que $f(k) \in Ker(g)$, então $g(f(k)) = 0$, logo $g \circ f(k) = 0$. Reciprocamente, se para todo $k \in Im(f)$ tem-se que $k = f(x)$, para algum $x \in F$, então $g(k) = g[f(x)] = g \circ f(x) = 0$. Logo, $k \in Ker(g)$, e portanto $Im(f) \subset Ker(g)$.

Definição 4.2. *Seja $\{\dots, M_{i-1}, M_i, M_{i+1}, \dots\}$ uma família, eventualmente infinita, de A-módulos e $\{\dots, f_i : M_i \to M_{i+1}, \dots\}$ uma família de homomorfismos. Dizemos que o diagrama*

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \cdots$$

é uma sequência exata, se é exata em M_i, para todo $i \in I$, isto é, se $Im(f_{i-1}) = Ker(f_i)$, para todo $i \in I$.

Proposição 4.3. *A sequência*

$$0 \longrightarrow E \xrightarrow{f} F$$

é exata, se e somente se, f é um monomorfismo.

Demonstração: De fato, tome $g : 0 \longrightarrow E$ o homomorfismo nulo e $f : E \longrightarrow F$ como um homomorfismo qualquer. Como a sequência é exata, $Im(g) = Ker(f)$, logo $\{0\} = Im(g) = Ker(f)$. Utilizando a Proposição 3.18, como $Ker(f) = 0$, f é um monomorfismo. Reciprocamente, se f for um monomorfismo, novamente pela Proposição 3.18, $Ker(f) = 0$. Como g é o homomorfismo nulo e $Im(g) = 0$, temos que $Im(g) = 0 = Ker(f)$ e a sequência é exata. $\square$

Proposição 4.4. *A sequência*

$$E \xrightarrow{f} F \longrightarrow 0$$

é exata, se e somente se, f é um epimorfismo.

Demonstração: De fato, tome $f : E \longrightarrow F$ como um homomorfismo qualquer e $g : F \longrightarrow 0$ como o homomorfismo nulo. Como a sequência é exata, tem-se que $Im(f) = Ker(g)$, que implica em $Im(f) = F$. Deste modo, pela proposição 3.18 conclui-se que f é um epimorfismo. Por outro lado, se f é um epimorfismo, então novamente pela Proposição 3.18 $Im(f) = F$. Além disso, como g é o homomorfismo nulo, então $F = Ker(g)$, e portanto $Im(f) = F = Ker(g)$ e a sequência é exata. □

Corolário 4.5. *A sequência dada por*

$$0 \longrightarrow E \xrightarrow{f} F \longrightarrow 0$$

é exata, se e somente se, f é um isomorfismo.

Exemplo 4.6. *A sequência $0 \longrightarrow M \longrightarrow 0$ é exata, se e somente se, $M = 0$.*
De fato, defina $f_1 : 0 \longrightarrow M$ e $f_2 : M \longrightarrow 0$. Suponha que $M \neq 0$, logo existe ao menos um elemento $k \in M$ tal que $k \neq 0$. Como f_2 tem como contradomínio o conjunto 0, temos que $f_2(k) = 0$ e portanto $k \in Ker(f_2)$, o que é um absurdo, pois como a sequência é exata, $Ker(f_2) = Im(f_1)$, o que implica em $f_1(0) = k$ e $f_1(0) = 0$. Assim, $M = 0$. Reciprocamente, como $M = 0$, segue trivialmente o resultado.

Exemplo 4.7. *A sequência*

$$0 \longrightarrow 2\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{w} \mathbb{Z}_2 \longrightarrow 0\,,$$

onde $i : 2\mathbb{Z} \longrightarrow \mathbb{Z}$ é a inclusão e $w : \mathbb{Z} \longrightarrow \mathbb{Z}_2$ é a função que associa a cada inteiro sua classe em $\mathbb{Z}_2$ é uma sequência exata.
De fato, note que $Im(i) = 2\mathbb{Z}$, ou seja, o conjunto dos inteiros pares. Além disso, dado $k \in 2\mathbb{Z}$, $w(k) = w(2z) = \overline{0}$, com $z \in \mathbb{Z}$. Portanto, $Im(i) \subset Ker(w)$. Analogamente, dado $k \in Ker(w), k = 2z$, para algum $z \in \mathbb{Z}$. Deste modo, $k \in 2\mathbb{Z}$ e $Im(i) = Ker(w)$ e portanto a sequência é exata em $\mathbb{Z}$.

