Universidade Federal do Espírito Santo

Centro Universitário Norte do Espírito Santo

Colegiado do Curso de Licenciatura em Matemática

Filipe de Oliveira Barbosa

MÓDULOS LIVRES: UM TÓPICO EM TEORIA DE MÓDULOS

São Mateus

2019

Filipe de Oliveira Barbosa

MÓDULOS LIVRES: UM TÓPICO EM TEORIA DE MÓDULOS

Trabalho submetido ao Colegiado do Curso de Licenciatura em Matemática da UFES (Campus São Mateus), como requisito parcial para a obtenção do grau de Licenciado em Matemática.

Orientador: Prof. Ms. Michel Guimarães Coswosck.

São Mateus

2019

Filipe de Oliveira Barbosa

MÓDULOS LIVRES: UM TÓPICO EM TEORIA DE MÓDULOS

Trabalho submetido ao Colegiado do Curso de Licenciatura em Matemática da UFES (Campus São Mateus), como requisito parcial para a obtenção do grau de Licenciado em Matemática.

Orientador: Prof. Ms. Michel Guimarães Coswosck.

Aprovada em 19 de dezembro de 2019.

Comissão Examinadora

Prof. Ms. Michel Guimarães Coswosck
Universidade Federal do Espírito Santo
Orientador

Prof. Dr. Leandro Domingues
Universidade Federal do Espírito Santo

Prof. Dr. Lúcio Souza Fassarella
Universidade Federal do Espírito Santo

Agradecimentos

À toda a minha família, especialmente à minha mãe Antônia e à minha namorada Gizeli, pelo carinho, compreensão e apoio em tudo que faço.

Ao meu orientador, Prof. Michel Guimarães Coswosck, por ter me auxiliado na produção deste material por meio de aulas, orientações, sugestões bibliográficas e discussões.

Aos meus amigos e colegas do curso de Licenciatura em Matemática, Luan, Ana Paula, Caique, Naidhila, Rômulo, Diogo e Vitor, por todos os momentos compartilhados e todo apoio que me deram no decorrer do curso.

Aos professores Leandro Domingues e Lúcio Souza Fassarella, por aceitarem o convite para participarem da banca e por contribuírem para meu trabalho.

A todos os docentes do CEUNES que contribuíram para minha formação, em especial aos professores: Moysés Gonçalves Siqueira Filho, Andressa Cesana, Leandro Domingues, Genilson Ferreira da Silva e Michel Guimarães Coswosck. Vocês são exemplos de professores a serem seguidos.

A todos que de alguma forma contribuíram para a minha formação.

Resumo

Apresenta a Teoria de Módulos, com ênfase em Módulos Livres. No primeiro capítulo são apresentadas as definições, propriedades e os resultados básicos sobre Módulos, Submódulos, Módulos Quocientes, Homomorfismos de Módulos, Produtos, Coprodutos, Somas Diretas e Sequências Exatas. Enuncia e prova teoremas clássicos como os Primeiro, Segundo e Terceiro teoremas do Isomorfismo e o Teorema da Correspodência. Além disso, exemplifica casos atípicos quando comparados com a teoria de espaços vetoriais, como a existência de módulos finitamente gerados que possuem submódulos que não são finitamente gerados e módulos que não são finitamente gerados cujos submódulos próprios são todos finitamente gerados. Finaliza mostrando a existência dos Módulos Livres, desenvolvendo exemplos e teoremas básicos sobre o assunto.

Palavras-chave: Teoria de Módulos. Módulos Livres.

Abstract

In this work we study about Module Theory, with emphasis on Free Modules. The first chapter presents the definitions, properties and basic results on Modules, Submodules, Quotient Modules, Module Homomorphisms, Products, Coproducts, Direct Sums and Exact Sequences. We enunciate and prove classical theorems such as the First, Second, and Third Isomorphism Theorems and the Matching Theorem. In addition, we exemplify atypical cases when compared to vector space theory, such as the existence of finitely generated modules that have submodules that are not finitely generated and modules that are not finitely generated whose submodules are all finitely generated. We conclude by showing the existence of Free Modules, developing examples and basic theorems on the subject.

Keywords: Module Theory, Free Modules.

Sumário

Introdução

Até o início do século XIX, as preocupações dos matemáticos, que estudavam Álgebra, estavam voltadas para o estudo das operações entre números reais e para a resolução de equações algébricas. Isso mudou a partir de 1815, quando um grupo de matemáticos da Universidade de Cambridge, criou a Analytical Society, cujo objetivo era reformular o ensino do cálculo. Como consequência dos estudos desenvolvidos por esse grupo, ocorreu uma reformulação do estudo da Álgebra, repensando todos os seus fundamentos baseados em axiomas. Dentre os vários matemáticos que faziam parte desse grupo estavam Charles Babbage (1792-1871), George Peacock (1791-1858) e John Herschel (1792-1878). Em 1830, Peacock publicou uma obra chamada Treatise on Álgebra, na qual ele já apresentava todo o desenvolvimento da Álgebra por meio de postulados. Esse foi o marco inicial para o seguimento da Álgebra mais abstrata que conhecemos nos dias atuais (MILIES, 2004).

No século XIX, com o desenvolvimento da Álgebra, foram criadas algumas estruturas algébricas, como os Anéis, Grupos, Corpos entre outras, que hoje possuem grande importância nessa área da matemática. Dentre essas estruturas estão os Espaços Vetoriais, que surgiram em 1888, por meio do texto intitulado *Calcolo Geometrico* do matemático Giuseppe Peano (1858-1952). Nessa obra foi dada a primeira definição axiomática sobre o assunto, porém a teoria de Espaços Vetoriais só se desenvolveu de fato, a partir de 1920 (DORIER, 1995). A definição de um espaço vetorial exige que o conjunto dos escalares seja um corpo, com a intenção de criar uma generalização dos espaços vetoriais, ou seja, desenvolver uma estrutura algébrica em que o conjunto dos escalares seja apenas um anel, Richard Dedekind (1831-1916), em 1882, por meio de um artigo escrito junto com Heinrich Weber (1842-1913) criou o conceito de Módulos (FERREIRÓS, 2007). O objetivo inicial para o desenvolvimento da Teoria de Módulos foi verificar se os resultados apresentados para Espaços Vetoriais também se preservariam para ela.

Neste trabalho discutiremos sobre Módulos Livres, conteúdo que integra a Teoria de Módulos. No primeiro capítulo, apresentaremos com detalhes toda a parte introdutória da teoria, servindo como base para os resultados desenvolvidos no capítulo seguinte. No segundo capítulo, abordaremos sobre os módulos que admitem uma base, chamados de Módulos Livres. A ideia de desenvolver o trabalho com esse tema surgiu no primeiro

semestre do ano de 2018, quando cursei a disciplina de Álgebra 2, ministrada pelo professor Michel Guimarães Coswosck, docente do curso de Licenciatura em Matemática, do Centro Universitário do Norte do Espírito Santo. Fiquei muito admirado por esta disciplina e, no decorrer do semestre, surgiu o convite do próprio professor para estudar, mais profundamente, Álgebra. Devido a isso, resolvi desenvolver este trabalho junto a ele, voltado para a Teoria de Módulos, já que seria um conteúdo desafiador para ambos.

Percebemos que existem poucos trabalhos relacionados a este tema em língua portuguesa, e além disso, a maioria deles estão voltados para cursos de mestrado. Por esse motivo, existe uma dificuldade em encontrar um material sobre o assunto que seja acessível para alunos de graduação em matemática. O objetivo geral deste trabalho foi desenvolver um texto, em língua portuguesa, sobre o conteúdo de Módulos Livres.

1 Módulos

Discutiremos no decorrer das seções deste capítulo os conceitos de Módulo, Submódulo, Módulo Quociente, Homomorfismo de Módulo, Produto, Coproduto, Soma Direta e Sequências Exatas. Em cada uma delas, apresentaremos resultados básicos que serão úteis no decorrer do texto. Além disso, exemplificaremos alguns resultados conhecidos na teoria de Espaços Vetoriais que não se aplicam à teoria de Módulos.

No decorrer deste trabalho, usaremos a expressão anel, subentendendo que todos os anéis considerados possuem o elemento unidade 1_A. Deixaremos de explicitar as operações dos anéis, escrevendo simplesmente A para denotar $(A, +, \cdot)$. Utilizaremos os símbolos (a, b) e $[a, b]$, com a, $b \in \mathbb{Z}$, para indicar o máximo divisor comum e o mínimo múltiplo comum positivos de a e b, respectivamente.

Definição 1.0.1. *Sejam A um anel e M um conjunto não vazio. M é dito um A-módulo à esquerda, se M munido de uma operação, que indicaremos por $+$, é um grupo abeliano e está definida uma lei de composição externa*

$$\begin{aligned} A \times M &\longrightarrow M \\ (a, m) &\longmapsto a \cdot m \end{aligned}$$

que satisfaz os seguintes axiomas:

I) (Associatividade) $\alpha \cdot (\beta \cdot m) = (\alpha\beta) \cdot m$; para todo $\alpha, \beta \in A$ e $m \in M$;

II) (Distributividade com relação às escalares) $\alpha \cdot (m + n) = \alpha \cdot m + \alpha \cdot n$; para todo $\alpha \in A$ e $m, n \in M$;

III) (Distributividade com relação aos elemtentos do A-módulo) $(\alpha+\beta)\cdot m = \alpha\cdot m+\beta\cdot m$; para todo $\alpha, \beta \in A$ e $m \in M$;

IV) (Elemento Neutro) $1_A \cdot m = m$; *para todo* $m \in M$.

Definição 1.0.2. *Sejam A um anel e M um conjunto não vazio. M é dito um A-módulo à direita, se M munido de uma operação, que indicaremos por $+$, é um grupo abeliano e está definida uma lei de composição externa*

$$\begin{aligned} M \times A &\longrightarrow M \\ (m, a) &\longmapsto m \cdot a \end{aligned}$$

que satisfaz os seguintes axiomas:

I) $(m \cdot \beta) \cdot \alpha = m \cdot (\beta\alpha)$; *para todo* $\alpha, \beta \in A$ *e* $m \in M$;

II) $(m + n) \cdot \alpha = m \cdot \alpha + n \cdot \alpha$; *para todo* $\alpha \in A$ *e* $m, n \in M$;

III) $m \cdot (\alpha + \beta) = m \cdot \alpha + m \cdot \beta$; *para todo* $\alpha, \beta \in A$ *e* $m \in M$;

IV) $m \cdot 1_A = m$; *para todo* $m \in M$.

Todos os resultados apresentados para os A-módulos à esquerda também serão válidos para os à direita e vice-versa. Para comprovar tal afirmação, dado um anel A qualquer, definiremos o anel oposto de A.

Definição 1.0.3. *Seja $(A, +, \cdot)$ um anel. Denotaremos por A^{op}, o conjunto $(A, +, \bullet)$, onde a operação de multiplicação $\bullet$ é dada por*

$$\begin{aligned} \bullet : A \times A &\longrightarrow A \\ (x, y) &\longmapsto x \bullet y = y \cdot x. \end{aligned}$$

É de fácil verificação que $(A, +, \bullet)$ é um anel. Chamaremos A^{op} de anel oposto de A.

Proposição 1.0.4. *Seja M um A-módulo à esquerda. A aplicação*

$$\begin{aligned} M \times A^{op} &\longrightarrow M \\ (m, a) &\longmapsto m \odot a = a \cdot m \end{aligned}$$

mune M de um estrutura de A^{op}-módulo à direita.

Demonstração. De fato, dados $a, b \in A^{op}$ e $m, n \in M$ quaisquer, tem-se que

I)

$$\begin{aligned}(m \odot a) \odot b &= (a \cdot m) \odot b \\ &= b \cdot (a \cdot m) \\ &= (b \cdot a) \cdot m \\ &= m \odot (b \cdot a) \\ &= m \odot (a \bullet b)\end{aligned}$$

II)

$$\begin{aligned}m \odot (a + b) &= (a + b) \cdot m \\ &= a \cdot m + b \cdot m \\ &= m \odot a + m \odot b\end{aligned}$$

III)

$$\begin{aligned}(m + n) \odot a &= a \cdot (m + n) \\ &= a \cdot m + a \cdot n \\ &= m \odot a + n \odot a\end{aligned}$$

IV)

$$\begin{aligned}m \odot 1_A &= 1_A \cdot m \\ &= m\end{aligned}$$

Portanto, M é um A^{op}-módulo à direita. □

Proposição 1.0.5. *Seja M um A-módulo à esquerda. Então:*

I) $0_A \cdot m = 0_M$, para todo $m \in M$.

Demonstração. De fato,

$$\begin{aligned}0_A \cdot m = (0_A + 0_A) \cdot m = 0_A \cdot m + 0_A \cdot m \\ \Rightarrow 0_A \cdot m + 0_A \cdot m = 0_A \cdot m \\ \Rightarrow 0_A \cdot m = 0_M.\end{aligned}$$

□

II) $\alpha \cdot 0_M = 0_M$, *para todo* $\alpha \in A$.

Demonstração. Com efeito,

$$\begin{aligned} \alpha \cdot 0_M = \alpha \cdot (0_M + 0_M) = \alpha \cdot 0_M + \alpha \cdot 0_M \\ \Rightarrow \alpha \cdot 0_M + \alpha \cdot 0_M = \alpha \cdot 0_M \\ \Rightarrow \alpha \cdot 0_M = 0_M. \end{aligned}$$

□

III) $(-a) \cdot m = -(a \cdot m) = a \cdot (-m)$, *para todo* $a \in A$ *e* $m \in M$.

Demonstração. De fato,

$$\begin{aligned} (-a) \cdot m + a \cdot m = [(-a) + a] \cdot m = 0_A \cdot m = 0_M \\ \Rightarrow (-a) \cdot m = -(a \cdot m). \end{aligned}$$

Analogamente,

$$\begin{aligned} a \cdot (-m) + a \cdot m = a \cdot [(-m) + m] = a \cdot 0_M = 0_M \\ \Rightarrow a \cdot (-m) = -(a \cdot m). \end{aligned}$$

Portanto,

$$(-a) \cdot m = -(a \cdot m) = a \cdot (-m).$$

□

IV) $(a - b) \cdot m = a \cdot m - b \cdot m$, *para todo* $a, b \in A$ *e* $m \in M$.

Demonstração. Com efeito,

$$\begin{aligned} (a - b) \cdot m &= [a + (-b)] \cdot m \\ &= a \cdot m + (-b) \cdot m \\ &= a \cdot m + [-(b \cdot m)] \\ &= a \cdot m - b \cdot m. \end{aligned}$$

□

V) $a \cdot (m - n) = a \cdot m - b \cdot n$, *para todo* $a \in A$ *e* $m, n \in M$.

Demonstração. De fato,

$$\begin{aligned} a \cdot (m-n) &= a \cdot [m + (-n)] \\ &= a \cdot m + a \cdot (-n) \\ &= a \cdot m + [-(a \cdot n)] \\ &= a \cdot m - a \cdot n. \end{aligned}$$

□

Exemplo 1.0.6. *Seja V um espaço vetorial sobre um corpo K. Então V possui uma estrutura de K-módulo à esquerda e à direita, cuja lei de composição externa $\cdot : K \times V \longrightarrow V$ dada por $\alpha \cdot v = v \cdot \alpha$, onde $\cdot$ é a operação de multiplicação por escalar do espaço vetorial V.*

Exemplo 1.0.7. *Seja $(G, +)$ um grupo abeliano. Podemos introduzir em G uma estrutura de $\mathbb{Z}$-módulo à esquerda, utilizando a lei de composição externa $\cdot : \mathbb{Z} \times G \longrightarrow G$ definida indutivamente por*

$$(n, g) \longmapsto n \cdot g = \begin{cases} (n-1) \cdot g + g, & se \quad n \geq 1; \\ 0_G, & se \quad n = 0; \\ -(-n) \cdot g, & se \quad n < 0. \end{cases}$$

Com efeito, dados $m, n \in \mathbb{Z}$ e $g, g_1, g_2 \in G$ as seguintes propriedades são válidas:

I) $m \cdot (n \cdot g) = (m \cdot n) \cdot g$;

II) $m \cdot (g_1 + g_2) = m \cdot g_1 + m \cdot g_2$;

III) $(m + n) \cdot g = m \cdot g + n \cdot g$;

IV) $1 \cdot g = g$.

Portanto, G é um $\mathbb{Z}$-módulo à esquerda.

Exemplo 1.0.8. *Sejam $(G, +)$ um grupo abeliano e*

$$End(G) = \{f : G \to G; \quad f \text{ é um homomorfismo de grupos}\}.$$

Introduziremos uma estrutura de anel em $End(G)$ dada por:

$$\begin{aligned} (f+g)(x) &= f(x) + g(x), \quad \text{para todo } x \in G; \\ (f \cdot g)(x) &= f(g(x)), \quad \text{para todo } x \in G. \end{aligned}$$

É de fácil verificação que $(End(G), +, \cdot)$ é um anel. Defina a lei de composição externa dada por

$$\begin{aligned} \odot : End(G) \times G &\longrightarrow G \\ (f, x) &\longmapsto f \odot x = f(x). \end{aligned}$$

Afirmação: *G é um $End(G)$-módulo à esquerda.*

De fato, dados $f, g \in End(G)$ e $x, y \in G$ quaisquer, tem-se:

I)

$$\begin{aligned} f \odot (g \odot x) &= f \odot g(x) \\ &= f(g(x)) \\ &= (f \cdot g)(x) \\ &= (f \cdot g) \odot x \end{aligned}$$

II)

$$\begin{aligned} f \odot (x + y) &= f(x + y) \\ &= f(x) + f(y) \\ &= f \odot x + f \odot y \end{aligned}$$

III)

$$\begin{aligned} (f + g) \odot x &= (f + g)(x) \\ &= f(x) + g(x) \\ &= f \odot x + g \odot x \end{aligned}$$

IV)

$$\begin{aligned} Id_G \odot x &= Id_G(x) \\ &= x. \end{aligned}$$

Portanto, G é um $End(G)$-módulo à esquerda.

Exemplo 1.0.9. *Sejam V um espaço vetorial sobre K e $T : V \to V$ um operador linear fixo. Considere a operação $\odot : K[x] \times V \to V$ dada por $f \odot v = f(T)(v)$. Deste modo, V*

é um $K[x]$-módulo à esquerda.

Com efeito, dados f, $g \in K[x]$ e u, $v \in V$ quaisquer, tem-se

I)

$$\begin{aligned} f \odot (g \odot v) &= f \odot (g(T)(v)) \\ &= f(T)(g(T)(v)) \\ &= (f(T)g(T))(v) \\ &= (fg)(T)(v) = (fg) \odot (v). \end{aligned}$$

II)

$$\begin{aligned} f \odot (u + v) &= f(T)(u + v) \\ &= f(T)(u) + f(T)(v) \\ &= f \odot u + f \odot v. \end{aligned}$$

III)

$$\begin{aligned} (f + g) \odot u &= (f + g)(T)(u) \\ &= (f(T) + g(T))(u) \\ &= f(T)(u) + g(T)(u) \\ &= f \odot u + g \odot u. \end{aligned}$$

IV)

$$\begin{aligned} 1_K \odot u &= Id_V(u) \\ &= u. \end{aligned}$$

Portanto, V é um $K[x]$-módulo à esquerda.

Proposição 1.0.10. *Se M é um ideal à esquerda do anel comutativo com elemento unidade A, então M é um A-módulo à esquerda.*

Demonstração. De fato, basta considerar a multiplicação induzida do A como lei de composição externa. □

Corolário 1.0.11. *Todo anel A pode ser considerado um A-módulo à esquerda (ou à direita). Para indicar que A é um A-módulo à esquerda, utilizaremos o símbolo A^A.*

Seja A um anel. Em determinados casos, é possível converter um A-módulo à esquerda em um A-módulo à direita, invertendendo o lado das ações das escalares (Exemplo 1.0.12), mas nem sempre isso é possível (Exemplo 1.0.13).