Exemplo 4.8. *Em geral, se E é um submódulo de um A-módulo F e indicamos por $i : E \longrightarrow F$ a inclusão e por $j : F \longrightarrow F/E$ a projeção canônica, então a sequência a seguir é exata.*

$$0 \longrightarrow E \xrightarrow{i} F \xrightarrow{j} F/E \longrightarrow 0\,.$$

De fato, note primeiro que pela definição de i, $Im(i) = E$. Além disso, dado um elemento $a \in F/E$, $a = f + E$, para algum elemento $f \in F$. Deste modo, dado $k \in E$, é obtido que $j(k) = k + E = E \subset Ker(j)$, ou seja, $E \subset Ker(j)$. Além disso, dado um elemento $k \in Ker(j)$ tem-se que $k \in E$, portanto $Ker(j) \subset E$. Logo a sequência é exata em F.

Exemplo 4.9. *Em certo sentido, dar uma sequência exata do tipo:*

$$0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G \longrightarrow 0$$

onde E, F e G são A-módulos quaisquer, é equivalente a dar uma sequência similar a dada no exemplo anterior.

De fato, chamando $E' = Im(i)$, temos que E' é um submódulo de F isomorfo a E. Ainda, do Corolário 3.28 vem que $G \cong F/Ker(g) = F/Im(f) = F/E'$.

Temos então a sequência exata:

$$0 \longrightarrow E' \xrightarrow{i} F \xrightarrow{j} F/E' \longrightarrow 0$$

onde os módulos são ordenadamente isomorfos aos da sequência original.

Definição 4.10. *Considere agora os seguintes diagramas:*

$$\begin{tikzcd} E \arrow[r, "\varphi"] \arrow[dr, "\theta"'] & F \arrow[d, "\psi"] \\ & G \end{tikzcd} \qquad\qquad \begin{tikzcd} M \arrow[r, "f"] \arrow[d, "h"'] & N \arrow[d, "g"] \\ P \arrow[r, "k"'] & Q \end{tikzcd}$$

O primeiro diagrama é chamado de **diagrama comutativo** *se $\theta = \psi \circ \varphi$. Da mesma forma, o segundo diagrama é chamado comutativo se $g \circ f = k \circ h$.*

Em geral, dizemos que uma família de A-módulos M_i e uma família de homomorfismos h_i forma um **diagrama comutativo** *se para todo par de módulos e todo par de homomorfismos tais que $h_1 : M_1 \longrightarrow M_2$ e $h_2 : M_1 \longrightarrow M_2$, então $h_1 = h_2$.*

O emprego combinado de diagramas comutativos e sequências exatas é frequente em algumas teorias (por exemplo, em topologia algébrica). Para dar uma idéia ao leitor deste tipo de resultados, incluímos a seguinte:

Teorema 4.11. *Se a sequência de homomorfismos de A-módulos abaixo é exata, então as seguintes afirmações são equivalentes:*

$$M \xrightarrow{f} N \xrightarrow{g} R \xrightarrow{h} S$$

a) f é um epimorfismo;

b) $Im(g) = 0$;

c) h é um monomorfismo.

Demonstração:
$(a) \Rightarrow (b)$ Como f é um epimorfismo, então $Im(f) = N$, e pela sequência ser exata tem-se que $Im(f) = Ker(g) = N$, o que implica $g(N) = 0$.
$(b) \Rightarrow (c)$ Se $Im(g) = 0$, pela sequência ser exata $Im(g) = Ker(h) = 0$, logo pela Proposição 3.18, h é um monomorfismo.
$(c) \Rightarrow (a)$ Se h é um monomorfismo, então $Ker(h) = 0$. Logo, como a sequência é exata, $Im(g) = 0$, o que implica $Ker(g) = N = Im(f)$. Portanto f é epimorfismo. $\square$

Corolário 4.12. *Seja*

$$A \xrightarrow{f} B \xrightarrow{\varphi} C \xrightarrow{h} D \xrightarrow{k} E$$

uma sequência exata de homomorfismos de A-módulos. Nestas condições, f será um epimorfismo e k um monomorfismo se, e somente se, C é o módulo nulo.

Demonstração: De fato, se $C = 0$, então $h(C) = h(0) = 0$ e portanto

$$C = Ker(h) = 0.$$

Logo, pela Proposição 3.18, h é um monomorfismo. Além disso, como a sequência é exata,

$$Ker(h) = Im(\varphi) = C$$

e utilizando novamente a Proposição 3.18, concluímos que φ é um epimorfismo.

Por outro lado, se h é um monomorfismo e φ é epimorfismo, então $Ker(h) = 0$ e $Im(\varphi) = C$. Como a sequência é exata por hipótese, tem-se que

$$0 = Ker(h) = Im(\varphi) = C$$

e portanto C é o módulo nulo. $\square$

Corolário 4.13. *Se a sequência de homomorfismos de A-módulos*

$$0 \xrightarrow{f} C \xrightarrow{g} 0$$

é exata, então C é o módulo nulo.

Demonstração: De fato, note que $f(0) = Im(f) = 0$. Além disso, $Im(g) \subset \{0\}$, o que implica $Im(g) = 0$, logo $Ker(g) = C$. Deste modo, como a sequência é exata, $Im(f) = Ker(g)$, o que resulta em

$$0 = Im(f) = Ker(g) = C,$$

e portanto $C = 0$. $\square$

Corolário 4.14. *Se a sequência de homomorfismos de A-módulos abaixo é exata, então as seguintes afirmações são equivalentes:*

$$A \xrightarrow{d} B \xrightarrow{f} C \xrightarrow{g} D \xrightarrow{h} E \xrightarrow{k} F$$

a) g é um isomorfismo;

b) f e h são homomorfismos nulos;

c) d é um epimorfismo e k é um monomorfismo.

Demonstração:

$(a) \Rightarrow (b)$ Se g é um isomorfismo, então $Ker(g) = 0$, pois é monomorfismo, e $Im(g) = D$, pois é também epimorfismo. Como a sequência é exata, $Ker(g) = Im(f)$ e $Im(g) = Ker(h)$, logo $Im(f) = 0$ e $Ker(h) = D$, ou seja, ambos são homomorfismos nulos.
$(b) \Rightarrow (c)$ Como f e h são homomorfismos nulos, então $Ker(f) = B$ e $Im(h) = 0$. Desta forma, utilizando o fato da sequência ser exata, $Ker(k) = 0$ e $Im(d) = B$ e portanto, pela Proposição 3.18 k é monomorfismo e d é epimorfismo.
$(c) \Rightarrow (a)$ Se d é um epimorfismo, então $Im(d) = B = Ker(f)$. Logo $f(B) = 0 = Ker(g)$, o que implica g ser um monomorfismo. Por outro lado, como k é monomorfismo, $Ker(k) = 0 = Im(h)$. Logo $Ker(h) = D = Im(g)$ e g é um epimorfismo. Portanto, g é um isomorfismo. $\square$

Proposição 4.15 (Lema dos Três). *Seja*

$$\begin{tikzcd} & M' \arrow[r, "f'"] \arrow[d, "\varphi'"] & M \arrow[r, "f"] \arrow[d, "\varphi"] & M'' \arrow[d, "\varphi''"] \\ 0 \arrow[r] & N' \arrow[r, "g'"] & N \arrow[r, "g"] & N'' \end{tikzcd}$$

um diagrama comutativo, onde as linhas são sequências exatas de homomorfismos de A-módulos. Se φ' e φ'' são monomorfismos, então φ é um monomorfismo.

Demonstração: De fato, seja $x \in M$ tal que $\varphi(x) = 0$. Assim,

$$g \circ \varphi(x) = g(0) = 0,$$

e pela comutatividade do diagrama,

$$g \circ \varphi(x) = \varphi'' \circ f(x) = 0.$$

Como φ'' é monomorfismo, então $f(x) = 0$. Deste modo, $x \in Ker(f)$ e mais, como a sequência é exata, existe $y \in M'$ tal que $f'(y) = x$, pois $Ker(f) = Im(f')$. Note agora que

$$\varphi \circ f'(y) = \varphi(x) = 0,$$

e novamente pela comutatividade do diagrama

$$\varphi \circ f'(y) = g' \circ \varphi'(y) = 0,$$

que implica em

$$g'(\varphi'(y)) = 0.$$

Utilizando a Proposição 4.3, é possível afirmar que g' é monomorfismo, logo $\varphi'(y) = 0$. Além disso, φ' também é monomorfismo, de onde concluímos que $y = 0$. Logo,

$$f'(y) = x = 0,$$

portanto $Ker(\varphi) = 0$ e, pela Proposição 3.18, φ é um monomorfismo. $\square$