Exemplo 1.0.12. *Seja V um $K[x]$-módulo à esquerda conforme o Exemplo 1.0.9. Defina a lei de composição externa $\otimes : V \times K[x] \to V$ dada por $v \otimes f = f \odot v = f(T)(v)$.*

Afirmação: *V com essa lei de composição externa é um $K[x]$-módulo à direita. Com efeito, para quaisquer f, $g \in K[x]$ e u, $v \in V$ tem-se*

I)

$$\begin{aligned}(v \otimes f) \otimes g &= (f \odot v) \otimes g \\ &= (f(T)(v)) \otimes g \\ &= g \odot (f(T)(v)) \\ &= g(T)(f(T)(v)) \\ &= (g(T)f(T))(v) \\ &= (gf)(T)(v) \\ &= v \otimes (gf) \\ &= v \otimes (fg).\end{aligned}$$

II)

$$\begin{aligned}(u+v) \otimes f &= f \odot (u+v) \\ &= f(T)(u+v) \\ &= f(T)(u) + f(T)(v) \\ &= f \odot u + f \odot v \\ &= u \otimes f + v \otimes f\end{aligned}$$

III)

$$\begin{aligned} u \otimes (f+g) &= (f+g) \odot u \\ &= (f+g)(T)(u) \\ &= (f(T)+g(T))(u) \\ &= f(T)(u) + g(T)(u) \\ &= f \odot u + g \odot u \\ &= u \otimes f + u \otimes g. \end{aligned}$$

IV)

$$\begin{aligned} u \otimes Id_V &= Id_V \odot u \\ &= Id_V(u) = u. \end{aligned}$$

Portanto, V é um $K[x]$-módulo à direita.

Exemplo 1.0.13. *Seja $G = \{e, a, b, ab\}$ um grupo abeliano, onde $a^2 = b^2 = e$ e $ab = ba$. Tome $f, g \in End(G) = \{f : G \to G; f$ é um homomorfismo de grupos$\}$ definidos por*

$$\begin{array}{cc} f : G \longrightarrow G & g : G \longrightarrow G \\ e \longmapsto e & e \longmapsto e \\ a \longmapsto a & a \longmapsto b \\ b \longmapsto ab & b \longmapsto a \\ ab \longmapsto b & ab \longmapsto ab. \end{array}$$

Observe que $f \circ g \neq g \circ f$, pois

$$\begin{aligned} (f \circ g)(a) = f(g(a)) = f(b) = ab \\ (g \circ f)(a) = g(f(a)) = g(a) = b. \end{aligned}$$

Pelo Exemplo 1.0.8, segue que G é um $End(G)$-módulo á esquerda quando adotamos a lei de composição externa dada por $f \odot x = f(x)$, para todo $x \in G$ e $f \in End(G)$. Defina uma nova lei de composição externa

$$\begin{aligned} \otimes : G \times End(G) &\longrightarrow G \\ (x, f) &\longmapsto x \otimes f = f \odot x = f(x), \end{aligned}$$

para todo $x \in G$ e $f \in End(G)$.

***Afirmação**: G com a lei de composição externa $\otimes$ não é um $End(G)$-módulo à direita.*

De fato,

$$\begin{aligned}(a \otimes f) \otimes g &= (f \odot a) \otimes g \\ &= f(a) \otimes g \\ &= g \odot f(a) = g(f(a)) = b\end{aligned}$$

e

$$\begin{aligned}a \otimes (fg) &= (fg) \odot a \\ &= (fg)(a) \\ &= f(g(a)) = f(b) = ab\end{aligned}$$

ou seja, $(a \otimes f) \otimes g \neq a \otimes (fg)$. Portanto, G com a lei de composição externa $\otimes$ não é um $End(G)$-módulo à direita.

Observação 1.0.14. *No que segue, estudaremos A-módulos à esquerda. Por essa razão, usaremos a expressão A-módulo, caso não haja confusão. Da mesma forma, dados um A-módulo M, $a \in A$ e $m \in M$, escreveremos am, ao invés de $a \cdot m$, caso não exista ambiguidade.*

1.1 Submódulos

Definição 1.1.1. *Sejam M um A-módulo e $N \subset M$, onde $N \neq \emptyset$. Diremos que N é um submódulo de M se N é um A-módulo com as operações de M.*

Observação 1.1.2. *Um conjunto $N \subset M$ não vazio é um submódulo de um A-modulo M se, e somente se,*

I) $0_M \in N$;

II) Se $x, y \in N$, *então* $x - y \in N$;

III) Se $a \in A$, $x \in N$ *então,* $ax \in N$.

Exemplo 1.1.3. *Seja M um A-módulo. Então $\{0_M\}$ e M são submódulos de M, chamados de submódulos triviais de M.*

Exemplo 1.1.4. *Os submódulos de A^A são os ideais à esquerda do anel A.*

De fato, seja N um submódulo de A^A. Desta forma,

I) $0_A \in N$;

II) *se* $x, y \in N$, *então* $x - y \in N$;

III) *se* $a \in A$ *e* $x \in N$, *então* $ax \in N$.

Portanto, N é um ideal à esquerda de A.

Exemplo 1.1.5. *Seja M um grupo abeliano. Então os submódulos do $\mathbb{Z}$-módulo M são os subgrupos de M.*

Com efeito, seja N um submódulo de M. Logo,

I) $0_M \in N$;

II) *Se* $x, y \in N$, *então* $x - y \in N$.

Portanto, N é um subgrupo de M.

Definição 1.1.6. *Seja M um A-módulo. O conjunto*

$$Anl(M) = \{a \in A; am = 0_M; \text{ para todo } m \in M\}$$

é dito anulador de M. Em particular, se $Anl(M) = \{0_A\}$, M é dito um A-módulo fiel.

Proposição 1.1.7. *Se M um A-módulo, então $Anl(M)$ é um ideal de A.*

Demonstração. De fato,

I) $0_A \in Anl(M)$, pois $0_A m = 0_M$, para todo $m \in M$;

II) Tome $x, y \in Anl(M)$. Como

$$\begin{aligned}(x-y)m &= xm - ym \\ &= 0_M - 0_M = 0_M,\end{aligned}$$

para todo $m \in M$, concluímos que $x - y \in Anl(M)$;

III) Dado $x \in Anl(M)$ e $a \in A$, tem-se

$$(ax)m = a(xm) = a0_M = 0_M$$

e

$$(xa)m = x(am) = 0_M$$

para todo $m \in M$. Logo, ax, $xa \in Anl(M)$.

Portanto, $Anl(M)$ é um ideal de A. □

Definição 1.1.8. *Sejam M um grupo abeliano e A um anel. Uma representação de A por M é um homomorfismo de anéis $f : A \to End(M)$.*

Proposição 1.1.9. *Sejam M um grupo abeliano e A um anel. Se M tem uma estrutura de A-módulo, então a aplicação*

$$\begin{array}{rccccc} \psi: & A & \longrightarrow & End(M) & & \\ & a & \longmapsto & \psi(a): & M & \longrightarrow & M \\ & & & & m & \longmapsto & \psi(a)(m) = am \end{array}$$

é um homomorfismo de anéis, isto é, ψ é uma representação de A por M.

Demonstração. Com efeito, dados a, $b \in A$, tem-se

$$\begin{aligned} \psi(a+b)(m) &= (a+b)m \\ &= am + bm \\ &= \psi(a)(m) + \psi(b)(m) \\ &= (\psi(a) + \psi(b))(m), \end{aligned}$$

para todo $m \in M$, o que implica que $\psi(a+b) = \psi(a) + \psi(b)$.

Por outro lado,

$$\begin{aligned} \psi(ab)(m) &= (ab)m \\ &= a(bm) \\ &= \psi(a)(bm) \\ &= \psi(a)[\psi(b)(m)] \\ &= (\psi(a) \circ \psi(b))(m), \end{aligned}$$

para todo $m \in M$, o que implica que $\psi(ab) = \psi(a) \circ \psi(b)$.

Portanto, ψ é uma representação de A por M. □

Proposição 1.1.10. *M é um A-módulo fiel se, e somente se, a representação ψ de A por M é injetora.*

Demonstração. De fato, seja $\psi : A \to End(M)$, dada por

$$\begin{array}{rccl} \psi: & A & \longrightarrow & End(M) \\ & a & \longmapsto & \psi(a): \quad M \longrightarrow M \\ & & & \qquad\quad m \longmapsto \psi(a)(m) = am. \end{array}$$

Suponha que M seja um A-módulos fiel. Tome $a \in Ker(\psi)$ qualquer. Desta forma, $\psi(a) = 0_{End(M)}$, o que implica em $\psi(a)(m) = 0(m)$, ou seja, $am = 0_M$, para todo $m \in M$. Assim, pela Definição 1.1.6, $a \in Anl(M) = \{0_A\}$, pois M é um A-módulo fiel. Logo, $Ker(\psi) = \{0_A\}$ e, portanto, ψ é injetora.

Reciprocamente, tome $a \in Anl(M)$. Assim, para todo $m \in M$, tem-se $am = 0_M$. Desta forma, tem-se $\psi(a)(m) = am = 0_M$, para $m \in M$, o que implica que $\psi(a) = 0_{End(M)}$, ou seja, $a \in Ker(\psi) = \{0_A\}$, pois ψ é injetora. Logo $a = 0_A$ e, consequentemente, $Anl(M) = \{0_A\}$. Portanto M é um A-módulo fiel.

□

Exemplo 1.1.11. *$\mathbb{Z}_6 \times \mathbb{Z}_9$ não é um $\mathbb{Z}$-módulo fiel.*

Com efeito, considere o seguinte homomorfismo de aneis:

$$\begin{array}{rccl} \psi: & \mathbb{Z} & \longrightarrow & End(\mathbb{Z}_6 \times \mathbb{Z}_9) \\ & n & \longmapsto & \psi(n): \quad \mathbb{Z}_6 \times \mathbb{Z}_9 \longrightarrow \mathbb{Z}_6 \times \mathbb{Z}_9 \\ & & & \qquad\quad ([a]_6, [b]_9) \longmapsto \psi(n)[([a]_6, [b]_9)] = ([na]_6, [nb]_9). \end{array}$$

Tome $n \in Ker(\psi)$. Desta forma:

$$\begin{aligned} \psi(n) &= 0_{End(\mathbb{Z}_6 \times \mathbb{Z}_9)} \\ \psi(n)([a]_6, [b]_9) &= ([0]_6, [0]_9), \text{ para todo } ([a]_6, [b]_9) \in \mathbb{Z}_6 \times \mathbb{Z}_9. \end{aligned}$$

Em particular, $\psi(n)([1]_6, [1]_9) = ([0]_6, [0]_9)$. Assim, $([n]_6, [n]_9) = ([0]_6, [0]_9)$, o que implica que $[n]_6 = [0]_6$ e $[n]_9 = [0]_9$. Desta forma, $[6, 9]|n$ e, consequentemente, $18|n$, ou seja, $n \in 18\mathbb{Z}$. Logo $Ker(\psi) \subset 18\mathbb{Z}$.

Por outro lado, tome $n = 18l \in 18\mathbb{Z}$ *arbitrário. Assim, para todo* $([a]_6, [b]_9) \in \mathbb{Z}_6 \times \mathbb{Z}_9$, *tem-se*

$$\begin{aligned} \psi(n)([a]_6, [b]_9) &= ([na]_6, [nb]_9) \\ \psi(n)([a]_6, [b]_9) &= ([18la]_6, [18lb]_9) \\ \psi(n)([a]_6, [b]_9) &= ([0]_6, [0]_9), \end{aligned}$$

o que implica que $\psi(n) = 0$, *ou seja,* $n \in Ker(\psi)$. *Deste modo,* $18\mathbb{Z} \subset Ker(\psi)$. *Assim,* $Ker(\psi) = 18\mathbb{Z} \neq \{0\}$. *Logo, pela Proposição 1.1.10,* $\mathbb{Z}_6 \times \mathbb{Z}_9$ *não é um* $\mathbb{Z}$*-módulo fiel.*

Definição 1.1.12. *Seja* M *um* A*-módulo e* $S \subset M$ *não vazio qualquer. É de fácil verificação que o conjunto* $((S)) = \{\sum_{i=1}^{n} a_i s_i, n \in \mathbb{N}, a_i \in A, s_i \in S\}$ *é um submódulo de* M. *Se* $S = \{m_1, m_2, ..., m_r\}$, *denotaremos por* $((m_1, m_2, ..., m_r))$, *em invés de* $((\{m_1, m_2, ..., m_r\}))$. *Deste modo, se* $S \subset M$, *diremos que* $((S))$ *é um submódulo de* M *gerado por* S. *Se* $S = \{m\}$, *então* $((S)) = ((m))$ *e o chamaremos de submódulo de* M *gerado por* m. *Mais especificamente, o submódulo* $((S)) = ((m))$ *é chamado de módulo cíclico gerado por* m. *Diremos que o* A*-módulo é finitamente gerado, se existe* $S \subset M$ *finito tal que* $M = ((S))$.

Exemplo 1.1.13. *Se* V *é um espaço vetorial sobre* K, *de dimensão finita, então* V *é um* K*-módulo finitamente gerado.*

Exemplo 1.1.14. $\mathbb{Q}$ *é um* $\mathbb{Z}$*-módulo não finitamente gerado.*

Com efeito, este fato é consequência das seguintes afirmações:

I) $\mathbb{Q}$ não é um $\mathbb{Z}$-módulo cíclico.

II) Seja $S \subset \mathbb{Q}$ tal que $((S)) = \mathbb{Q}$. Se $a \in S$, então $((S - \{a\})) = ((S)) = \mathbb{Q}$.

I) De fato, suponhamos que exista $\frac{a}{b} \in \mathbb{Q}$, com $a, b \in \mathbb{Z}, b \neq 0, a, b > 0$ e $(a, b) = 1$, tais que $((\frac{a}{b})) = \mathbb{Q}$. Como existem infinitos primos, tome $q \in \mathbb{N}$, primo, tal que q não divide b. Como $\frac{1}{q} \in \mathbb{Q}$ e $((\frac{a}{b})) = \mathbb{Q}$, existe $\alpha \in \mathbb{Z}$, tal que

$$\frac{1}{q} = \alpha \frac{a}{b}.$$

Daí $b = \alpha aq$, ou seja, q divide b, o que é um absurdo! Portanto $\mathbb{Q}$ não é um $\mathbb{Z}$-módulo cíclico.

II) Com efeito, defina $S_0 = S - \{a\}$. Como $a \in \mathbb{Q} = ((S))$, existem $k_0, k_1, k_2, ..., k_n \in \mathbb{Z}$ e $a_1, a_2, ..., a_n \in S$ tais que

$$\begin{aligned} \frac{a}{2} &= k_0 a + \sum_{i=1}^{n} k_i a_i \\ a &= (2k_0)a + \sum_{i=1}^{n} (2k_i)a_i \\ (1 - 2k_0)a &= \sum_{i=1}^{n} (2k_i)a_i. \end{aligned}$$

Tome $m = 1 - 2k_0$. Como $k_0 \in \mathbb{Z}$, segue que $m \neq 0$, o que implica em $\frac{a}{m} \in \mathbb{Q} = ((S))$. Então existem $k_0', k_1', ..., k_r' \in \mathbb{Z}$ e $b_1, b_2, ..., b_r \in S$, tais que

$$\begin{aligned} \frac{a}{m} &= k_0' a + \sum_{i=1}^{r} k_i' b_i \\ a &= m(k_0' a) + \sum_{i=1}^{r} (mk_i')b_i \\ a &= k_0'(ma) + \sum_{i=1}^{r} (mk_i')b_i \\ a &= k_0' \sum_{i=1}^{n} (2k_i)a_i + \sum_{i=1}^{r} (mk_i')b_i \\ a &= \sum_{i=1}^{n} (2k_0' k_i)a_i + \sum_{i=1}^{r} (mk_i')b_i, \end{aligned}$$

o que implica que $a \in ((S - \{a\})) = ((S_0))$, ou seja, $((S)) \subset ((S_0))$. Como $((S_0)) \subset ((S))$ segue que $((S_0)) = ((S)) = \mathbb{Q}$.

Por fim, suponha que $\mathbb{Z}$-módulo $\mathbb{Q}$ seja finitamente gerado. Assim, existe $S \subset \mathbb{Q}$, finito, tal que $((S)) = \mathbb{Q}$. Aplicando a afirmação (II) $n(S) - 1$ vezes, onde $n(S)$ é o número de elementos do conjunto S, segue que o conjunto obtido gera $\mathbb{Q}$, o que implica que $\mathbb{Q}$ é um $\mathbb{Z}$-módulo cíclico, absurdo!

Portanto, o $\mathbb{Z}$-módulo $\mathbb{Q}$ não é finitamente gerado.

Exemplo 1.1.15. *A^A é cíclico, pois $A = ((1_A))$.*

Na teoria de Espaços Vetoriais, todo subespaço de um espaço vetorial finitamente gerado é finitamente gerado. No entanto, nem todo submódulo de um A-módulo finitamente gerado é finitamente gerado. No Exemplo 1.1.16 será apresentado um resultado que comprova esse fato.

Exemplo 1.1.16. *Seja A um anel e considere o anel $B = A^{\mathbb{N}} = \{(a_1, a_2, ...);\ a_i \in A\}$ das sequências em A. Notemos que B^B é finitamente gerado, pois $B^B = (((1_A, 1_A, ...)))$. Considere $N = \{f \in B;\ f(k) = 0_A$, exceto para um n^o finito de $k \in \mathbb{N}\}$.*

Afirmação 1: N é um submódulo de B^B.

De fato,

I) $0_B = (0_A, 0_A, ...) \in N$;

II) Tome $f, g \in N$ quaisquer. Desta forma, existem $i, j \in \mathbb{N}$ tais que $f(k) = 0_A$, para todo $k > i$ e $g(k) = 0_A$, para todo $k > j$. Considere $r = max\{i, j\}$. Como

$$(f - g)(k) = f(k) - g(k) = 0_A - 0_A = 0_A,$$

para todo $k > r$, segue que $f - g \in N$;

III) Como $(fg)(k) = f(k)g(k) = 0_A$, para todo $k > i$, segue que $fg \in N$.

De (I), (II) e (III) concluímos que N é um submódulo de B^B.

Afirmação 2: N não é finitamente gerado.

Com efeito, suponha que N seja finitamente gerado. Assim, existem $f_1, f_2, f_3, ..., f_n \in B^B$ tais que

$$N = ((f_1, f_2, f_3, ..., f_n)).$$

Deste modo, para cada $i \in \{1, ..., n\}$, considere $X_i = \{k \in \mathbb{N};\ f_i(k) \neq 0_A\}$. Por definição, X_i é finito e, consequentemente, $X = X_1 \cup X_2 \cup ... \cup X_n$ é um conjunto finito.

Tome $m \in \mathbb{N} - X$ e $f \in N$ dada por:

$$f(k) = \begin{cases} 1_A, & \text{se} \quad k = m; \\ 0_A, & \text{se} \quad k \neq m. \end{cases}$$

Por outro lado, como $f \in N = ((f_1, f_2, ..., f_n))$, existem $g_1, g_2, ..., g_n \in B$, tais que

$$f = f_1 \cdot g_1 + f_2 \cdot g_2 + ... + f_n \cdot g_n.$$

Assim, $1_A = f(m) = f_1(m) \cdot g_1(m) + f_2(m) \cdot g_2(m) + ... + f_n(m) \cdot g_n(m)$, ou seja, $1_A = 0_A$, o que é um absurdo. Portanto, N não é finitamente gerado.

Definição 1.1.17. *Seja M um A-módulo.*

i) M é dito um A-módulo simples, se os seus únicos submódulos são os triviais;

ii) Um submódulo $N \neq M$ é dito maximal de M, se $N \subset N'$ implica em $N' = N$ ou $N' = M$, para todo submódulo N' de M;

iii) Um submódulo $N \neq \{0_M\}$ é dito minimal em M, se $N' \subset N$ implica em $N' = \{0_M\}$ ou $N' = N$, para cada submódulo N' de N.

Exemplo 1.1.18. *Os submódulos de $\mathbb{Z}^{\mathbb{Z}}$ são da forma $((n))$, onde $n \geq 0$. Além disso, $((p))$ é maximal se, e somente se, p é primo. Notemos, também, que $\mathbb{Z}^{\mathbb{Z}}$ não possui submódulos minimais, pois $((2n)) \subsetneqq ((n))$, para $n \neq 0$.*

Proposição 1.1.19. *Seja M um A-módulo e N um submódulo próprio de M. Então N é maximal se, e somente se, $M = N + ((x))$, para todo $x \in M - N$.*

Demonstração. Considere $R = N + ((x))$, com $x \in M - N$. Como R é um submódulo de M tal que $N \subset R$, então pela maximalidade de N, segue que $R = N$ ou $R = M$. Como $x \in R$ e $x \notin N$, então, $R = M$.

Reciprocamente, suponha que $M = N + ((x))$ para todo $x \in M - N$. Desta forma, como $N \neq M$, tome R um submódulo de M tal que $N \subsetneqq R \subset M$. Assim, existem $y \in R$ e $y \notin N$. Por hipótese, segue que $M = N + ((y))$, o que implica que $M = N + ((y)) \subset N + R = R$, ou seja, $M \subset R$. Como $R \subset M$, concluímos que $M = R$. Portanto, N é um submódulo maximal de M. □

Exemplo 1.1.20. *$\mathbb{Q}$ é um $\mathbb{Z}$-módulo que não possui submódulos maximais.*

De fato, seja N um submódulo maximal de $\mathbb{Q}$. Desta forma, tem-se $N \neq \mathbb{Q}$ e, pela Proposição 1.1.19, segue que $\mathbb{Q} = N + ((x))$, para todo $x \in \mathbb{Q} - N$. Logo, $N \cup \{x\}$ é um conjunto de geradores de $\mathbb{Q}$, ou seja, $\mathbb{Q} = ((N \cup \{x\}))$. Do item (II), do Exemplo 1.1.14, $\mathbb{Q} = ((N \cup \{x\})) = ((N))$, o que é um absurdo, pois $x \notin N$. Portanto, $\mathbb{Q}$ não possui submódulos maximais.

1.2 Módulos Quociente

Seja M um A-módulo e N um submódulo de M. Considerando apenas a estrutura do grupo aditivo abeliano de M, podemos construir o grupo quociente

$$\frac{M}{N} = \{m + N;\, m \in M\},$$

com a operação $\oplus : \frac{M}{N} \times \frac{M}{N} \longrightarrow \frac{M}{N}$ dada por $(m_1 + N) \oplus (m_2 + N) = (m_1 + m_2) + N$.

Afirmação 1: A operação está bem definida.

De fato, sejam $r_1 + N,\ r_2 + N,\ s_1 + N,\ s_2 + N \in \frac{M}{N}$ tais que $r_1 + N = r_2 + N$ e $s_1 + N = s_2 + N$. Desta forma, $r_1 - r_2,\ s_1 - s_2 \in N$ e segue que $(r_1 - r_2) + (s_1 - s_2) \in N$. Assim, $(r_1 + s_1) - (r_2 + s_2) \in N$, o que implica que $(r_1 + s_1) + N = (r_2 + s_2) + N$, ou seja, $(r_1 + N) \oplus (s_1 + N) = (r_2 + N) \oplus (s_2 + N)$.

Afirmação 2: $(\frac{M}{N}, \oplus)$ é um grupo abeliano.

Com efeito, dados $r, s, t \in M$ tem-se

I) (Associatividade)

$$\begin{aligned}(r + N) \oplus [(s + N) \oplus (t + N)] &= (r + N) \oplus [(s + t) + N] \\ &= [r + (s + t)] + N \\ &= [(r + s) + t] + N \\ &= [(r + s) + N] \oplus (t + N) \\ &= [(r + N) \oplus (s + N)] \oplus (t + N).\end{aligned}$$

II) (Elemento Neutro) $(0_M + N) \oplus (m + N) = (0_M + m) + N = m + N$, para todo $m \in M$. Desta forma, $0_M + N$ é o elemento neutro de $\frac{M}{N}$.

III) (Inverso Aditivo) $(r + N) \oplus (-r + N) = [r + (-r)] + N = 0_M + N$, ou seja, $-r + N$ é o inverso aditivo de $r + N$.

IV) (Comutatividade) $(r+N) \oplus (s+N) = (r+s)+N = (s+r)+N = (s+N) \oplus (r+N)$.

Portanto, $(\frac{M}{N}, \oplus)$ é um grupo abeliano. Considere a lei de composição externa

$$\begin{array}{rcl} A \times \dfrac{M}{N} & \longrightarrow & \dfrac{M}{N} \\ (a, m+N) & \longmapsto & a(m+N) = am + N. \end{array}$$

Note que essa lei de composição externa está bem definida, pois dados $m + N = r + N$, tem-se $m - r \in N$, e dado $a \in A$, segue que $a(m-r) = am - ar \in N$, o que implica que $am + N = ar + N$, ou seja, $a(m+N) = a(r+N)$.

Afirmação 3: O grupo aditivo $\dfrac{M}{N}$, com essa lei de composição externa, define uma estrutura de A-módulo.

Demonstração. De fato, dados $m+N$, $r+N$, $s+N \in \dfrac{M}{N}$ e α, $\beta \in A$ quaisquer, tem-se:

I)

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

II)

$$\begin{aligned} \alpha[(m+N) \oplus (r+N)] &= \alpha[(m+r)+N] \\ &= \alpha(m+r) + N \\ &= (\alpha m + \alpha r) + N \\ &= (\alpha m + N) \oplus (\alpha r + N) \\ &= \alpha(m+N) \oplus \alpha(r+N). \end{aligned}$$

III)

$$\begin{aligned} (\alpha+\beta)(m+N) &= [(\alpha+\beta)m] + N \\ &= (\alpha m + \beta m) + N \\ &= (\alpha m + N) \oplus (\beta m + N) \\ &= \alpha(m+N) \oplus \beta(m+N). \end{aligned}$$

IV)

$$\begin{aligned} 1_A.(m+N) &= 1_A.m+N \\ &= m+N. \end{aligned}$$

Portanto, $\frac{M}{N}$ é um A-módulo. □

Definição 1.2.1. *$\frac{M}{N}$ é um A-módulo chamado de módulo quociente de M pelo submódulo N.*

Exemplo 1.2.2. *Se J é um ideal à esquerda de um anel A, então $\frac{A}{J}$ é um A-módulo.*

Proposição 1.2.3. *Seja N um submódulo de um A-módulo M. Se N e $\frac{M}{N}$ são finitamente gerados, então M é finitamente gerado.*

Demonstração. Considere $S_1 = \{m_1 + N, ..., m_r + N\}$ um conjunto gerador de $\frac{M}{N}$ e $S_2 = \{n_1, n_2, ..., n_s\}$ um conjunto gerador de N.

Afirmação: $S = \{m_1, m_2, ..., m_r, n_1, n_2, ..., n_s\}$ é um conjunto de geradores de M.

De fato, tome $m \in M$ qualquer. Deste modo, $m + N \in \frac{M}{N}$, o que implica que existem $a_1, a_2, ..., a_r \in A$, tais que $m + N = a_1(m_1 + N) \oplus ... \oplus a_r(m_r + N)$. Assim, $m+N = (a_1m_1+N)\oplus...\oplus(a_rm_r+N) = (a_1m_1+a_2m_2+...+a_rm_r)+N$, o que implica que $m-(a_1m_1+a_2m_2+...+a_rm_r) \in N$ e, como S_2 gera N, existem $b_1, b_2, ..., b_s \in A$, tais que $m-(a_1m_1+...+a_rm_r) = b_1n_1+...+b_sn_s$. Logo, $m = a_1m_1+...+a_rm_r+b_1n_1+...+b_sn_s$, ou seja, S gera M. □

Exemplo 1.2.4. *$\frac{\mathbb{Q}}{\mathbb{Z}}$ é um $\mathbb{Z}$-módulo não finitamente gerado.*

De fato, sabemos que $\mathbb{Z}^{\mathbb{Z}}$ é um submódulo do $\mathbb{Z}$-módulo $\mathbb{Q}$, o que implica que $\frac{\mathbb{Q}}{\mathbb{Z}}$ é um $\mathbb{Z}$-módulo. Suponha que $\frac{\mathbb{Q}}{\mathbb{Z}}$ seja um $\mathbb{Z}$-módulo finitamente gerado. Assim, como $\mathbb{Z}^{\mathbb{Z}}$ é finitamente gerado, pela Proposição 1.2.3, segue que $\mathbb{Q}$ é um $\mathbb{Z}$-módulo finitamente gerado, o que é um absurdo! Portanto, $\frac{\mathbb{Q}}{\mathbb{Z}}$ é um $\mathbb{Z}$-módulo não finitamente gerado.

Observação 1.2.5. *Seja N um submódulo do A-módulo M. Por simplicidade, denotaremos o elemento $m + N \in \frac{M}{N}$, como sendo $\overline{m} = m + N \in \frac{M}{N}$.*

O Exemplo 1.2.6 mostrará um A-módulo M não finitamente gerado, no qual todos os seus submódulos próprios são finitamente gerados.

Exemplo 1.2.6. *Seja A um domínio de ideais principais, K o seu corpo de frações e $p \in A$ um elemento irredutível. Considere o conjunto*

$$K_p = \{\frac{a}{p^k};\ k \geq 0 \ e\ a \in A\}.$$

Afirmação 1: *K_p é um submódulo do A-módulo K.*

De fato,

- $0_K = \dfrac{0_A}{1_A} = \dfrac{0_A}{p^0} \in K_p$.
- *Tome $x, y \in K_p$ quaisquer. Assim, existem $a, b \in A$ e $r, s \in \mathbb{N}$ tais que $x = \dfrac{a}{p^r}$ e $y = \dfrac{b}{p^s}$. Logo, $x - y = \dfrac{a}{p^r} - \dfrac{b}{p^s} = \dfrac{ap^s - bp^r}{p^{r+s}} \in K_p$.*
- *Tome $c \in A$ qualquer. Desta forma, $cx = c(\dfrac{a}{p^r}) = \dfrac{ca}{p^r} \in K_p$.*

Portanto, K_p é um submódulo do A-módulo K. Notemos que $A \subset K_p$, pois dado $a \in A$ qualquer, podemos escrever $a = \dfrac{a}{p^0} \in K_p$.

Afirmação 2: *$K_p = \bigcup_{k=0}^{\infty}((\dfrac{1}{p^k}))$.*

De fato, como $\dfrac{1}{p^k} \in K_p$, então $((\dfrac{1}{p^k})) \subset K_p$, e consequentemente, $\bigcup_{k=0}^{\infty}((\dfrac{1}{p^k})) \subset K_p$.

Por outro lado, tome $\dfrac{a}{p^r} \in K_p$ qualquer. Como $\dfrac{a}{p^r} = a\dfrac{1}{p^r} \in ((\dfrac{1}{p^r})) \subset \bigcup_{k=0}^{\infty}((\dfrac{1}{p^k}))$, segue que $K_p \subset \bigcup_{k=0}^{\infty}((\dfrac{1}{p^k}))$.

Portanto, $K_p = \bigcup_{k=0}^{\infty}((\dfrac{1}{p^k}))$.

Afirmação 3: *$((\dfrac{1}{p^r}))$ é um submódulo maximal de $((\dfrac{1}{p^{r+1}}))$.*

Com efeito, se $x \in ((\dfrac{1}{p^r}))$, existe $a \in A$ tal que $x = \dfrac{a}{p^r}$. Como $x = \dfrac{a}{p^r} = \dfrac{ap}{p^{r+1}} \in ((\dfrac{1}{p^{r+1}}))$, segue que $((\dfrac{1}{p^r})) \subset ((\dfrac{1}{p^{r+1}}))$. Se $((\dfrac{1}{p^r})) = ((\dfrac{1}{p^{r+1}}))$, existe $b \in A$ tal que $\dfrac{1}{p^{r+1}} = b\dfrac{1}{p^r}$, o que implica que $bp^{r+1} = p^r$ e, consequentemente, $bp = 1_A$. Logo, p é um elemento inversível de A, o que é um absurdo, pois p é um elemento irredutível de A. Desta forma, $((\dfrac{1}{p^r})) \subsetneq ((\dfrac{1}{p^{r+1}}))$.

Tome $x \in ((\frac{1}{p^{r+1}})) - ((\frac{1}{p^r}))$ *qualquer. Assim,* $x = \frac{a}{p^{r+1}}$, *para algum* $a \in A$ *e é tal que* $(a,p) = 1$. *De* $(a,p) = 1$, *existem* $x_0, y_0 \in A$, *tais que* $ax_0 + py_0 = 1$. *Como*

$$\frac{b}{p^{r+1}} = \frac{abx_0 + pby_0}{p^{r+1}} = (bx_0)\frac{a}{p^{r+1}} + (by_0)\frac{1}{p^r} \in ((x)) + ((\frac{1}{p^r})),$$

segue que $((\frac{1}{p^{r+1}})) \subset ((x)) + ((\frac{1}{p^r}))$. *Sabendo que* $((x)) + ((\frac{1}{p^r})) \subset ((\frac{1}{p^{r+1}}))$, *concluímos que* $((\frac{1}{p^{r+1}})) = ((x)) + ((\frac{1}{p^r}))$. *Como* $x \in ((\frac{1}{p^{r+1}})) - ((\frac{1}{p^r}))$ *é arbitrário, pela Proposição 1.1.19, segue que* $((\frac{1}{p^r}))$ *é um submódulo maximal de* $((\frac{1}{p^{r+1}}))$.

Da Afirmação 1, K_p *é um submódulo do* A*-módulo* K, *o que implica que* K_p *é um* A*-módulo. Como* $A \subset K^p$, *tem-se que* A^A *é um submódulo do* A*-módulo* K_p. *Deste modo, podemos considerar o* A*-módulo* $A_{p^\infty} = \frac{K_p}{A}$.

Afirmação 4: $\frac{((\frac{1}{p^r}))}{A}$ *é um submódulo maximal de* $\frac{((\frac{1}{p^{r+1}}))}{A}$.

De fato, de $((\frac{1}{p^r})) \subsetneq ((\frac{1}{p^{r+1}}))$, *então* $\frac{((\frac{1}{p^r}))}{A} \subsetneq \frac{((\frac{1}{p^{r+1}}))}{A}$. *Notemos que não pode ocorrer* $\frac{((\frac{1}{p^r}))}{A} = \frac{((\frac{1}{p^{r+1}}))}{A}$, *pois caso contrário, teríamos* $\overline{\frac{1}{p^{r+1}}} \in \frac{((\frac{1}{p^r}))}{A} = \frac{((\frac{1}{p^{r+1}}))}{A}$, *o que implica que* $\frac{1}{p^{r+1}} \in ((\frac{1}{p^r}))$, *o que é um absurdo! Logo* $\frac{((\frac{1}{p^r}))}{A} \subsetneq \frac{((\frac{1}{p^{r+1}}))}{A}$.

Tome $\overline{\frac{a}{p^{r+1}}} \in \frac{((\frac{1}{p^{r+1}}))}{A}$ *tal que* $\overline{\frac{a}{p^{r+1}}} \notin \frac{((\frac{1}{p^r}))}{A}$. *Isto implica que* $\frac{a}{p^{r+1}} \notin ((\frac{1}{p^r}))$ *e, consequentemente,* $(a,p) = 1$. *Pela identidade de Bezout, existem* $x_0, y_0 \in A$ *tais que* $ax_0 + py_0 = 1$.

Dado $\overline{\frac{b}{p^{r+1}}} \in \frac{((\frac{1}{p^{r+1}}))}{A}$, *tem-se que* $\overline{\frac{b}{p^{r+1}}} = \overline{\frac{abx_0+pby_0}{p^{r+1}}} = \overline{(bx_0)\frac{a}{p^{r+1}} + (by_0)\frac{1}{p^r}} \in \frac{((\frac{1}{p^{r+1}}))}{A} + \frac{((\frac{1}{p^r}))}{A}$, *ou seja,* $\frac{((\frac{1}{p^{r+1}}))}{A} \subset \frac{((\frac{a}{p^{r+1}}))}{A} + \frac{((\frac{1}{p^r}))}{A}$ *e, portanto* $\frac{((\frac{1}{p^{r+1}}))}{A} = \frac{((\frac{1}{p^r}))}{A} + \frac{((\frac{a}{p^{r+1}}))}{A}$.

Como $\frac{((\frac{1}{p^{r+1}}))}{A} = \frac{((\frac{1}{p^r}))}{A} + \frac{((\frac{a}{p^{r+1}}))}{A}$ *e* $\frac{\overline{a}}{p^{r+1}} \in \frac{((\frac{1}{p^{r+1}}))}{A} - \frac{((\frac{1}{p^r}))}{A}$ *é arbitrário, pela proposição 1.1.19,* $\frac{((\frac{1}{p^r}))}{A}$ *é um submódulo maximal de* $\frac{((\frac{1}{p^{r+1}}))}{A}$.