Teorema 4.16 (Lema dos Quatro). *Seja*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r, "h"] \arrow[d, "\gamma"] & D \arrow[d, "\delta"] \\ A' \arrow[r, "\alpha'"] & B' \arrow[r, "g'"] & C' \arrow[r, "h'"] & D' \end{tikzcd}$$

um diagrama de homomorfismos de A-módulos onde as duas filas são sequências exatas, os três quadrados são comutativos, α é um epimorfismo e δ é um monomorfismo. Sob estas condições, são válidas as seguintes igualdades:

a) $Im(\beta) = g'^{-1}[Im(\gamma)]$

b) $Ker(\gamma) = g[Ker(\beta)]$.

Demonstração:

a) De fato, seja $b' \in Im(\beta)$, logo existe $b \in B$ tal que $\beta(b) = b'$. Pela comutatividade,

$$g'(b') = g' \circ \beta(b) = \gamma \circ g(b) \in Im(\gamma),$$

aplicando g'^{-1} em toda a igualdade, obtém-se

$$g'^{-1} \circ g'(b') = g'^{-1}[g' \circ \beta(b)] = g'^{-1}[\gamma \circ g(b)] \in g'^{-1}[Im(\gamma)],$$

por outro lado

$$g'^{-1} \circ g'(b') = g'^{-1} \circ g' \circ \beta(b) = Idn \circ \beta(b) = \beta(b) \in Im(\beta),$$

de onde concluí-se que $Im(\beta) \subset g'^{-1}[Im(\gamma)]$.

Agora tome $b' \in g'^{-1}[Im(\gamma)]$, logo existe $c' \in Im(\gamma)$ tal que $g'(b') = c'$. Desta forma, como $c' \in Im(\gamma)$, existe $c \in C$ tal que $\gamma(c) = c'$ e, como a sequência é exata, $c' \in Im(g') = Ker(h')$ e portanto $h'(c') = 0$. Assim, pela comutatividade

$$h' \circ \gamma(c) = \delta \circ h(c) = 0,$$

o que implica $h(c) \in Ker(\delta)$. Como δ é monomorfismo, $Ker(\delta) = 0$ e portanto $h(c) = 0$, logo $c \in Ker(h)$. Como por hipótese a fila superior é exata, $Ker(h) = Im(g)$, o que garante existir $b \in B$ de modo que $g(b) = c$ e consequentemente

$$\gamma \circ g(b) = \gamma(c) = c'.$$

Novamente pela comutatividade

$$\gamma \circ g(b) = g' \circ \beta(b),$$

aplicando g'^{-1} em ambos os lados da igualdade obtém-se

$$g'^{-1}[\gamma \circ g(b)] = g' \circ \beta(b) \in Im(\beta),$$

por outro lado

$$g'^{-1}[\gamma \circ g(b)] = g'^{-1}[\gamma(c)] \in g'^{-1}[Im(\gamma)]$$

o que mostra que $g'^{-1}[Im(\gamma)] \subset Im(\beta)$, e portanto $g'^{-1}[Im(\gamma)] = Im(\beta)$.

b) De fato, tome $c \in Ker(\gamma)$. Deste modo, $\gamma(c) = 0$ e portanto $h' \circ \gamma(c) = h'(0) = 0$. Logo, pela comutatividadedo quadrado direito

$$h' \circ \gamma(c) = \delta \circ h(c) = 0.$$

Como δ é monomorfismo, pela proposição 3.18 $Ker(\delta) = 0$, o que mostra que $h(c) = 0$, e portanto $c \in Ker(h)$. Além disso, como a fila superior é uma sequência exata, $c \in Ker(h) = Im(g)$, logo existe $b \in B$ de modo que $g(b) = c$ e, além disso

$$\gamma \circ g(b) = \gamma(c) = 0.$$

Pela comutatividade,

$$g' \circ \beta(b) = \gamma \circ g(b) = 0,$$

o que implica $\beta(b) \in Ker(g') = Im(f')$, pois a fila inferior é uma sequência exata. Logo, existe $a' \in A'$ tal que $f'(a') = \beta(b)$ e pela sobrejetividade de α, existe $a \in A$ tal que $\alpha(a) = a'$ e $\beta(b) = f' \circ \alpha(a)$. Assim, pela comutatividade, tem-se que

$$f' \circ \alpha(a) = \beta \circ f(a) = \beta(b).$$

Como $b \in B$ e $f(a) \in B$ e B é um módulo, então $b - f(a) \in B$. Logo,

$$\beta[b - f(a)] = \beta(b) - \beta(f(a)) = \beta(b) - \beta(b) = 0,$$

o que implica que $b - f(a) \in Ker(\beta)$. Por outro lado, como a fila superior é uma sequência exata,

$$g[b - f(a)] = g(b) - g(f(a)) = c - 0 = c,$$

ou seja, $c \in g[Ker(\beta)]$ e portanto $Ker(\gamma) \subset g[Ker(\beta)]$.