Afirmação 5: $A_{p^\infty} = \frac{K_p}{A}$ *não é finitamente gerado.*

Com efeito, suponha que A_{p^∞} *seja finitamente gerado. Assim, existem* $\frac{a_1}{p^{\alpha_1}}, \frac{a_2}{p^{\alpha_2}}, ..., \frac{a_r}{p^{\alpha_r}}$ *em* K_p, *tais que* $A_{p^\infty} = (\overline{\frac{a_1}{p^{\alpha_1}}}, \overline{\frac{a_2}{p^{\alpha_2}}}, ..., \overline{\frac{a_r}{p^{\alpha_r}}})$. *Tome* $\alpha = max\{\alpha_1, \alpha_2, ..., \alpha_r\}$. *Dado* $\frac{1}{p^{\alpha+1}} \in K_p$, *segue que existem* $x_1, x_2, ..., x_r \in A$, *tais que* $\overline{\frac{1}{p^{\alpha+1}}} = x_1\overline{\frac{a_1}{p^{\alpha_1}}} + x_2\overline{\frac{a_2}{p^{\alpha_2}}} + ... + x_r\overline{\frac{a_r}{p^{\alpha_r}}}$. *Assim,*

$$\overline{\frac{1}{p^{\alpha+1}}} = \overline{\frac{x_1a_1}{p^{\alpha_1}}} + \overline{\frac{x_2a_2}{p^{\alpha_2}}} + ... + \overline{\frac{x_ra_r}{p^{\alpha_r}}} = \overline{\frac{x_1a_1}{p^{\alpha_1}} + \frac{x_2a_2}{p^{\alpha_2}} + ... + \frac{x_ra_r}{p^{\alpha_r}}},$$

ou seja, $\overline{\frac{1}{p^{\alpha+1}}} = \overline{\frac{c}{p^{\alpha}}}$*, para algum* $c \in A$*. Desta forma,* $\overline{\frac{1}{p^{\alpha+1}} - \frac{c}{p^{\alpha}}} = \overline{0}$*, o que implica que* $\frac{1}{p^{\alpha+1}} - \frac{c}{p^{\alpha}} = b \in A$*. Desenvolvendo tal igualdade, segue que* $1 = p(c + bp^{\alpha})$*, ou seja,* p *é um elemento inversível de* A*, o que é um absurdo, pois* p *é um elemento irredutível de* A*. Logo* $A_{p^\infty} = \frac{K_p}{A}$ *não é finitamente gerado.*

Afirmação 6: *Se* N *é um submódulo próprio de* A_{p^∞}*, então existe* $s \in \mathbb{N}^*$ *tal que* $N = \frac{((\frac{1}{p^s}))}{A}$*.*

Com efeito, sendo $N \neq \frac{K_p}{A}$*, então existe* $\overline{\frac{1}{p^n}} \in \frac{K_p}{A}$ *tal que* $\overline{\frac{1}{p^n}} \notin N$*. Seja* m *o menor inteiro positivo com esta propriedade, ou seja,* $\overline{\frac{1}{p^m}} \notin N$ *e* $\overline{\frac{1}{p^{m-1}}} \in N$*. De* $\overline{\frac{1}{p^{m-1}}} \in N$*, segue que* $\frac{((\frac{1}{p^{m-1}}))}{A} \subset N$*. Por outro lado, suponha que exista* $\overline{\frac{a}{p^r}} \in N$ *tal que* $\overline{\frac{a}{p^r}} \notin \frac{((\frac{1}{p^{m-1}}))}{A}$*. De* $\overline{\frac{a}{p^r}} \notin \frac{((\frac{1}{p^{m-1}}))}{A}$*, segue que* $\frac{a}{p^r} \notin ((\frac{1}{p^{m-1}}))$*, o que implica em* $r > m - 1$*, ou seja,* $r \geq m$*. Sem perda de generalidade, suponha que* $(a, p^r) = 1$*. Assim, existem* $x_0, y_0 \in A$ *tais que* $ax_0 + p^r y_0 = 1$*. Deste modo,* $\overline{\frac{1}{p^r}} = \overline{\frac{ax_0}{p^r}} = x_0\overline{\frac{a}{p^r}} \in N$*, o que implica em* $\frac{((\frac{1}{p^r}))}{A} \subset N$ *e, consequentemente,* $\overline{\frac{1}{p^m}} \in \frac{((\frac{1}{p^r}))}{A} \subset N$*, o que é um absurdo! Portanto,* $N \subset \frac{((\frac{1}{p^{m-1}}))}{A}$ *e, consequentemente,* $N = \frac{((\frac{1}{p^{m-1}}))}{A}$*.*

Portanto, $A_{p^\infty} = \frac{K_p}{A}$ *é um* A*-módulo não finitamente gerado na qual todo submódulo* N *de* A_{p^∞} *é cíclico, ou seja, todo submódulo próprio* N *de* A_{p^∞} *é finitamente gerado.*

1.3 Homomorfismos de A-módulos

Definição 1.3.1. *Sejam* M *e* N *A-módulos. Diremos que uma aplicação* $f : M \to N$ *é um A-homomorfismo ou um homomorfismo de A-módulos, se para todo* $m_1, m_2 \in M$ *e* $a \in A$*, vale:*

I) $f(m_1 + m_2) = f(m_1) + f(m_2)$*.*

II) $f(am_1) = af(m_1)$*.*

Definição 1.3.2. *Seja* $f : M \to N$ *um A-homomorfismo.*

a) Se $f : M \to N$ *é um A-homomorfismo injetivo, diremos que* f *é um A-monomorfismo.*

b) Se $f : M \to N$ *é um A-homomorfismo sobrejetivo, diremos que* f *é um A-epimorfismo.*

c) Se $f : M \to N$ é um A-homomorfismo bijetivo, diremos que f é um A-isomorfismo.

d) Se $f : M \to N$ é um A-isomorfismo, diremos que M e N são A-módulos isomorfos e denotaremos por $M \cong N$.

e) Os A-homomorfismos $f : M \to M$ são chamados de A-endomorfismos.

f) Os A-isomorfismos $f : M \to M$ são chamados de A-automorfismos.

g) Denotaremos por:

$$End_A(M) = \{f : M \to M;\ f \text{ é um } A\text{-endomorfismo}\}$$
$$Aut_A(M) = \{f : M \to M;\ f \text{ é um } A\text{-automorfismo}\}$$
$$Hom_A(M; N) = \{f : M \to N;\ f \text{ é um } A\text{-homomorfismo}\}.$$

Proposição 1.3.3. *(Propriedades elementares)*

a) Se $f : M \to N$ é um A-homomorfismo, então:

i) $f(0_M) = 0_N$;

Demonstração. De fato, $f(0_M) = f(0_M + 0_M) = f(0_M) + f(0_M)$. Subtraindo $f(0_M)$, em ambos os lados da igualdade, tem-se $f(0_M) = 0_N$. □

ii) $f(-m) = -f(m)$, para todo $m \in M$;

Demonstração. Com efeito, $0_N = f(0_M) = f(m + (-m)) = f(m) + f(-m)$. Subtraindo $f(m)$, em ambos os lado da igualdade, tem-se $f(-m) = -f(m)$. □

iii) $f(m - n) = f(m) - f(n)$, para todo $m, n \in M$.

Demonstração. De fato,

$$\begin{aligned} f(m-n) &= f(m+(-n)) \\ &= f(m) + f(-n) \\ &= f(m) + [-f(m)] = f(m) - f(n). \end{aligned}$$

□

b) Se $f : M \to M'$ e $g : M' \to M''$ são A-homomorfismos, então $g \circ f : M \to M''$ também é um A-homomorfismo.

Demonstração. Com efeito, dados $m_1, m_2 \in M$ e $a \in A$, tem-se

I)

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

II)

$$\begin{aligned}(g \circ f)(am_1) &= g(f(am_1)) \\ &= g(af(m_1)) \\ &= ag(f(m_1)) \\ &= a(g \circ f)(m_1).\end{aligned}$$

Portanto, $g \circ f$ é um A-homomorfismo. □

c) Se $f : M \to M'$ e $g : M' \to M$ são A-homomorfismos tais que $g \circ f = Id_M$, então f é um A-monomorfismo e g é um A-epimorfismo.

Demonstração. Sejam m_1, $m_2 \in M$ tais que $f(m_1) = f(m_2)$. Desta forma,

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

Logo, f é um um A-homomorfismo injetivo. Por outro lado, tome $m \in M$ arbitrário. Assim, $m = Id_M(m) = (g \circ f)(m) = g(f(m))$, ou seja, $m \in Im(g)$, o que implica que g é um A-homomorfismo sobrejetivo. Portanto, f é um A-monomorfismo e g é um A-epimorfismo. □

d) Se $f : M \to M'$ e $g : M' \to M''$ são A-epimorfismos, então $g \circ f : M \to M''$ também é um A-epimorfismo.

Demonstração. Com efeito, do item (b) dessa proposição, segue que $g \circ f : M \to M''$ é um A-homomorfismo. Por outro lado, como a composição de funções sobrejetoras

é uma função sobrejetora, segue que $g \circ f : M \to M''$ é sobrejetora. Portanto, $g \circ f : M \to M''$ é um A-epimorfismo. □

e) Se $f : M \to M'$ e $g : M' \to M''$ são A-monomorfismos, então $g \circ f : M \to M''$ também é um A-monomorfismo.

Demonstração. Com efeito, do item (b) dessa proposição, segue que $g \circ f : M \to M''$ é um A-homomorfismo. Por outro lado, como a composição de funções injetoras é uma função injetora, segue que $g \circ f : M \to M''$ é injetora. Portanto, $g \circ f : M \to M''$ é um A-monomorfismo. □

f) Se $f : M \to M'$ e $g : M' \to M''$ são A-isomorfismos, então $g \circ f : M \to M''$ também é um A-isomorfismo.

Demonstração. Segue imediatamente dos itens (d) e (e). □

Proposição 1.3.4. *Sejam M e N A-módulos e $f : M \to N$ uma aplicação.*
f é um A-homomorfismo se, e somente se, para quaisquer $m_1, m_2 \in M$ e $a \in A$, tem-se $f(am_1 + m_2) = af(m_1) + f(m_2)$.

Demonstração. Suponha que f seja um A-homomorfismo. Assim, para quaisquer $a \in A$ e $m_1, m_2 \in M$, segue que

$$\begin{aligned} f(am_1 + m_2) &= f(am_1) + f(m_2) \\ &= af(m_1) + f(m_2). \end{aligned}$$

Reciprocamente, suponha que $f(am_1+m_2) = af(m_1)+f(m_2)$, para quaisquer $m_1, m_2 \in M$ e $a \in A$. Em particular, tome $a = 1_A$. Assim,

$$\begin{aligned} f(m_1 + m_2) &= f(1_A m_1 + m_2) \\ &= 1_A f(m_1) + f(m_2) \\ &= f(m_1) + f(m_2). \end{aligned}$$

Por outro lado, tome $m_2 = 0_M$. Desta forma,

$$\begin{aligned} f(am_1) &= f(am_1 + 0_M) \\ &= af(m_1) + f(0_M) \\ &= af(m_1) + 0_N \\ &= af(m_1). \end{aligned}$$

□

Exemplo 1.3.5. *Aplicação $f : M \to N$ dada por $f(m) = 0_N$, para todo $m \in M$, é um A-homomorfismo chamado de homomorfismo nulo.*

Exemplo 1.3.6. *Seja N um submódulo de um A-módulo M. A aplicação de inclusão $Id : N \longrightarrow M$ dada por $Id(x) = x$ é um A-homomorfismo.*

Exemplo 1.3.7. *Seja N um submódulo de um A-módulo M. A projeção canônica*

$$\begin{array}{rcl} \pi : M & \longrightarrow & \dfrac{M}{N} \\ x & \longmapsto & \overline{x} = x + N \end{array}$$

é um A-homomorfismo.

Com efeito, considere $m_1, m_2 \in M$ e $\alpha \in A$ quaisquer. Assim, tem-se:

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

Logo, π é um A-homomorfismo. Como π é sobrejetora, concluimos que π é um A-epimorfismo.

Definição 1.3.8. *Seja $f : M \to N$ um A-homomorfismo.*

a) O subconjunto de M definido por $Ker(f) = \{m \in M;\ f(m) = 0_N\}$ é denominado o kernel ou núcleo do A-homomorfismo f.

b) O subconjunto de N definido por $Im(f) = \{f(m), m \in M\}$ é chamado de imagem do A-homomorfismo f.

c) Se $X \subset M$, então $f(X) = \{f(x); x \in X\}$ é chamado de imagem direta de X por f.

d) Se $Y \subset N$, então $f^{-1}(Y) = \{m \in M; f(m) \in Y\}$ é denominado imagem inversa de Y por f.

Proposição 1.3.9. *Seja $f : M \to N$ um A-homomorfismo. Então:*

a) $Ker(f) = f^{-1}(0_N)$ *é um submódulo do* A*-módulo* M*.*

Demonstração. De fato,

I) $0_M \in Ker(f)$, pois $f(0_M) = 0_N$

II) Dados m_1, $m_2 \in Ker(f)$, tem-se $f(m_1) = f(m_2) = 0_N$, o que implica que $0_N = f(m_1) - f(m_2) = f(m_1 - m_2)$, ou seja, $m_1 - m_2 \in Ker(f)$.

III) Dados $m \in Ker(f)$ e $a \in A$, segue que $f(am) = af(m) = a0_N = 0_N$, o que implica que $am \in Ker(f)$.

Portanto $Ker(f) = f^{-1}(0_N)$ é um submódulo do A-módulo M. □

b) $Im(f) = f(M)$ *é um submódulo do* A*-módulo* N*.*

Demonstração. Com efeito,

I) $0_N \in Im(f)$, pois $0_N = f(0_M)$.

II) Dados n_1, $n_2 \in Im(f)$, existem m_1, $m_2 \in M$ tais que $f(m_1) = n_1$ e $f(m_2) = n_2$. Desta forma, $n_1 - n_2 = f(m_1) - f(m_2) = f(m_1 - m_2)$, ou seja, $n_1 - n_2 \in Im(f)$.

III) Dados $n \in Im(f)$ e $a \in A$, existe $m \in M$ tal que $f(m) = n$. Deste modo, $an = af(m) = f(am)$, ou seja, $an \in Im(f)$.

Portanto, $Im(f)$ é um submódulo do A-módulo N. □

c) f *é um* A*-monomorfismo se, e somente se,* $Ker(f) = \{0_M\}$*.*

Demonstração. Suponha que f seja um A-monomorfismo e $m \in Ker(f)$ arbitrário. Assim, $f(m) = 0_N = f(0_M)$. Como f é injetora, segue que $m = 0_M$. Logo, $Ker(f) = \{0_M\}$.

Reciprocamente, suponha que $Ker(f) = \{0_M\}$. Sejam m_1, $m_2 \in M$ tais que $f(m_1) = f(m_2)$. Assim, $f(m_1 - m_2) = f(m_1) - f(m_2) = 0_N$, o que implica que $m_1 - m_2 \in Ker(f) = \{0_M\}$, ou seja, $m_1 - m_2 = 0_M$ e, consequentemente, $m_1 = m_2$. Logo, f é um A-monomorfismo. □

d) Se N' *é um submódulo do* A*-módulo* N*, então* $f^{-1}(N')$ *é um submódulo do* A*-módulo* M *e* $Ker(f) \subset f^{-1}(N')$*.*

Demonstração. De fato,

I) $0_M \in f^{-1}(N')$, pois $f(0_M) = 0_N \in N'$.

II) Dados m_1, $m_2 \in f^{-1}(N')$ quaisquer, existem n_1, $n_2 \in N'$ tais que $f(m_1) = n_1$ e $f(m_2) = n_2$. Como $f(m_1 - m_2) = f(m_1) - f(m_2) = n_1 - n_2 \in N'$, segue que $m_1 - m_2 \in f^{-1}(N')$.

III) Dados $m \in f^{-1}(N')$ e $a \in A$, existe $n \in N'$ tal que $f(m) = n$. Assim, $f(am) = af(m) = an \in N'$, o que implica em $am \in f^{-1}(N')$.

Por outro lado, tome $m \in Ker(f)$ arbitrário. Assim, $f(m) = 0_N \in N'$, o que implica que $m \in f^{-1}(N')$. Como $m \in Ker(f)$ é arbitrário, segue que $Ker(f) \subset f^{-1}(N')$. Portanto, $f^{-1}(N')$ é um submódulo do A-módulo M e $Ker(f) \subset f^{-1}(N')$. □

e) Se M' é um submódulo do A-módulo M, então $f(M')$ é um submódulo do A-módulo de N.

Demonstração. Com efeito,

I) $0_N \in f(M')$, pois $0_M \in M'$ e $f(0_M) = 0_N$.

II) Dados n_1, $n_2 \in f(M')$, existem m_1, $m_2 \in M'$ tais que $f(m_1) = n_1$ e $f(m_2) = n_2$. Assim, $n_1 - n_2 = f(m_1) - f(m_2) = f(m_1 - m_2)$. Como $m_1 - m_2 \in M'$, segue que $n_1 - n_2 \in f(M')$.

III) Dados $a \in A$ e $n \in f(M')$, existe $m \in M'$ tal que $f(m) = n$. Como $am \in M'$ e $an = af(m) = f(am)$, segue que $an \in f(M')$.

Portanto, $f(M')$ é um submódulo do A- módulo N. □

f) Se M' é um submódulo do A-módulo M, então $f^{-1}(f(M')) = M' + Ker(f)$.

Demonstração. Tome $m_1 \in f^{-1}(f(M'))$ arbitrário. Assim, $f(m_1) \in f(M')$, o que implica que existe $m_2 \in M'$ tal que $f(m_1) = f(m_2)$. Desta forma,

$$\begin{aligned} f(m_1 - m_2) &= f(m_1) - f(m_2) \\ &= 0_N. \end{aligned}$$

Desta forma, $m_1 - m_2 \in Ker(f)$. Sabendo que $m_1 = m_2 + (m_1 - m_2)$, segue que $m_1 \in M' + Ker(f)$. Como $m_1 \in f^{-1}(f(M'))$, segue que $f^{-1}(f(M')) \subset M' + Ker(f)$.

Reciprocamente, tome $m \in M' + Ker(f)$ arbitrário. Assim, existem $m_1 \in M'$ e $k_1 \in Ker(f)$ tais que $m = m_1 + k_1$, o que implica que

$$\begin{aligned} f(m) &= f(m_1 + k_1) \\ &= f(m_1) + f(k_1) \\ &= f(m_1). \end{aligned}$$

Deste modo, $f(m) = f(m_1) \in f(M')$, o que implica que $m \in f^{-1}(f(M'))$. Logo $M' + Ker(f) \subset f^{-1}(f(M'))$ e, portanto, $f^{-1}(f(M')) = M' + Ker(f)$. □

g) Se N' é um submódulo do A-módulo N, então $f(f^{-1}(N')) = N' \cap Im(f)$.

Demonstração. Tome $n \in f(f^{-1}(N'))$ arbitrário. Assim, existe $m \in f^{-1}(N')$ tal que $n = f(m)$. De $m \in f^{-1}(N')$, tem-se $n = f(m) \in N'$. Como $n \in N'$ e $n \in Im(f)$, segue que $n \in N' \cap Im(f)$ e, consequentemente, $f(f^{-1}(N')) \subset N' \cap Im(f)$.

Por outro lado, tome $n \in N' \cap Im(f)$ qualquer. Desta forma, $n \in N'$ e $n \in Im(f)$. Como $n \in Im(f)$, existe $m \in M$ tal que $f(m) = n$. De $f(m) = n \in N'$, segue que $m \in f^{-1}(N')$, o que implica em $n = f(m) \in f(f^{-1}(N'))$, ou seja, $N' \cap Im(f) \subset f(f^{-1}(N'))$. Portanto, $f(f^{-1}(N')) = N' \cap Im(f)$. □

Definição 1.3.10. *O diagrama (Triângulo) de A-módulos e A-homomorfismos abaixo é dito comutativo se $h \circ f = g$.*

$$\begin{array}{ccc} M & \xrightarrow{g} & N \\ {\scriptstyle f}\downarrow & \nearrow_{h} & \\ P & & \end{array}$$

Definição 1.3.11. *O diagrama (Quadrado) de A-módulos e A-homomorfismos abaixo é dito comutativo se $g \circ \alpha = \beta \circ f$.*

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \alpha}\downarrow & & \downarrow{\scriptstyle \beta} \\ M' & \xrightarrow[g]{} & N' \end{array}$$

Definição 1.3.12. *O diagrama de A-módulos e A-homomorfismos abaixo é dito comutativo se cada um dos quadrados é comutativo, isto é, $f' \circ \alpha = \beta \circ f$ e $g' \circ \beta = \gamma \circ g$.*

$$\begin{array}{ccccc} M & \xrightarrow{f} & N & \xrightarrow{g} & P \\ {\scriptstyle \alpha}\downarrow & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\ M' & \xrightarrow[f']{} & N' & \xrightarrow[g']{} & P' \end{array}$$

Proposição 1.3.13. *Sejam M, N e P A-módulos, $g : M \to N$ um A-homomorfismo e $f : M \to P$ um A-epimorfismo. Existe um único A-homomorfismo $h : P \to N$ tal que $h \circ f = g$ se, e somente se, $Ker(f) \subset Ker(g)$. Além disso, h é um A-monomorfismo se, e somente se, $Ker(f) = Ker(g)$.*

$$\begin{array}{ccc} M & \xrightarrow{g} & N \\ {\scriptstyle f}\big\downarrow & & \\ P & & \end{array}$$

Demonstração. Suponha que exista um único A-homomorfismo $h : P \to N$ tal que $h \circ f = g$. Tome $x \in Ker(f)$ qualquer. Assim,

$$\begin{aligned} g(x) &= (h \circ f)(x) \\ &= h(f(x)) \\ &= h(0_p) \\ &= 0_N, \end{aligned}$$

o que implica que $x \in Ker(g)$. Logo, $Ker(f) \subset Ker(g)$.

Reciprocamente, suponha que $Ker(f) \subset Ker(g)$. Sejam $x, y \in M$ quaisquer tais que $f(x) = f(y)$. Desta forma, $f(x - y) = f(x) - f(y) = 0_p$, o que implica que $x - y \in Ker(f) \subset Ker(g)$. Logo, $g(x - y) = 0_N$, ou seja, $g(x) = g(y)$.

Considere o conjunto $G = \{(y, z);\ y = f(m) \text{ e } z = g(m), \text{ para algum } m \in M\}$. Note que $G \subset Im(f) \times Im(g)$ e $G \neq \emptyset$, pois para cada $x \in M$, tem-se que $(f(x), g(x)) \in G$.

Afirmação: Para cada $y \in Im(f)$, existe um único $z \in N$ tal que $(y, z) \in G$.

De fato, seja $y \in Im(f)$ qualquer. Assim, existe $x \in M$ tal que $y = f(x)$. Tome $z = g(x)$. Desta forma, $(y, z) \in G$. Suponha que exista $(y, z') \in G$, para algum $z' \in N$. Pela definição de G, existe $x' \in M$ tal que $y = f(x) = f(x')$ e $z' = g(x')$. Como $f(x) = f(x')$, segue que $g(x) = g(x')$ e, consequentemente, $z = z'$.

Deste modo, considere a aplicação $\phi : Im(f) \to N$, dada por $\phi(f(x)) = g(x)$. Da afirmação anterior, segue que a aplicação ϕ está bem definida e, como f é um A-epimorfismo, tem-se $Im(f) = P$. Considere $h = \phi$. Desta forma, para cada $x \in M$, $(h \circ f)(x) = h(f(x)) = \phi(f(x)) = g(x)$, ou seja, $h \circ f = g$. Como f é sobrejetora, então a aplicação h é única, pois se $h_1 : P \to N$ é um A-homomorfismo tal que $h_1 \circ f = g$, então

$h_1 \circ f = h \circ f$. Além disso, f admite uma inversa à direita $f_1 : P \to N$. Deste modo,

$$\begin{aligned}(h_1 \circ f) \circ f_1 &= (h \circ f) \circ f_1 \\ h_1 \circ (f \circ f_1) &= h \circ (f \circ f_1) \\ h_1 \circ Id_P &= h \circ Id_P \\ h_1 &= h.\end{aligned}$$

Por outro lado, h é um A-homomorfismo, pois dados $y, y' \in P = Im(f)$ e $\alpha \in A$ quaisquer, existem $x, x' \in M$ tais que $f(x) = y$ e $f(x') = y'$. Assim,

$$\begin{aligned}h(\alpha y + y') = h(\alpha f(x) + f(x')) &= h(f(\alpha x + x')) \\ &= (h \circ f)(\alpha x + x') \\ &= g(\alpha x + x') \\ &= \alpha g(x) + g(x') \\ &= \alpha(h \circ f)(x) + (h \circ f)(x') \\ &= \alpha h(f(x)) + h(f(x')) = \alpha h(y) + h(y').\end{aligned}$$

Portanto, existe um único A-homorfismo $h : P \to N$ tal que $h \circ f = g$.

Por fim, suponha que h seja um A-monomorfismo. Assim, $Ker(f) \subset Ker(g)$. Tome $x \in Ker(g)$ qualquer. Desta forma, $0_N = g(x) = (h \circ f)(x) = h(f(x))$, o que implica em $f(x) \in Ker(h) = \{0_P\}$, ou seja, $x \in Ker(f)$. Logo, $Ker(g) \subset Ker(f)$ e, concluímos que $Ker(f) = Ker(g)$.

Reciprocamente, tome $y = f(x) \in Ker(h)$. Assim,

$$0_N = h(y) = h(f(x)) = (h \circ f)(x) = g(x),$$

o que implica que $g(x) = 0_N$. Desta forma, $x \in Ker(g) = Ker(f)$, ou seja, $y = f(x) = 0_P$. Logo, h é um A-monomorfismo. □

Teorema 1.3.14. *Sejam M, N A-módulos e $f : M \to N$ um A-homomorfismo. Se F e H são submódulos dos A-módulos M e N, respectivamente, então $f(F) \subset H$ se, e somente se, existe um único A-homomorfismo $\tilde{f} : \frac{M}{F} \to \frac{N}{H}$ tal que o diagrama*

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \pi_F}\downarrow & & \downarrow{\scriptstyle \pi_H} \\ \frac{M}{F} & \xrightarrow{\tilde{f}} & \frac{N}{H} \end{array}$$

é comutativo. Além disso, se $\tilde{f}$ *existir, segue que:*

a) $\tilde{f}$ *é um A-monomorfismo se, e somente se,* $F = f^{-1}(H)$*;*

b) $\tilde{f}$ *é um A-epimorfismo se, e somente se,* $N = H + Im(f)$*.*

Demonstração. Considere o diagrama

$$\begin{array}{ccc} M & \xrightarrow{\pi_H \circ f} & \frac{N}{H} \\ {\scriptstyle \pi_F}\downarrow & & \\ \frac{M}{F} & & \end{array}$$

Notemos que π_F é um A-epimorfismo e $Ker(\pi_F) = F \subset Ker(\pi_H \circ f)$. Pela Proposição 1.3.13 , existe um único A-homomorfismo $\tilde{f} : \frac{M}{F} \to \frac{N}{H}$, tal que $\tilde{f} \circ \pi_F = \pi_H \circ f$.

Reciprocamente, tome $m' \in F$ qualquer. Como o diagrama

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \pi_F}\downarrow & & \downarrow{\scriptstyle \pi_H} \\ \frac{M}{F} & \xrightarrow[\tilde{f}]{} & \frac{N}{H} \end{array}$$

é comutativo, então $(\tilde{f} \circ \pi_F)(m') = (\pi_H \circ f)(m')$. Assim, $\pi_H(f(m')) = \tilde{f}(\pi_F(m')) = \overline{0_M}$, o que implica que $f(m') \in Ker(\pi_H) = H$. Desta forma, $f(m') \in H$. Como $m' \in F$ é arbitrário, concluímos que $f(F) \subset H$.

a) Suponha que $\tilde{f}$ seja um A-monomorfismo. Pela primeira parte do teorema, segue que $f(F) \subset H$, ou seja, $F \subset f^{-1}(H)$.
Por outro lado, tome $c \in f^{-1}(H)$ qualquer. Assim, $f(c) \in H$ e daí

$$\begin{aligned} \tilde{f}(\pi_F(c)) &= (\tilde{f} \circ \pi_F)(c) \\ &= (\pi_H \circ f)(c) \\ &= \pi_H(f(c)) = \overline{0_N}. \end{aligned}$$

Desta forma, $\pi_F(c) = \overline{0_M}$, o que implica que $c \in F$. Assim, $f^{-1}(H) \subset F$. Portanto, $f^{-1}(H) = F$.

Reciprocamente, suponha que $f^{-1}(H) = F$. Tome $\overline{m} \in Ker(\tilde{f})$. Assim,

$$\begin{aligned} \pi_H(f(m)) &= (\pi_H \circ f)(m) \\ &= (\tilde{f} \circ \pi_F)(m) \\ &= \tilde{f}(\overline{m}) \\ &= \overline{0_N}. \end{aligned}$$

Assim, $f(m) \in Ker(\pi_H) = H$, o que implica que $m \in f^{-1}(H) = F$. Logo $\overline{m} = \overline{0_M}$ e, consequentemente, $Ker(\tilde{f}) = \{\overline{0_N}\}$. Portanto, $\tilde{f}$ é um A-monomorfismo.

b) Suponha que $\tilde{f}$ seja um A-epimorfismo e tome $n \in N$ qualquer. Assim, existe $m \in M$ tal que $\tilde{f}(\overline{m}) = \overline{n}$. Daí,

$$\begin{aligned} \overline{n} &= \tilde{f}(\overline{m}) \\ &= (\tilde{f} \circ \pi_F)(m) \\ &= (\pi_H \circ f)(m) \\ &= \overline{f(m)}. \end{aligned}$$

Desta forma, $n - f(m) = n' \in H$, o que implica que $n = n' + f(m) \in H + Im(f)$. Logo, $N \subset H + Im(f)$. Como $H \subset N$ e $Im(f) \subset N$, segue que $H + Im(f) \subset N$. Portanto, $N = H + Im(f)$.

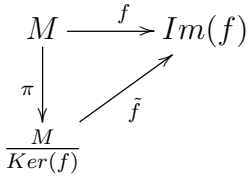
Reciprocamente, suponha que $N = H + Im(f)$. Tome $\overline{n} \in \dfrac{N}{H}$ qualquer. Assim, existem $h \in H$ e $m \in M$ tais que $n = h + f(m)$. Assim,

$$\begin{aligned} \tilde{f}(\overline{m}) &= \tilde{f}(\pi_F(m)) \\ &= (\tilde{f} \circ \pi_F)(m) \\ &= (\pi_H \circ f)(m) \\ &= \pi_H(f(m)) \\ &= \overline{f(m)} \\ &= \overline{n - h} \\ &= \overline{n}. \end{aligned}$$

Logo, $\tilde{f}$ é um A-epimorfismo.

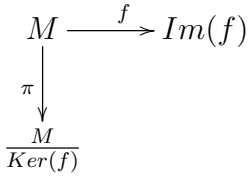
□

Teorema 1.3.15 (1º Teorema do Isomorfismo)**.** *Seja $f : M \to N$ um A-homomorfismo. Então existe um único A-isomorfismo $\tilde{f} : \frac{M}{Ker(f)} \to Im(f)$, de modo que o diagrama abaixo seja comutativo.*



Apresentaremos a seguir duas demonstrações para o teorema.

Demonstração 1: Considere o diagrama abaixo, onde π é a projeção canônica.



Como π é um A-epimorfismo e $Ker(f) = Ker(\pi)$, em particular, $Ker(\pi) \subset Ker(f)$. Pela Proposição 1.3.13, existe um único A-homomorfismo $\tilde{f} : \frac{M}{Ker(f)} \to Im(f)$ tal que $\tilde{f} \circ \pi = f$.

Afirmação: $\tilde{f}$ é um A-isomorfismo.

Com efeito, como $Ker(f) = Ker(\pi)$, pela Proposição 1.3.13, $\tilde{f}$ é um A-monomorfismo. Por outro lado, tome $f(m) \in Im(f)$. Assim, $f(m) = (\tilde{f} \circ \pi)(m) = \tilde{f}(\pi(m))$, o que implica que $f(m) \in Im(\tilde{f})$. Logo, $\tilde{f}$ é um A-epimorfismo. Portanto, $\tilde{f}$ é um A-isomorfismo.

Demonstração 2: Considere $\tilde{f} : \frac{M}{Ker(f)} \to Im(f)$ dada por $\tilde{f}(\overline{m}) = f(m)$.

Afirmação 1: f está bem definida.
De fato, $\overline{m} = \overline{n}$, implica em $m - n \in Ker(f)$, ou seja, $f(m - n) = 0_N$. Como f é um A-homomorfismo, tem-se $f(m) = f(n)$ e, consequentemente, $\tilde{f}(\overline{m}) = \tilde{f}(\overline{n})$.

Afirmação 2: $\tilde{f}$ é um A-isomorfismo.
Com efeito, dados $\alpha \in A$ e $\overline{m}$, $\overline{n} \in \frac{M}{Ker(f)}$ quaisquer, tem-se

$$\begin{aligned} \tilde{f}(\alpha\overline{m} + \overline{n}) = \tilde{f}(\overline{\alpha m} + \overline{n}) &= \tilde{f}(\overline{\alpha m + n}) \\ &= f(\alpha m + n) \\ &= \alpha f(m) + n = \alpha\tilde{f}(\overline{m}) + \tilde{f}(\overline{n}). \end{aligned}$$

Logo, $\tilde{f}$ é um A-homomorfismo.

Tome $\overline{m} \in Ker(\tilde{f})$ arbitrário. Assim, $f(m) = (\tilde{f} \circ \pi)(m) = \tilde{f}(\pi(m)) = \tilde{f}(\overline{m}) = 0_N$, ou seja, $m \in Ker(f)$. Desta forma, $\overline{m} = \overline{0_M}$, o que implica em $Ker(\tilde{f}) = \{\overline{0_M}\}$. Logo, $\tilde{f}$ é um A-monomorfismo. Por outro lado, $\tilde{f}$ é claramente um A-epimorfismo e, portanto, $\tilde{f}$ é um A-isomorfismo.

Seja $g : \frac{M}{Ker(f)} \to Im(f)$ um A-isomorfismo tal que $g \circ \pi = f$. Desta forma, dado $\overline{m} \in \frac{M}{Ker(f)}$ qualquer, tem-se

$$\begin{aligned} g(\overline{m}) &= g(\pi(m)) \\ &= (g \circ \pi)(m) \\ &= f(m) \\ &= (\tilde{f} \circ \pi)(m) \\ &= \tilde{f}(\pi(m)) \\ &= \tilde{f}(\overline{m}) \end{aligned}$$

Logo, $g = \tilde{f}$.

Corolário 1.3.16. *Se $f : M \to N$ um A-homomorfismo, então $\frac{M}{Ker(f)} \cong Im(f)$.*

Corolário 1.3.17 (Decomposição canônica)**.** *Todo A-homomorfismo $f : M \to N$ pode ser expresso como a composição de um A-epimorfismo, um A-isomorfismo e um A-monomorfismo.*

Demonstração. Considere o diagrama a seguir, onde π_1 é a projeção canônica e i é a inclusão.

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \pi_1}\downarrow & & \uparrow{\scriptstyle i} \\ \frac{M}{Ker(f)} & \xrightarrow[\tilde{f}]{} & Im(f) \end{array}$$

Observe que $f = i \circ \tilde{f} \circ \pi_1$, onde π_1 é um A-epimorfismo, $\tilde{f}$ é um A-isomorfismo e i é um A-monomorfismo. □

Corolário 1.3.18. *M é um A-módulo cíclico se, e somente se, $M \cong \dfrac{A}{I}$, onde I é um ideal à esquerda de A.*

Demonstração. Seja $m \in M$ tal que $M = ((m))$. Considere $\psi : A^A \to M$ um A-homomorfismo dado por $\psi(a) = am$. Observe que ψ é claramente um A-epimorfismo e, pelo Teorema 1.3.15, tem-se $\frac{A^A}{Ker(\psi)} \cong Im(\psi) = M$. Reciprocamente, suponha que $\frac{A}{I} \cong M$, sendo I é um ideal de A. Como $\frac{A}{I}$ é um A-módulo gerado por $\overline{1_A}$, segue que M é um A-módulo cíclico. □

Definição 1.3.19. *Diremos que um A-módulo N é uma imagem holomorfa de um A-módulo M, se existe um A-epimorfismo de M em N.*

Proposição 1.3.20. *Sejam M e N A-módulos. Se N é uma imagem holomorfa de M, então existe um submódulo M' do A-módulo M tal que $N \cong \frac{M}{M'}$. Reciprocamente, para cada submódulo M' do A-módulo M, o A-módulo quociente $\frac{M}{M'}$ é uma imagem holomorfa de M.*

Demonstração. Sejam $f : M \to N$ um A-epimorfismo e $M' = Ker(f)$. Pelo Teorema 1.3.15 segue que $\frac{M}{Ker(f)} \cong Im(f)$, ou seja, $\frac{M}{M'} \cong N$. A recíproca é consequência da projeção canônica $\pi : M \to \frac{M}{M'}$. □

Teorema 1.3.21 (Teorema da Correspondência)**.** *Seja $f : M \to N$ um A-epimorfismo. Existe uma correspondência bijetiva entre os submódulos de M que contém o $Ker(f)$ e os submódulos de N.*

Demonstração. Considere os conjuntos

$$F_1 = \{M'; M' \text{ é um submódulo do } A\text{-módulo } M \text{ que contém } Ker(f)\}$$

$$F_2 = \{N'; N' \text{ é um submódulo do } A\text{-módulo } N\}.$$

Seja $\psi : F_1 \to F_2$ dada por $\psi(M') = f(M')$. Tome M_1', $M_2' \in F_1$ arbitrários tais que $\psi(M_1') = \psi(M_2')$. Assim, $f(M_1') = f(M_2')$, o que implica que $f^{-1}(f(M_1')) = f^{-1}(f(M_2'))$ e, consequentemente, $M_1' + Ker(f) = M_2' + Ker(f)$. Como $Ker(f) \subset M_1'$ e $Ker(f) \subset M_2'$, segue que $M_1' = M_2'$ e, concluímos que ψ é injetora.

Por outro lado, tome $N' \in F_2$ qualquer. Pela Proposição 1.3.9, item (d), $f^{-1}(N')$ é um submódulo do A-módulo M que contém $Ker(f)$. Assim, $f^{-1}(N') \in F_1$ e $f(f^{-1}(N')) = N' \cap Im(f)$. Como f é um A-epimorfismo, resulta que $f(f^{-1}(N')) = N'$, o que implica em $\psi(f^{-1}(N')) = N'$. Logo ψ é sobrejetora e, portanto, segue que ψ é bijetora. □

Corolário 1.3.22. *Sejam M um A-módulo e M_1 um submódulo de M. Então existe uma correspondência bijetiva entre F_1 e F_2, sendo*

$$F_1 = \{F;\ F \text{ é um submódulo de } M \text{ tal que } M_1 \subset F\}$$

$$F_2 = \{L;\ L \text{ é um submódulo de } \tfrac{M}{M_1}\}.$$

Demonstração. Uma vez que a projeção canônica $\pi : M \to \frac{M}{M_1}$ é um A-epimorfismo e $Ker(\pi) = M_1$, então pelo Teorema 1.3.21, segue o resultado pretendido. □

Corolário 1.3.23. *Seja M um A-módulo e M' um submódulo de M. Todo submódulo do A-módulo $\frac{M}{M'}$ é da forma $\frac{F}{M'}$, onde F é um submódulo de M que contém M'.*

Demonstração. Considere a projeção canônica $\pi : M \to \frac{M}{M'}$. Como π é um A-epimorfismo, pelo Corolário 1.3.22, existe uma correspondência bijetiva entre F_1 e F_2, sendo

$$F_1 = \{F;\ F \text{ é um submódulo de } M \text{ tal que } M' \subset F\}$$

$$F_2 = \{L;\ L \text{ é um submódulo de } \tfrac{M}{M'}\}.$$

Seja $\psi : F_1 \to F_2$ tal bijeção. Deste modo, dado $L \in F_2$ qualquer, existe um único $F \in F_1$ tal que $\psi(F) = L$. Pelo Teorema 1.3.21, $\psi = \pi$ e $L = \psi(F) = \pi(F) = \frac{F}{M'}$. □

Exemplo 1.3.24. *Se $n \mid m$, então existe um $\mathbb{Z}$-homomorfismo $\psi : \mathbb{Z}_m \to \mathbb{Z}_n$.*

Demonstração. Considere $\pi : \mathbb{Z} \to \mathbb{Z}_n$, o $\mathbb{Z}$-homomorfismo dado por $\psi(r) = \overline{r}$. De $n \mid m$ tem-se $m\mathbb{Z} \subset n\mathbb{Z} = Ker(\pi)$. Considere o diagrama abaixo, onde π_1 é a projeção canônica.