Por outro lado, dado $c \in g[Ker(\beta)]$, existe $b \in Ker(\beta)$ tal que $g(b) = c$, e pela comutatividade do diagrama

$$\gamma(c) = \gamma \circ g(b) = g' \circ \beta(b) = g'(0) = 0$$

que implica $\gamma(c) = 0$ e $c \in Ker(\gamma)$. Por fim, tem-se $g[Ker(\beta)] \subset Ker(\gamma)$, e portanto $g[Ker(\beta)] = Ker(\gamma)$, o que conclui a demonstração. $\square$

Corolário 4.17. *Seja*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r, "h"] \arrow[d, "\gamma"] & D \arrow[d, "\delta"] \\ A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r, "h'"] & D' \end{tikzcd}$$

um diagrama de homomorfismos de A-módulos onde as duas filas são sequências exatas, os três quadrados são comutativos, α é um epimorfismo e δ é um monomorfismo. Se γ é um epimorfismo, então β também é. Da mesma forma, se β é um monomorfismo, então γ também é.

Demonstração: De fato, $Im(\beta) \subset B'$, basta portanto mostrar que $B' \subset Im(\beta)$. Tome $b' \in B'$, logo existe $c' \in C'$ tal que $c' = g'(b')$, e por sua vez existe $c \in C$ tal que $\gamma(c) = c'$, pois γ é um epimorfismo. Desta forma, como a fila inferior é uma sequência exata e $c' \in Im(g') = Ker(h')$, então

$$h' \circ \gamma(c) = h'(c') = 0.$$

Utilizando a comutatividade do quadrado direito, tem-se que

$$h' \circ \gamma(c) = \delta \circ h(c) = 0,$$

e como δ é monomorfismo, $\delta \circ h(c) = 0$ implica $h(c) = 0$. Assim, pode-se afirmar que $c \in Ker(h)$, e como a fila superior é uma sequência exata, $c \in Im(g)$ e portanto existe $b \in B$ tal que $g(b) = c$ e além disso $\gamma \circ g(b) = c'$. Utilizando desta vez a comutatividade do quadrado central,

$$c' = \gamma \circ g(b) = g' \circ \beta(b)$$

que implica em $g'(b') = c' = g'[\beta(b)]$. Desta forma,

$$0 = c' - c' = g'(b') - g'[\beta(b)] = g'[b' - \beta(b)]$$

que implica em $b' - \beta(b) \in Ker(g')$. Tome agora $k \in Ker(g')$ de modo que $k = b' - \beta(b)$. Com efeito, como a fila inferior é uma sequência exata, $k \in Ker(g') = Im(f')$ e com isso existe $a' \in A'$ tal que $f'(a') = k$. Desta forma, como α é um epimorfismo, existe $a \in A$ tal que $\alpha(a) = a'$ e $f' \circ \alpha(a) = k$. Pela comutatividade do primeiro quadrado

$$f' \circ \alpha(a) = \beta \circ f(a) = k$$

que implica

$$\beta[f(a)] = [b' - \beta(b)] \in Im(\beta).$$

Portanto, como $\beta(b) \in Im(\beta)$ e $b' - \beta(b) \in Im(\beta)$, e além disso $Im(\beta)$ é um submódulo,

$$[b' - \beta(b)] + \beta(b) = b' \in Im(\beta).$$

Portanto $B' \subset Im(\beta)$, o que implica em $B' = Im(\beta)$ e resulta em β ser um epimorfismo, o que concluí a primeira parte.