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\ \pi\ } & \mathbb{Z}_n \\ {\scriptstyle \pi_1}\downarrow & & \\ \frac{\mathbb{Z}}{m\mathbb{Z}} & & \end{array}$$

Como π_1 é um $\mathbb{Z}$-epimorfismo tal que $Ker(\pi_1) = m\mathbb{Z} \subset n\mathbb{Z} = Ker(\pi)$, então pela Proposição 1.3.13, existe um único $\mathbb{Z}$-homomorfismo $f : \frac{\mathbb{Z}}{m\mathbb{Z}} \to \mathbb{Z}_n$ tal que $f \circ \pi_1 = \pi$. Por outro lado, como $\mathbb{Z}_m = \frac{\mathbb{Z}}{m\mathbb{Z}}$, existe um A-isomorfismo $g : \mathbb{Z}_m \to \frac{\mathbb{Z}}{m\mathbb{Z}}$. Deste modo, $\psi = f \circ g : \mathbb{Z}_m \to \mathbb{Z}_n$ é um A-homomorfismo. □

Teorema 1.3.25 (2º Teorema do Isomorfismo)**.** *Se F e H são submódulos de um A-módulo M, então $\frac{F+H}{H} \cong \frac{F}{F \cap H}$.*

Demonstração. É de fácil verificação que H e $F \cap H$ são submódulos dos A-módulos $F+H$ e F, respectivamente. Considere o diagrama abaixo, onde π_1 e π_2 são projeções canônicas e i é a aplicação de inclusão.

$$\begin{array}{ccc} F & \xrightarrow{\ i\ } & F+H \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ \frac{F}{F\cap H} & & \frac{F+H}{H} \end{array}$$

Como $i(F \cap H) = F \cap H \subset H$, pelo Teorema 1.3.14, existe um único A-homomorfismo $\theta : \frac{F}{F\cap H} \to \frac{F+H}{H}$, que comuta o diagrama. Como $i^{-1}(H) = F \cap H$ e $F+H = Im(i)+H$, pelo Teorema 1.3.14, itens (a) e (b), concluímos que θ é um A-isomorfismo e, consequentemente, $\frac{F}{F\cap H} \cong \frac{F+H}{H}$. □

Teorema 1.3.26 (3º Teorema do Isomorfismo)**.** *Sejam F e H submódulos do A-módulo M. Se $F \subset H$, então* $\dfrac{\frac{M}{F}}{\frac{H}{F}} \cong \dfrac{M}{H}$.

Demonstração. Pelo Teorema 1.3.21 e seus corolários, os submódulos do A-módulo $\frac{M}{F}$ são da forma $\frac{L}{F}$, onde L é um submódulo de M, que contém F. Deste modo, $\frac{H}{F}$ é um submódulo de $\frac{M}{F}$. Considere o diagrama abaixo, onde π é a projeção canônica e $f : \frac{M}{F} \to \frac{M}{H}$ é o A-epimorfismo definido por $f(m+F) = m+H$.

$$\begin{array}{ccc} \frac{M}{F} & \xrightarrow{\ f\ } & \frac{M}{H} \\ {\scriptstyle \pi}\downarrow & \nearrow_{\tilde{f}} & \\ \frac{\frac{M}{F}}{\frac{H}{F}} & & \end{array}$$

Como $Ker(\pi) = \frac{H}{F} = Ker(f)$ e π é um A-epimorfismo, então pela Proposição 1.3.13, existe um único $\tilde{f} : \frac{\frac{M}{F}}{\frac{H}{F}} \to \frac{M}{H}$ A-monomorfismo que comuta o diagrama. Por outro lado, dado $m+H \in \frac{M}{H}$ qualquer, tem-se que

$$\begin{aligned} m+H &= f(m+F) \\ &= (\tilde{f} \circ \pi)(m+F) \\ &= \tilde{f}(\pi(m+F)), \end{aligned}$$

o que implica que $\tilde{f}$ é um A-epimorfismo. Portanto, $\tilde{f}$ é um A-isomorfismo e, consequentemente, $\dfrac{\frac{M}{F}}{\frac{H}{F}} \cong \dfrac{M}{H}$. □

Exemplo 1.3.27. *Determine as imagens holomorfas do $\mathbb{Z}$-módulo $\mathbb{Z}_{12}$.*

Demonstração. Seja M uma imagem holomorfa do $\mathbb{Z}$-módulo $\mathbb{Z}_{12}$. Assim, pela Proposição

1.3.20, existe um submódulo F do $\mathbb{Z}$-módulo $\mathbb{Z}_{12}$ tal que $M \cong \frac{\mathbb{Z}_{12}}{F}$. Por outro lado, pelo Corolário 1.3.23, todo submódulo do $\mathbb{Z}$-módulo $\mathbb{Z}_{12}$ é da forma $\frac{n\mathbb{Z}}{12\mathbb{Z}}$, para $n \in \mathbb{Z}$ tal que $12\mathbb{Z} \subset n\mathbb{Z}$. Logo, $n \in \{1, 2, 3, 4, 6, 12\}$. Pelo Teorema 1.3.26, segue que

$$M \cong \frac{\mathbb{Z}_{12}}{F} = \frac{\frac{\mathbb{Z}}{12\mathbb{Z}}}{\frac{n\mathbb{Z}}{12\mathbb{Z}}} \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_n.$$

Deste modo,

$$M \cong \{\overline{0}\},\ M \cong \mathbb{Z}_2,\ M \cong \mathbb{Z}_3,\ M \cong \mathbb{Z}_4,\ M \cong \mathbb{Z}_6 \text{ ou } M \cong \mathbb{Z}_{12}.$$

□

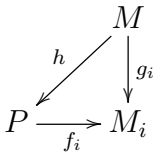
1.4 Produtos

Dados M_1 e M_2 A-módulos quaisquer, definiremos uma nova estrutura de A-módulo em $M_1 \times M_2$ utilizando as operações $+ : (M_1 \times M_2) \times (M_1 \times M_2) \to M_1 \times M_2$ e $\cdot : A \times (M_1 \times M_2) \to M_1 \times M_2$ dadas por

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

para todo $a_1,\ a_2 \in M_1,\ b_1,\ b_2 \in M_2$ e $\alpha \in A$. Naturalmente podemos associar ao A-módulo $M_1 \times M_2$ os A-epimorfismos $\pi_1 : M_1 \times M_2 \to M_1$, $\pi_2 : M_1 \times M_2 \to M_2$, dados por $\pi_1(a_1, b_1) = a_1$ e $\pi_2(a_1, b_1) = b_1$. Estenderemos o conceito do produto $M_1 \times M_2$ para uma família $(M_i)_{i\in I}$ de A-módulos, onde I é um conjunto qualquer.

Definição 1.4.1. *Seja $(M_i)_{i\in I}$ uma família de A-módulos. Chamamos de módulo-produto ou simplesmente de produto da família $(M_i)_{i\in I}$, o A-módulo P juntamente com uma família $(f_i)_{i\in I}$ de A-homomorfismos $f_i : P \to M_i$, tal que para todo A-módulo M e toda família $(g_i)_{i\in I}$ de A-homomorfismos $g_i : M \to M_i$, existe um único A-homomorfismo $h : M \to P$ que torna comutativo o diagrama abaixo, para todo $i \in I$.*



Denotaremos o módulo-produto por $(P, (f_i)_{i\in I})$.

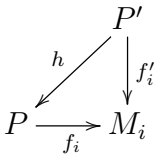
Teorema 1.4.2. *Se $(P, (f_i)_{i\in I})$ é um produto da família de A-módulos $(M_i)_{i\in I}$, então cada f_i é um A-epimorfismo.*

Demonstração. Fixe $i \in I$ qualquer e considere $M = M_i$, $g_i = Id_{M_i}$ e $g_j = 0$, para $i \neq j$. Assim, existe um único A-homomorfismo $h : M_i \to P$ tal que $f_j \circ h = g_j$, para todo $j \in I$. Em particular, $f_i \circ h = g_i = Id_{M_i}$. Logo, f_i admite uma inversa à direita, o que implica que f_i é um A-epimorfismo. □

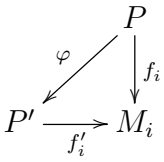
Teorema 1.4.3 (Unicidade do Produto)**.** *Seja $(P, (f_i)_{i\in I})$ um produto da família de A-módulos $(M_i)_{i\in I}$. Então $(P', (f'_i)_{i\in I})$ é um produto dessa família se, e somente se, existe um único A-isomorfismo $h : P' \to P$ tal que $f_i \circ h = f'_i$, para todo $i \in I$.*

Demonstração. Suponha que $(P', (f'_i)_{i\in I})$ seja um produto da família de A-módulos

$(M_i)_{i\in I}$. Como $(P,(f_i)_{i\in I})$ é um produto dessa família, então existe um único A-homomorfismo $h : P' \to P$, tal que o diagrama abaixo comuta, para todo $i \in I$.



Analogamente, como $(P',(f'_i)_{i\in I})$ é um produto da família de A-módulos $(M_i)_{i\in I}$, existe um único A-homomorfismo $\varphi : P \to P'$ tal que o diagrama abaixo comuta, para todo $i \in I$.



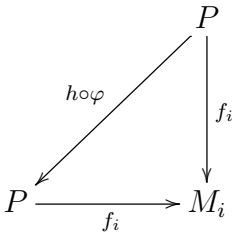
Como

$$\begin{aligned} f_i \circ (h \circ \varphi) &= (f_i \circ h) \circ \varphi \\ &= f'_i \circ \varphi \\ &= f_i, \end{aligned}$$

ou seja,

$$f_i \circ (h \circ \varphi) = f_i, \text{ para todo } i \in I,$$

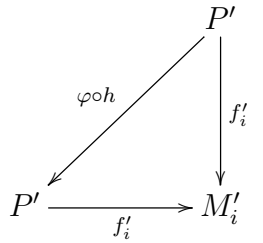
o que implica que o diagrama



é comutativo, para todo $i \in I$. No entanto, pela definição de produto, existe um único A-homomorfismo que comuta esse diagrama. Logo, $h \circ \varphi = Id_P$. Analogamente, como

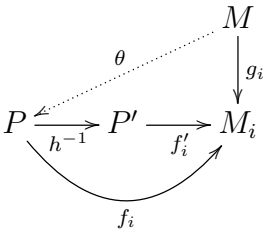
$$\begin{aligned} f'_i \circ (\varphi \circ h) &= (f'_i \circ \varphi) \circ h \\ &= f_i \circ h \\ &= f'_i, \end{aligned}$$

para todo $i \in I$, ou seja, $f'_i \circ (\varphi \circ h) = f'_i$, o que implica que o diagrama

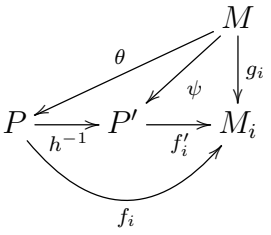


comuta para todo $i \in I$. No entanto, pela definição de produto, existe um único A-homomorfismo que comuta o último diagrama. Logo, $\varphi \circ h = Id_{P'}$. Assim, $\varphi \circ h = Id_{P'}$ e $h \circ \varphi = Id_P$, o que implica que $h : P \to P'$ é um A-isomorfismo tal que $f_i \circ h = f'_i$, para todo $i \in I$.

Reciprocamente, de $f_i \circ h = f'_i$, segue que $f_i = f'_i \circ h^{-1}$, para todo $i \in I$. Tome M um A-módulo qualquer e $(g_i)_{i \in I}$ uma família de A-homomorfismos $g_i : M \to M_i$. Considere o diagrama a seguir:



Como $(P, (f_i)_{i \in I})$ é um produto da família, existe um único A-homomorfismo $\theta : M \to P$ tal que $f_i \circ \theta = g_i$, para todo $i \in I$. Desta forma, considere $\psi = h^{-1} \circ \theta : M \to P'$ e o seguinte diagrama



Note que ψ é um A-homomorfismo tal que, para todo $i \in I$, tem-se

$$\begin{aligned} f'_i \circ \psi &= f'_i \circ (h^{-1} \circ \theta) \\ &= (f'_i \circ h^{-1}) \circ \theta \\ &= f_i \circ \theta \\ &= g_i. \end{aligned}$$

Seja $\varphi' : M \to P'$ um A-homomorfismo tal que $f'_i \circ \varphi' = g_i$, para todo $i \in I$. Assim, para todo $i \in I$, tem-se

$$\begin{aligned} g_i &= f_i' \circ \varphi' \\ &= f_i' \circ (Id_{P'} \circ \varphi') \\ &= f_i' \circ (h^{-1} \circ h) \circ \varphi' \\ &= (f_i' \circ h^{-1}) \circ (h \circ \varphi') \\ &= f_i \circ (h \circ \varphi'). \end{aligned}$$

Da unicidade do A-homomorfismo θ, segue que $h \circ \varphi' = \theta$, ou seja, $\varphi = h^{-1} \circ \theta = \psi$. Portanto, $(P', (f_i')_{i\in I})$ também é um produto da família de A-módulos $(M_i)_{i\in I}$. □

Com o intuito de provar a existência do produto de uma familia de A-módulos $(M_i)_{i\in I}$ qualquer, definiremos o produto direto de $(M_i)_{i\in I}$.

Definição 1.4.4. *Seja $(M_i)_{i\in I}$ uma família de A-módulos, onde I é um conjunto não vazio. O produto cartesiano desta família de A-módulos, o qual denotaremos por $\prod_{i\in I} M_i$, é definido como*

$$\prod_{i\in I} M_i = \{f : I \to \bigcup_{i\in I} M_i; f(i) \in M_i, \forall i \in I\}.$$

Denotaremos a imagem $f(i)$ por x_i, para todo $i \in I$. Portanto, os elementos do $\prod_{i\in I} M_i$ são da forma

$$\begin{aligned} f &= \{f(i); i \in I\} \\ &= \{x_i; i \in I\} \\ &= (x_i)_{i\in I}. \end{aligned}$$

Em $(M_i)_{i\in I}$, vamos considerar as seguintes operações:

i) Dados $f = (x_i)_{i\in I}$, $g = (y_i)_{i\in I} \in (M_i)_{i\in I}$, definimos

$$\begin{aligned} f + g &= (x_i)_{i\in I} + (y_i)_{i\in I} \\ &= (x_i + y_i)_{i\in I}. \end{aligned}$$

ii) Dados $f = (x_i)_{i\in I} \in (M_i)_{i\in I}$ e $\alpha \in A$, definimos

$$\begin{aligned} \alpha f &= \alpha(x_i)_{i\in I} \\ &= (\alpha x_i)_{i\in I}. \end{aligned}$$

É de fácil verificação que tais operações definem em $(M_i)_{i\in I}$ uma estrutura de A-módulo, denominada produto direto da família $(M_i)_{i\in I}$. Para cada $i \in I$, a projeção canônica $\pi_i : (M_i)_{i\in I} \to M_i$, dada por $\pi_i((x_i)_{i\in I}) = x_i$ é claramente um A-epimorfismo.

Teorema 1.4.5 (Existência do Produto)**.** *$(\prod_{i\in I} M_i, (\pi_i)_{i\in I})$ é um produto da família $(M_i)_{i\in I}$.*

Demonstração. Sejam M um A-módulo arbitrário e $(g_i)_{i\in I}$ uma família de A-homomorfismos $g_i : M \to M_i$, para todo $i \in I$. Definamos $h : M \to \prod_{i\in I} M_i$, dado por $h(x) = (g_i(x))_{i\in I}$. Observe que h é um A-homomorfismo, pois dados $x, y \in M$ e $\alpha \in A$ quaisquer, tem-se

$$\begin{aligned} h(\alpha x + y) &= (g_i(\alpha x + y))_{i\in I} \\ &= (\alpha g_i(x) + g(y))_{i\in I} \\ &= \alpha(g_i(x))_{i\in I} + (g(y))_{i\in I} \\ &= \alpha h(x) + h(y). \end{aligned}$$

Além disso,

$$\begin{aligned} (\pi_i \circ h)(x) &= \pi_i(h(x)) \\ &= \pi_i((g_i(x))_{i\in I}) \\ &= g_i(x), \end{aligned}$$

o que implica em $\pi_i \circ h = g_i$, para todo $i \in I$.

Suponha que $h', h'' : M \to \prod_{i\in I} M_i$ sejam A-homomorfismos tais que $\pi_i \circ h' = g_i$, para todo $i \in I$. Tome $x \in M$ arbitrário. Assim, $h'(x) = (x_i)_{i\in I}$ e $h''(x) = (y_i)_{i\in I}$.
Deste modo, para todo $i \in I$,

$$\begin{aligned} g_i(x) = (\pi_i \circ h')(x) = \pi_i(h'(x)) &= \pi_i((x_i))_{i\in I} = x_i \\ g_i(x) = (\pi_i \circ h'')(x) = \pi_i(h''(x)) &= \pi_i((y_i)_{i\in I}) = y_i. \end{aligned}$$

Logo, $x_i = y_i$, para todo $i \in I$ e, consequentemente, $h'(x) = h''(x)$. Como $x \in M$ é arbitrário, então $h' = h''$.

Portanto, $(\prod_{i\in I} M_i, (\pi_i)_{i\in I})$ é produto da família $(M_i)_{i\in I}$.

□

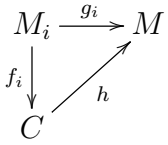
Devido ao Teorema 1.4.5, dado uma família de A-módulos qualquer, existe, a menos de isomorfismo, um único produto da família de A-módulos $(M_i)_{i\in I}$. Deste modo, consideraremos $(\prod_{i\in I} M_i, (\pi_i)_{i\in I})$ como o produto da família de A-módulos $(M_i)_{i\in I}$. No caso em que I é um conjunto finito, digamos $I = \{1, 2, ..., n\}$, escreveremos

$$\prod_{i\in I} M_i = \prod_{i=1}^{n} M_i = M_1 \times M_2 \times ... \times M_n,$$

cujos elementos são n-uplas $(m_1, m_2, ..., m_n)$, com $m_i \in M_i$, para todo $i \in \{1, 2, ..., n\}$.

1.5 Coprodutos e Somas Diretas

Definição 1.5.1. *Seja $(M_i)_{i\in I}$ uma família de A-módulos. Chamamos de coproduto dessa família o A-módulo C juntamente com uma família $(f_i)_{i\in I}$ de A-homomorfismos $f_i : M_i \to C$, tal que para todo A-módulo M e toda família $(g_i)_{i\in I}$ de A-homomorfismos $g_i : M_i \to M$, existe um único A-homomorfismo $h : C \to M$ que comuta o diagrama abaixo, para todo $i \in I$.*



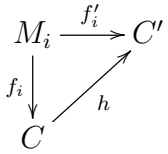
Denotaremos o coproduto por $(C, (f_i)_{i\in I})$.

Teorema 1.5.2. *Se $(C, (f_i)_{i\in I})$ é um coproduto da família de A-módulos $(M_i)_{i\in I}$, então cada f_i é um A-monomorfismo.*

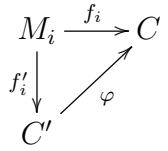
Demonstração. Considere $i \in I$ qualquer. Tome $M = M_i$, $g_i = Id_{M_i}$ e $g_j = 0$, para $j \neq i$. Assim, pela definição de coproduto,existe um único A-homomorfismo $h : C \to M$ tal que $h \circ f_j = g_j$, para todo $j \in I$. Em particular, $h \circ f_i = g_i = Id_{M_i}$, o que implica que f_i é um A-monomorfismo. □

Teorema 1.5.3 (Unicidade do Coproduto)**.** *Seja $(C, (f_i)_{i\in I})$ um coproduto da família de A-módulos $(M_i)_{i\in I}$. Então $(C', (f'_i)_{i\in I})$ é um coproduto de $(M_i)_{i\in I}$ se, e somente se, existe um único A-isomorfismo $h : C \to C'$ tal que $h \circ f_i = f'_i$, para todo $i \in I$.*

Demonstração. Como $(C, (f_i)_{i\in I})$ é um coproduto de $(M_i)_{i\in I}$, existe um único A-homomorfismo $h : C \to C'$ tal que $h \circ f_i = f'_i$, para todo $i \in I$.



Suponha que $(C', (f_i')_{i\in I})$ é um coproduto de $(M_i)_{i\in I}$. Assim, existe um único A-homomorfismo $\varphi : C' \to C$ tal que $\varphi \circ f_i' = f_i$.



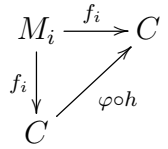
Como

$$\begin{aligned}(\varphi \circ h) \circ f_i &= \varphi \circ (h \circ f_i) \\ &= \varphi \circ f_i' \\ &= f_i,\end{aligned}$$

ou seja,

$$(\varphi \circ h) \circ f_i = f_i, \text{ para todo } i \in I,$$

então o diagrama



é comutativo, para todo $i \in I$. No entanto, pela definição de coproduto, existe um único A-homomorfismo que comuta esse diagrama. Logo, $\varphi \circ h = Id_C$.

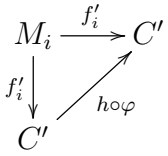
Analogamente, como

$$\begin{aligned}(h \circ \varphi) \circ f_i' &= h \circ (\varphi \circ f_i') \\ &= h \circ f_i \\ &= f_i',\end{aligned}$$

ou seja,

$$(h \circ \varphi) \circ f_i' = f_i', \text{ para todo } i \in I,$$

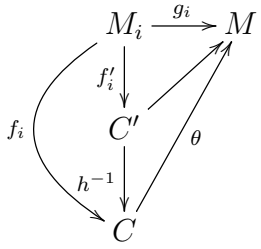
entaõ o diagrama



é comutativo, para todo $i \in I$. Porém, pela definição de coproduto, existe um único A-homomorfismo que comuta esse diagrama. Logo, $h \circ \varphi = Id_{C'}$.

Deste modo, $\varphi \circ h = Id_C$ e $h \circ \varphi = Id_{C'}$, o que implica que $h : C \to C'$ é um A-isomorfismo tal que $h \circ f_i = f_i'$, para todo $i \in I$.

Reciprocamente, suponha que $h : C \to C'$ seja um A-isomorfismo tal que $h \circ f_i = f_i'$, para todo $i \in I$. Sejam M um A-módulo e $(g_i)_{i\in I}$ uma família de A-homomorfismos $g_i : M_i \to M$. Como h é um A-isomorfismo e $h \circ f_i = f_i'$, então $f_i = h^{-1} \circ f_i'$, para todo $i \in I$. Considere o diagrama abaixo:



Como $(C, (f_i)_{i\in I})$ é um coproduto de $(M_i)_{i\in I}$, existe um único A-homomorfismo θ tal que $\theta \circ f_i = g_i$, para todo $i \in I$. Considere o A-homomorfismo $\psi = \theta \circ h^{-1} : C' \to M$. Assim, para todo $i \in I$ tem-se

$$\begin{aligned} \psi \circ f_i' &= (\theta \circ h^{-1}) \circ f_i' \\ &= \theta \circ (h^{-1} \circ f_i') \\ &= \theta \circ f_i \\ &= g_i. \end{aligned}$$

Seja $\psi' : C' \to M$ um A-homomorfismo tal que $\psi' \circ f_i' = g_i$, para todo $i \in I$. Como $h \circ f_i = f_i'$, para todo $i \in I$, então

$$\begin{aligned} g_i &= \psi' \circ f_i' \\ &= \psi' \circ (h \circ f_i) \\ &= (\psi' \circ h) \circ f_i. \end{aligned}$$

Sabendo que $\theta : C \to M$ é o único A-homomorfismo tal que $\theta \circ f_i = g_i$, para todo $i \in I$, segue que $\psi' \circ h = \theta$. Portanto, $\psi' = \theta \circ h^{-1} = \psi$, o que implica em $(C', (f_i')_{i\in I})$ é um coproduto de $(M_i)_{i\in I}$. □

Definição 1.5.4. *Seja $(M_i)_{i\in I}$ uma família de A-módulos. Uma família $(m_i)_{i\in I} \in \prod_{i\in I} M_i$ é dita quase-nula se $m_i = 0_{M_i}$, exceto para um número finito de índices.*

Observação 1.5.5. *No conjunto das famílias quase-nulas de $\prod_{i\in I} M_i$, podemos introduzir uma estrutura de A-módulo utilizando as operações de $\prod_{i\in I} M_i$, já que a soma e o produto de famílias quase-nulas é quase-nula.*

Definição 1.5.6. *Seja $(M_i)_{i\in I}$ uma família de A-módulos. O conjunto das famílias quase-nulas de $\prod_{i\in I} M_i$, com a estrutura de A-módulo definida por restrição das operações de $\prod_{i\in I} M_i$ é um A-módulo. Chamaremos tal A-módulo de soma direta externa da família $(M_i)_{i\in I}$ e indicaremos pelo símbolo $\bigoplus_{i\in I} M_i$.*

Definição 1.5.7. *Para cada $j \in I$, defina $\mu_j : M_j \to \bigoplus_{i\in I} M_i$, dado por $\mu_j(x) = (x_i)_{i\in I}$, onde $x_i = x$, se $i = j$ e $x_i = 0_{M_i}$, se $i \neq j$. É de fácil verificação que μ_j é um A-monomorfismo. Chamaremos μ_j de j-ésima injeção canônica de M_j sobre $\bigoplus_{i\in I} M_i$.*

Teorema 1.5.8 (Existência do Coproduto)**.** *$(\bigoplus_{i\in I} M_i, (\mu_i)_{i\in I})$ é um coproduto da família $(M_i)_{i\in I}$.*

Demonstração. Seja M um A-módulo qualquer e $(g_i)_{i\in I}$ uma família de A-homomorfismos $g_i : M_i \to M$. Considere $h : \bigoplus_{i\in I} M_i \to M$, dada por $h((m_i)_{i\in I}) = \sum_{i\in I} g_i(m_i)$. Notemos que a aplicação h está bem definida, pois sendo $(m_i)_{i\in I}$ uma família quase-nula, segue que $\sum_{i\in I} g_i(m_i)$ é finita. É de fácil verificação que h é um A-homomorfismo. Além disso, para todo $x \in M_i$ tem-se

$$\begin{aligned}(h \circ \mu_i)(x) &= h(\mu_i(x)) \\ &= h((x_i)_{i\in I}) \\ &= g_i(x),\end{aligned}$$

o que implica em $h \circ \mu_i = g_i$, para todo $i \in I$.

Suponha que $h' : \bigoplus_{i\in I} M_i \to M$ seja um A-homomorfismo tal que $h' \circ \mu_i = g_i$, para todo $i \in I$. Desta forma,

$$\begin{aligned} h'((m_i)_{i\in I}) &= h'(\sum_{i\in I} \mu_i(m_i)) \\ &= \sum_{i\in I} h'(\mu_i(m_i)) \\ &= \sum_{i\in I} (h' \circ \mu_i)(m_i) \\ &= \sum_{I\in I} g_i(m_i) \\ &= h((m_i)_{i\in I}), \end{aligned}$$

o que implica que $h' = h$. Portanto, $(\bigoplus_{i\in I} M_i, (\mu_i)_{i\in I})$ é um coproduto da família $(M_i)_{i\in I}$.

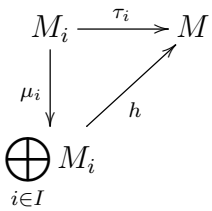
□

Observação 1.5.9. *Com base nos Teoremas 1.5.3 e Teorema 1.5.8, dado uma família de A-módulos $(M_i)_{i\in I}$ arbitrária, existe um único coproduto dessa família, a menos de isomorfismo. Deste modo, escolheremos $(\bigoplus_{i\in I} M_i, (\mu_i)_{i\in I})$ como o coproduto da família $(M_i)_{i\in I}$. Para o caso em que I é finito, digamos $I = \{1, 2, ..., n\}$, escreveremos*

$$\bigoplus_{i\in I} M_i = \bigoplus_{i=1}^{n} M_i = M_1 \bigoplus M_2 \bigoplus ... \bigoplus M_n,$$

cujos elementos da $\bigoplus_{i\in I} M_i$ são n-uplas $(m_1, m_2, m_3, ..., m_n)$, com $m_i \in M_i$ para todo $i \in \{1, 2, ..., n\}$. Logo, quando I for finito, os A-módulos $\bigoplus_{i\in I} M_i$ e $\prod_{i\in I} M_i$ coincidem.

Agora voltaremos nossa atenção para uma família $(M_i)_{i\in I}$, onde cada M_i é um submódulo de um A-módulo M. Para todo $i \in I$, tome $\tau_i : M_i \to M$, a inclusão natural e $h : \bigoplus_{i\in I} M_i \to M$ o único A-homomorfismo tal que o diagrama abaixo seja comutativo, para todo $i \in I$.



Seja a aplicação $\varphi : \bigoplus_{i\in I} M_i \to M$ dada por $\varphi((m_i)_{i\in I}) = \sum_{i\in I} m_i$. É de fácil verificação

que φ é um A-homomorfismo tal que

$$\begin{aligned}(\varphi \circ \mu_i)(m_i) &= \varphi(\mu_i(m_i)) \\ &= \varphi((n_j)_{j\in I}), \text{ onde } n_j = \begin{cases} 0_M, & \text{se } j \neq i; \\ m_i, & \text{se } j = i. \end{cases} \\ &= \sum_{j\in I} n_j \\ &= n_i \\ &= m_i \\ &= \tau_i(m_i),\end{aligned}$$

para todo $m_i \in M_i$, ou seja, $\varphi \circ \mu_i = \tau_i$, para todo $i \in I$. Como h é o único A-homomorfismo tal que $h \circ \mu_i = \tau_i$, para todo $i \in I$, então $h = \varphi$. Logo, $h((m_i)_{i\in I}) = \sum_{i\in I} m_i$. Além disso, note que $Im(h) = \sum_{i\in I} M_i = \{m = \sum_{i\in J} m_i, \text{ com } m_i \in M \text{ e } J \subset I \text{ finito}\}$.

Definição 1.5.10. *Sejam M é um A-módulo e $(M_i)_{i\in I}$ uma família de submódulos de M. Se o A-homomorfismo $h : \bigoplus_{i\in I} M_i \to M$ é uma bijeção, então diremos que M é a soma direta interna da família $(M_i)_{i\in I}$.*

Observação 1.5.11. *Com base na Definição 1.5.10, as somas diretas internas, caso existam, são isomorfas às somas diretas externas. Deste modo, omitiremos os adjetivos externa e interna, dizendo apenas soma direta e usaremos o símbolo $M = \bigoplus_{i\in I} M_i$ para representá-la.*

Teorema 1.5.12. *Um A-módulo M é soma direta da família $(M_i)_{i\in I}$ de submódulos de M se, e somente se, para todo $m \in M$ e $i \in I$, existem únicos $m_i \in M_i$ tais que $m = \sum_{i\in I} m_i$.*

Demonstração. Suponha que $M = \bigoplus_{i\in I} M_i$. Assim, por definição, o A-homomorfismo $h : \bigoplus_{i\in I} M_i \to M$, dado por $h((m_i)_{i\in I}) = \sum_{i\in I} m_i$ é um isomorfismo. Desta forma, dado $m \in M$, existe único $(m_i)_{i\in I} \in \bigoplus_{i\in I} M_i$ tal que $h((m_i)_{i\in I}) = \sum_{i\in I} m_i = m$, o que implica que existem únicos $m_i \in M_i$, com $i \in I$, tais que $m = \sum_{i\in I} m_i$.

Reciprocamente, suponha que dado $m \in M$ qualquer, existam únicos $m_i \in M_i$, com $i \in I$, tais que $m = \sum_{i\in I} m_i$. Assim, $m = \sum_{i\in I} m_i = h((m_i)_{i\in I})$, o que implica que h é um A-epimorfismo.

Por outro lado, seja $(m_i)_{i\in I} \in Ker(h)$. Assim, $\sum_{i\in I} m_i = h((m_i)_{i\in I}) = 0_M$ e, consequentemente, $m_i = 0_M$, para todo $i \in I$. Logo $Ker(h) = \{0_M\}$, o que implica que h é um A-monomorfismo. Portanto, h é um A-isomorfismo e segue que $M = \bigoplus_{i\in I} M_i$. □

Teorema 1.5.13. *Seja $(M_i)_{i\in I}$ uma família de submódulos do A-módulo M. As seguintes afirmações são equivalentes:*

1) $\sum_{i\in I} M_i$ *é uma soma direta de* $(M_i)_{i\in I}$.

2) Se $\sum_{i\in I} m_i = 0_M$, *com* $m_i \in M_i$, *para todo* $i \in I$, *então* $m_i = 0_M$, *para todo* $i \in I$.

3) $M_i \cap \sum_{i\neq j} M_j = \{0_M\}$, *para todo* $i \in I$.

Demonstração. (1) ⇒ (2) Decorre do Teorema 1.5.12.

(2) ⇒ (3) Seja $m \in M_i \cap \sum_{j\neq i} M_j$ qualquer. Assim, $m \in M_i$ e $m \in \sum_{j\neq i} M_j$.

De $m \in \sum_{j\neq i} M_j$, existe $m_j \in M_j$, com $j \neq i$, tal que $m = \sum_{j\neq i} m_j$. Desta forma, $m = \sum_{j\neq i} m_j$ implica que $\sum_{j\neq i} m_j + (-m) = 0_M$, ou seja, $m_j = 0_M$, para todo $j \neq i$ e $m = 0_M$. Assim, $M_i \cap \sum_{j\neq i} M_j = \{0_M\}$.

(3) ⇒ (1) Suponha que $\sum_{i\in I} m_i = \sum_{i\in I} n_i$, com $m_i, n_i \in M_i$, para todo $i \in I$. Assim, $m_i + \sum_{j\neq i} m_j = n_i + \sum_{j\neq i} n_j$, o que implica que $m_i - n_i = \sum_{j\neq i} n_j - \sum_{j\neq i} m_j = \sum_{j\neq i}(n_j - m_j)$. Como $m_i - n_i \in M_i$ e $\sum_{j\neq i}(n_j - m_j) \in \sum_{j\neq i} M_j$, segue que $m_i - n_i \in M_i \cap \sum_{j\neq i} m_j = \{0_M\}$. Logo, $m_i = n_i$, para todo $i \in I$. Portanto, pelo Teorema 1.5.12, concluímos que $\sum_{i\in I} M_i$ é uma soma direta da família $(M_i)_{i\in I}$. □

Corolário 1.5.14. *Seja F e H submódulos de M. Então $M = F \bigoplus H$ se, e somente se, $M = F + H$ e $F \cap H = \{0_M\}$.*

Exemplo 1.5.15. *Se $m, n \in \mathbb{Z}$ com $m, n \geq 2$ e $(m, n) = 1$, então $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \bigoplus \mathbb{Z}_n$.*

Com efeito, considere a aplicação $\psi : \mathbb{Z} \to \mathbb{Z}_m \bigoplus \mathbb{Z}_n$, dada por $\psi(x) = [x]_m + [x]_n$. Claramente ψ é um $\mathbb{Z}$-homomorfismo. Tome $x \in Ker(\psi)$. Assim, $\psi(x) = [0]_m + [0]_n$, ou seja,

$[x]_m + [x]_n = [0]_m + [0]_n$, o que implica em $[x]_m = [0]_m$ e $[x]_n = [0]_n$. Logo, $x \in m\mathbb{Z}$ e $x \in n\mathbb{Z}$. Desta forma, $x \in (mn)\mathbb{Z}$ e, consequentemente, tem-se $Ker(\psi) \subset (mn)\mathbb{Z}$.

Por outro lado, dado $x = (mn)a \in (mn)\mathbb{Z}$ qualquer, segue que

$$\psi(x) = [x]_m + [x]_n = [mna]_m + [mna]_n = [0]_m + [0]_n,$$

o que implica que $x \in Ker(\psi)$. Deste modo, $(mn)\mathbb{Z} \subset Ker(\psi)$ e concluímos que $Ker(\psi) = (mn)\mathbb{Z}$.

Considere $[r]_m + [s]_n \in \mathbb{Z}_m \bigoplus \mathbb{Z}_n$ qualquer. Como $(m, n) = 1$, existem $x_0, y_0 \in \mathbb{Z}$, tais que $mx_0 + ny_0 = 1$. Tome $x = mx_0s + ny_0r \in \mathbb{Z}$. Desta forma,

$$\begin{aligned} \psi(x) &= [x]_m + [x]_n \\ &= [ny_0r]_m + [mx_0s]_n \\ &= [r]_m + [s]_n. \end{aligned}$$

Como $[r]_m + [s]_n \in \mathbb{Z}_m \bigoplus \mathbb{Z}_n$ é arbitrário, concluímos que ψ é sobrejetora, ou seja, ψ é um A-epimorfismo. Pelo Teorema 1.3.15,

$$\mathbb{Z}_{mn} \cong \frac{\mathbb{Z}}{(mn)\mathbb{Z}} = \frac{\mathbb{Z}}{Ker(\psi)} \cong Im(\psi) = \mathbb{Z}_m \bigoplus \mathbb{Z}_n.$$

Portanto, $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \bigoplus \mathbb{Z}_n$.

Exemplo 1.5.16. *Considere o $\mathbb{Z}$-módulo $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. É de fácil verificação que $H_1 = \{\overline{0}, \overline{2}, \overline{4}\}$ e $H_2 = \{\overline{0}, \overline{3}\}$ são submódulos de $\mathbb{Z}_6$ tais que $H_1 \cap H_2 = \{\overline{0}\}$. Como*

$$\begin{aligned} \overline{0} &= \overline{0} + \overline{0} \in H_1 + H_2 \\ \overline{1} &= \overline{4} + \overline{3} \in H_1 + H_2 \\ \overline{2} &= \overline{2} + \overline{0} \in H_1 + H_2 \\ \overline{3} &= \overline{0} + \overline{3} \in H_1 + H_2 \\ \overline{4} &= \overline{4} + \overline{0} \in H_1 + H_2 \\ \overline{5} &= \overline{2} + \overline{3} \in H_1 + H_2, \end{aligned}$$

segue que $\mathbb{Z}_6 = H_1 + H_2$, e portanto, $\mathbb{Z}_6 = H_1 \bigoplus H_2$.

Definição 1.5.17. *Sejam M um A-módulo e N um submódulo de M.*

1) Diremos que N é um somando direto de M, se existe um submódulo N_1 de M tal que $M = N \bigoplus N_1$. Nesse caso, diremos que N_1 é um suplementar de N.

2) Diremos que M é um A-módulo irredutível, se $\{0\}$ e M são os seus únicos somandos diretos. Caso M não seja irredutível, diremos que ele é um A-módulo redutível.

Exemplo 1.5.18. *Todo A-módulo simples é irredutível. No entanto, nem sempre a recíproca é verdadeira.*

Afirmação: $\mathbb{Z}^{\mathbb{Z}}$ é um $\mathbb{Z}$-módulo irredutível e não é um $\mathbb{Z}$-módulo simples.

De fato, claramente $\mathbb{Z}^{\mathbb{Z}}$ não é um $\mathbb{Z}$-módulo simples. Por outro lado, seja $N = ((n))$ um somando direto de $\mathbb{Z}^{\mathbb{Z}}$. Assim, existe $N_1 = ((n_1))$ um submódulo de $\mathbb{Z}^{\mathbb{Z}}$ tal que $\mathbb{Z}^{\mathbb{Z}} = N \bigoplus N_1$. Como $nn_1 \in N = ((n))$ e $nn_1 \in N_1 = ((n_1))$, segue que $nn_1 \in N \cap N_1 = \{0\}$. Daí, $n = 0$ ou $n_1 = 0$, o que implica que $N = \{0\}$ ou $N = \mathbb{Z}^{\mathbb{Z}}$. Portanto, $\mathbb{Z}^{\mathbb{Z}}$ é um $\mathbb{Z}$-módulo irredutível.