Por outro lado, se β é um monomorfismo, então pela Proposição 3.18, $ker(\beta) = 0$. Utilizando o Teorema 4.16

$$Ker(\gamma) = g[Ker(\beta)] = g(0) = 0$$

e novamente pela Proposição 3.18 conclui-se que γ é um monomorfismo, o que finaliza a demonstração. □

Corolário 4.18 (Lema dos Cinco). *Seja*

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r, "h"] \arrow[d, "\gamma"] & D \arrow[r, "k"] \arrow[d, "\delta"] & E \arrow[d, "\epsilon"] \\
A' \arrow[r, "\alpha'"] & B' \arrow[r, "g'"] & C' \arrow[r, "h'"] & D' \arrow[r, "k'"] & E'
\end{tikzcd}$$

onde as duas filas são sequências exatas e os quatro quadrados são comutativos. Se α, β, δ e ϵ forem isomorfismos, então γ também será.

Demonstração: De fato, como β é um isomorfismo, é também um monomorfismo. Logo, pelo Corolário 4.17, γ é um monomorfismo. Analogamente, como δ é um isomorfismo, é também epimorfismo, e novamente pelo Corolário 4.17 γ é um epimorfismo. Deste modo, como γ é monomorfismo e epimorfismo simultaneamente, é portanto um isomorfismo, o que conclui a demonstração. □

Corolário 4.19 (Lema dos Cinco Curto). *Seja*

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0
\end{tikzcd}$$

um diagrama de homomorfismos de A-módulos onde as duas filas são sequências exatas e ambos os quadrados são comutativos. Sob estas condições, são válidas as seguintes afirmações:

a) Se α e γ são monomorfismos, então β também é.

b) Se α e γ são epimorfismos, então β também é.

Demonstração:

(a) Defina $h : 0 \longrightarrow 0$ como o homomorfismo nulo à direita do diagrama e denote por k_2, k_4, respectivamente, os homomorfismos $k_2 : C \longrightarrow 0$ e $k_4 : C' \longrightarrow 0$. Com efeito, note que $Ker(h) \subset \{0\}$, logo $Ker(h) = 0$, e pela Proposição 3.18, h é um monomorfismo. Além disso, dado $c \in C$

$$h \circ k_2(c) = h(0) = 0 = k_4 \circ \gamma(c),$$

o que implica o quadrado formado à direita do diagrama ser comutativo. Deste modo, como γ é um epimorfismo, pelo Corolário 4.17, β também é.

(b) Defina $j : 0 \longrightarrow 0$ como o homomorfismo nulo à esquerda do diagrama e denote por k_1, k_3, respectivamente, os homomorfismos $k_1 : 0 \longrightarrow A$ e $k_3 : 0 \longrightarrow A'$. De fato, note que $Im(j) \subset \{0\}$, logo $Im(j) = 0$, e pela Proposição 3.18, j é um epimorfismo. Além disso, dado $z \in 0$

$$\alpha \circ k_1(z) = \alpha(0) = 0 = k_3 \circ j(z),$$

e portanto o quadrado formado à esquerda é comutativo. Desta forma, como α é um monomorfismo, pelo Corolário 4.17, β também é. $\square$

5 CONSIDERAÇÕES FINAIS

Para finalizar este trabalho, consideramos que este projeto sobre Módulos e Sequências Exatas é uma alternativa para alunos que pretendem iniciar seus estudos em áreas da matemática não encontradas no curso de Licenciatura em Matemática da UTFPR. Aqui o aluno foi apresentado a diversas definições específicas da álgebra Homológica, e também teve acesso a resultados conhecidos, todos devidamente demonstrados. Ressalto também que, caso o leitor tenha interesse em resultados mais avançados, consultar as referências podem ser de grande ajuda. Como perspectiva, esperamos que o presente trabalho seja bem utilizado por estudantes curiosos de matemática, que são o público alvo deste projeto, para satisfazer suas necessidades de aprimoramento e também os motivar a sempre buscar conhecimento.

REFERÊNCIAS

DOMINGUES, Hygino H; IEZZI, Gelson. **Álgebra moderna.** 2018. Citado 2 vezes nas páginas 15 e 17.

HU, Sze Tsen. **Introduction to Homological Algebra**. 1. ed. Los Angeles: [s.n.], 1968. Citado 2 vezes nas páginas 15 e 29.

COELHO, Flávio Ulhoa; LOURENÇO, Mary Lílian. **Um curso de álgebra linear.** Ed usp. Brasil, 2005. Citado na página 29.

MILIES, Francisco Cesar Polcino. **Anéis e Módulos**. 1. ed. São Paulo: [s.n.], 1972. Citado 3 vezes nas páginas 15, 17 e 29.