Exemplo 1.5.19. *Seja $N = ((\overline{r}))$ um submódulo de $\mathbb{Z}_m$, para algum $r \in \{1, 2, ..., m\}$. N é um somando direto do $\mathbb{Z}$-módulo $\mathbb{Z}_m$ se, e somente se, $(r, \frac{m}{r}) = 1$.*

Com efeito, pelo Corolário 1.3.23, os submódulos de $\mathbb{Z}_m$ são da forma $\frac{n\mathbb{Z}}{m\mathbb{Z}}$, com $m\mathbb{Z} \subset n\mathbb{Z}$. Sendo $N = ((\overline{r})) = \frac{r\mathbb{Z}}{m\mathbb{Z}}$, um submódulo de $\mathbb{Z}_m$, então $r \mid m$, ou seja, $\frac{m}{r} \in \mathbb{Z}_+$ e é tal que $|N| = \frac{m}{r}$. Suponhamos que N seja um somando direto de $\mathbb{Z}_m$. Assim, existe um submódulo N_1 de $\mathbb{Z}_m$ tal que $\mathbb{Z}_m = N \bigoplus N_1$. Analogamente, pela observação anterior, existe $s \in \{1, 2, ..., m\}$ tal que $N_1 = ((\overline{s}))$, o que implica que $\frac{m}{s} \in \mathbb{Z}_+$ e é tal que $|N_1| = \frac{m}{s}$. Deste modo, $m = |\mathbb{Z}_m| = |N||N_1| = \frac{m}{r}\frac{m}{s} = \frac{m^2}{rs}$, o que implica que $m = rs$.

Por outro lado, tome $d = (r, s)$. Pela definição de mdc, $d \mid r$ e $d \mid s$, ou seja, $d \mid \frac{m}{s}$ e $d \mid \frac{m}{r}$. Como $d \mid \frac{m}{s}$ e $d \mid \frac{m}{r}$, existem únicos subgrupos H e H_1 de N e N_1, respectivamente, tais que $|H| = |H_1| = d$. No entanto, como $(\mathbb{Z}_m, +)$ é um grupo cíclico e $d \mid m$, existe um único subgrupo de $\mathbb{Z}_m$ de ordem d, o que implica que $H = H_1$. Logo, $H \in N \cap N_1 = \{\overline{0}\}$ e, consequentemente, $d = 1$. Portanto, $(r, \frac{m}{r}) = (r, s) = 1$.

Reciprocamente, suponha que $(r, \frac{m}{r}) = 1$. Considerando $s = \frac{m}{r}$ obtemos $m = rs$ e $(r, s) = 1$. De $(r, s) = 1$, existem $x_0, y_0 \in \mathbb{Z}$ tais que $rx_0 + sy_0 = 1$. Deste modo, $\overline{1} = \overline{rx_0} + \overline{sy_0} \in ((\overline{r})) + ((\overline{s})) = N + ((\overline{s}))$, o que implica que $\mathbb{Z}_m = N + N_1$, onde $N_1 = ((\overline{s}))$. Por outro lado, tome $\overline{n} \in N \cap N_1$ qualquer. Assim, $\overline{n} \in N$ e $\overline{n} \in N_1$. De $\overline{n} \in N$, segue que $\overline{n} = \alpha\overline{r} = \overline{\alpha r}$, para algum $\alpha \in \mathbb{Z}$. Assim, $n = \alpha r + mx$, para algum $x \in \mathbb{Z}$. De $\overline{n} \in N_1$, tem-se $\overline{n} = \beta\overline{s} = \overline{\beta s}$, para algum $\beta \in \mathbb{Z}$ e, consequentemente,

$n = \beta s + my$, para algum $y \in \mathbb{Z}$. Deste modo, $n = \alpha r + rsx$ e $n = \beta s + rsy$, o que implica que $r \mid n$ e $s \mid n$, ou seja, $[r, s] \mid n$. Como $(r, s) = 1$, então $[r, s] = rs$ e tem-se $rs \mid n$, o que implica que $m \mid n$. Assim, $\overline{n} = \overline{0}$ e segue que $N \cap N_1 = \{\overline{0}\}$. Portanto, $\mathbb{Z}_m = N \bigoplus N_1$.

Observação 1.5.20. *Do Exemplo 1.5.19, podemos concluir que se $m \in \mathbb{Z}$, com $m \geq 2$ é primo, então $\mathbb{Z}_m$ é um $\mathbb{Z}$-módulo irredutível. No entanto, a recíproca é falsa! Mostraremos que $\mathbb{Z}_8$ é um $\mathbb{Z}$-módulo irredutível. Com efeito, seja $N = ((\overline{r}))$ um somando direto de $\mathbb{Z}_8$, para algum $r \in \{1, 2, ..., 8\}$. Deste modo, existe $N_1 = ((\overline{s}))$, um submódulo de $\mathbb{Z}_8$, tal que $\mathbb{Z}_8 = N \bigoplus N_1$, para algum $s \in \{1, 2, ..., 8\}$. Como $|N| = \frac{8}{r}$, $|N_1| = \frac{8}{s}$ e $8 = |\mathbb{Z}_8| = |N||N_1|$, segue que $8 = \frac{8 \cdot 8}{rs}$, ou seja, $rs = 8$. Por outro lado, do Exemplo 1.5.19, $(r, \frac{8}{r}) = 1$, ou seja, $(r, s) = 1$. Sabendo que $r, s \in \{1, 2, ..., 8\}$, $rs = 8$ e $(r, s) = 1$, segue que $r = 1$ ou $r = 8$, o que implica que $N = \{\overline{0}\}$ ou $N = \mathbb{Z}_8$. Portanto $\mathbb{Z}_8$ é um $\mathbb{Z}$-módulo irredutível.*

Teorema 1.5.21. *Se M é um A-módulo e M_1, M_2 são submódulos de M tais que $M = M_1 \bigoplus M_2$, então $M_2 \cong \frac{M}{M_1}$.*

Demonstração. De $M = M_1 \bigoplus M_2$, segue que para cada $m \in M$, existem únicos $m_1 \in M_1$ e $m_2 \in M_2$ tais que $m = m_1 + m_2$. Considere a aplicação $\pi_2 : M \to M_2$ dada por $\pi_2(m) = \pi_2(m_1 + m_2) = m_2$. É de fácil verificações que π_2 é um A-epimorfismo tal que $Ker(\pi_2) = M_1$. Assim, pelo Teorema 1.3.15, concluímos que $\frac{M}{M_1} \cong M_2$. □

Corolário 1.5.22. *Se $M = M_1 \bigoplus M_2 = M_1 \bigoplus M_3$ então $M_2 \cong M_3$.*

Observação 1.5.23. *O Teorema 1.5.21 pode ser utilizado para demonstrar, de uma outra forma, que $\mathbb{Z}^{\mathbb{Z}}$ não contém somando diretos não triviais.*

Com efeito, se $M = ((m))$ for um somando direto de $\mathbb{Z}^{\mathbb{Z}}$, o seu suplementar deveria ser isomorfo ao quociente $\frac{\mathbb{Z}}{((m))} \cong \mathbb{Z}_m$, mas $\mathbb{Z}^{\mathbb{Z}}$ não possui submódulos finitos.

1.6 Sequências Exatas

Definição 1.6.1. *Sejam F, G, H A-módulos e, $f : F \to G$ e $g : G \to H$ A-homomorfismos. Se $Im(f) \subset Ker(g)$, ou seja, $g \circ f = 0$, diremos que o diagrama*

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

é uma sequência de ordem 2 em G. Em particular, se $Im(f) = Ker(g)$, diremos que a sequência é exata em G.

Definição 1.6.2. *Seja* $\{..., M_{i-1}, M_i, M_{i+1}, ...\}$ *uma família infinita de A-módulos e* $\{..., f_i : M_{i-1} \to M_i, ...\}$ *uma família de A-homomorfismos. Diremos que o diagrama*

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

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

Exemplo 1.6.3. *A sequência* $0 \longrightarrow E \xrightarrow{f} F$ *é exata se, e somente se,* f *é um A-monomorfismo.*

Exemplo 1.6.4. *A sequência* $E \xrightarrow{f} F \longrightarrow 0$ *é exata se, e somente se,* f *é um A-epimorfismo.*

Exemplo 1.6.5. *A sequência* $0 \longrightarrow E \xrightarrow{f} F \longrightarrow 0$ *é exata se, e somente se,* f *é um A-isomorfismo.*

Exemplo 1.6.6. *Seja* $i : 2\mathbb{Z} \to \mathbb{Z}$ *a inclusão e* $\pi : \mathbb{Z} \to \mathbb{Z}_2$ *a projeção canônica. A sequência* $0 \longrightarrow 2\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_2 \xrightarrow{g} 0$ *é exata, pois*

$$Ker(i) = \{0\},\ Im(i) = Ker(\pi) = 2\mathbb{Z} \text{ e } Im(\pi) = Ker(g) = \mathbb{Z}_2.$$

Exemplo 1.6.7. *Se* E *é um submódulo de um A-módulo* F*,* $i : E \to F$ *a inclusão e* $\pi : F \to \frac{F}{E}$ *a projeção canônica, então a sequência* $0 \xrightarrow[f]{} E \xrightarrow{i} F \xrightarrow{\pi} \frac{F}{E} \xrightarrow{g} 0$ *é exata, pois* $Im(f) = \{0\} = Ker(i)$*,* $Im(i) = E = Ker(\pi)$ *e* $Im(\pi) = \frac{F}{E} = Ker(g)$*.*

Definição 1.6.8. *Diremos que uma sequência exata de A-módulos* $0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G \longrightarrow 0$ *cinde se* $Im(f) = Ker(g)$ *é um somando direto de* F*.*

Teorema 1.6.9. *Seja* $f : M_1 \to M_2$ *um A-homomorfismo, então:*

I) f *é injetora e* $Im(f)$ *é um somando direto de* M_2 *se, e somente se, existe um A-homomorfismo* $\psi_1 : M_2 \to M_1$ *tal que* $\psi_1 \circ f = Id_{M_1}$*.*

II) f *é sobrejetora e* $Ker(f)$ *é um somando direto de* M_1 *se, e somente se, existe um A-homomorfismo* $\psi_2 : M_2 \to M_1$ *tal que* $f \circ \psi_2 = Id_{M_2}$*.*

Demonstração. (I) Seja M_2' um submódulo de M_2 tal que $M_2 = Im(f) \bigoplus M_2'$. Assim, para cada elemento $m \in M_2$, existem únicos $m' \in M_2'$ e $y \in Im(f)$ tais que $m = y + m'$. Como f é injetora, existe um único $x \in M_1$ tal que $f(x) = y$. Logo $m = m' + f(x)$, onde x está univocamente determinado por m, o que nos permite definir a aplicação

$$\begin{aligned} \psi_1 : M_2 &\longrightarrow M_1 \\ m &\longmapsto \psi_1(m) = x. \end{aligned}$$

É de fácil verificação que ψ_1 é um A-homomorfismo. Dado $w \in M_1$, $f(w) = f(w) + 0_{M_2}$, o que implica que $(\psi_1 \circ f)(w) = \psi_1(f(w)) = w$. Portanto, $\psi_1 \circ f = Id_{M_1}$.

Reciprocamente, se $\psi_1 \circ f = Id_{M_1}$, segue que f é injetora.

Afirmação: $M_2 = Im(f) \bigoplus Ker(\psi_1)$.

De fato, dado $y \in M_2$ qualquer, tem-se $y = (y - (f \circ \psi_1)(y)) + (f \circ \psi_1)(y)$, sendo $(f \circ \psi_1)(y) = f(\psi_1(y)) \in Im(f)$ e

$$\begin{aligned} \psi_1(y - (f \circ \psi_1)(y)) &= \psi_1(y) - \psi_1[(f \circ \psi_1)(y)] \\ &= \psi_1(y) - (\psi_1 \circ f)(\psi_1(y)) \\ &= \psi_1(y) - Id_{M_1}(\psi_1(y)) \\ &= \psi_1(y) - \psi_1(y) \\ &= 0_{M_1}, \end{aligned}$$

o que implica em $y - (f \circ \psi_1)(y) \in Ker(\psi_1)$. Logo, $M_2 = Im(f) + Ker(\psi_1)$.

Tome $y \in Im(f) \cap Ker(\psi_1)$. Assim, $y = f(x)$, para algum $x \in M_1$ e $\psi_1(y) = 0_{M_1}$. Então,

$$\begin{aligned} x &= Id_{M_1}(x) \\ &= (\psi_1 \circ f)(x)) \\ &= \psi_1(f(x)) \\ &= \psi_1(y) \\ &= 0_{M_1}, \end{aligned}$$

o que implica em $Im(f) \cap Ker(\psi_1) = \{0_{M_2}\}$. Portanto, $M_2 = Im(f) \bigoplus Ker(\psi_1)$ e, consequentemente, $Im(f)$ é um somando direto de M_2.

(II) Seja M_1' um submódulo de M_1 tal que $M_1 = Ker(f) \bigoplus M_1'$. Dado $m \in M_2$, existe $x \in M_1$ tal que $f(x) = m$. Como $M_1 = Ker(f) \bigoplus M_1'$, existem únicos $x_1 \in M_1'$ e

$x_2 \in Ker(f)$ tais que $x = x_1 + x_2$. Definamos

$$\begin{array}{rcl} \psi_2 : M_2 & \longrightarrow & M_1 \\ m & \longmapsto & x_1 \end{array}$$

Afirmação 1: ψ_2 está bem definida.

Com efeito, seja $x' \in M_1$ tal que $f(x') = m$, sendo $x' = x'_1 + x'_2$, com $x'_1 \in M'_1$ e $x'_2 \in Ker(f)$. Desta forma, $f(x') = f(x'_1)+f(x'_2)$, o que implica que $f(x) = f(x') = f(x'_1)$, ou seja, $f(x - x'_1) = 0_{M_2}$ e, consequentemente, tem-se $x - x'_1 \in Ker(f)$. Logo, existe $s \in Ker(f)$ tal que $x = x'_1 + s$. Desta forma, $x = x'_1 + s = x_1 + x_2$, o que resulta em $x_2 - s = x'_1 - x_1$. Como $M'_1 \cap Ker(f) = \{0_{M_1}\}$, segue que $x'_1 = x_1$ e concluímos que ψ_2 está bem definida. Por outro lado, ψ_2 é um A-homomorfismo que satisfaz

$$\begin{array}{rcl} (f \circ \psi_2)(m) & = & f(\psi_2(m)) \\ & = & f(x_1) \\ & = & f(x) \\ & = & m, \end{array}$$

para todo $m \in M$. Logo, $f \circ \psi_2 = Id_{M_2}$.

Reciprocamente, de $f \circ \psi_2 = Id_{M_2}$, segue que f é sobrejetora.

Afirmação 2: $M_1 = Ker(f) \bigoplus Im(\psi_2)$.

Dado $x \in M_1$, tem-se $x = (x - (\psi_2 \circ f)(x)) + (\psi_2 \circ f)(x)$.
Notemos que $(\psi_2 \circ f)(x) = \psi_2(f(x)) \in Im(\psi_2)$ e

$$\begin{array}{rcl} f(x - (\psi_2 \circ f)(x)) & = & f(x) - f((\psi_2 \circ f)(x)) \\ & = & f(x) - (f \circ \psi_2)(f(x)) \\ & = & f(x) - Id_{M_2}(f(x)) \\ & = & f(x) - f(x) \\ & = & 0_{M_2}, \end{array}$$

o que implica que $x - (\psi_2 \circ f)(x) \in Ker(f)$. Logo $M_1 = Ker(f) + Im(\psi_2)$.

Por outro lado, seja $x \in Ker(f) \cap Im(\psi_2)$. Assim, $x \in Ker(f)$ e $x = \psi_2(z)$, para algum $z \in M_2$. Então,

$$\begin{aligned} 0_{M_2} &= f(x) \\ &= f(\psi_2(z)) \\ &= (f \circ \psi_2)(z) \\ &= Id_{M_2}(z) \\ &= z, \end{aligned}$$

o que implica em $x = 0_{M_1}$ e, consequentemente, $Ker(f) \cap Im(\psi_2) = \{0_{M_1}\}$.

Logo, $M_1 = Ker(f) \bigoplus Im(\psi_2)$ e, portanto, $Ker(f)$ é um somando direto de M_1. □

Teorema 1.6.10. *Dada uma sequência exata de A-módulos* $0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G \longrightarrow 0$ *as seguintes afirmações são equivalentes:*

1) A sequência cinde.

2) Existe um A-homomorfismo $\psi_1 : F \to E$ *tal que* $\psi_1 \circ f = Id_E$.

3) Existe um A-homomorfismo $\psi_2 : G \to F$ *tal que* $g \circ \psi_2 = Id_G$.

Demonstração. Decorre do Teorema 1.6.9 . □

Corolário 1.6.11. *Nas condições do Teorema 1.6.9 tem-se* $F \cong E \bigoplus G$.

Demonstração. Suponha que a sequência de A-módulos $0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G \longrightarrow 0$ cinde. Sendo $Im(f) = Ker(g)$ um somando direto de F, existe um A-homomorfismo $\psi_1 : F \to E$ tal que $\psi_1 \circ f = Id_E$ e $F = Im(f) \bigoplus Ker(\psi_1)$.

Por outro lado, como g é sobrejetora e $Ker(g)$ é um somando direto de F, existe um A-homomorfismo $\psi_2 : G \to F$ tal que $g \circ \psi_2 = Id_G$ e $F = Ker(g) \bigoplus Im(\psi_2)$. Assim,

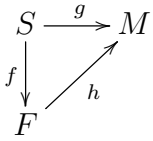
$$F = Im(f) \bigoplus Ker(\psi_1) = Im(f) \bigoplus Im(\psi_2).$$

Como f e ψ_2 são A-monomorfismos, pelo Teorema 1.3.15, $E \cong Im(f)$ e $G \cong Im(\psi_2)$. Portanto $F \cong E \bigoplus G$. □

2 Módulos Livres

As propriedades de independência linear e conjunto gerador, que conhecemos em espaços vetoriais, serão facilmente estendidas aos módulos. No entanto, devido à generalização do conjunto dos escalares, há conceitos que são perdidos, como o de base. Verificaremos neste capítulo a existência de módulos que não possuem uma base. Além disso, veremos que nem todo submódulo de um módulo que possui base também possui uma base, diferente dos espaços vetoriais.

Definição 2.0.1. *Sejam A um anel e S um conjunto não vazio qualquer. Diremos que o A-módulo F juntamente com uma aplicação $f : S \to F$, é um A-módulo livre sobre S se, para quaisquer A-módulo M e aplicação $g : S \to M$, existe um único A-homomorfismo $h : F \to M$ tal que o diagrama*



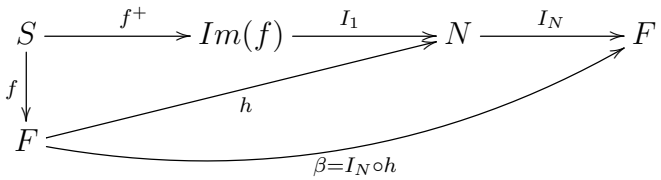
comuta, isto é, $h \circ f = g$. Denotaremos por $(F; f)$.

Teorema 2.0.2. *Se (F, f) é um A-módulo livre sobre S, então f é injetora e $Im(f)$ gera F.*

Demonstração. Sejam $x, y \in S$ tais que $x \neq y$. Considere M um A-módulo com mais de um elemento e $g : S \to M$ uma aplicação tal que $g(x) \neq g(y)$. Como $(F; f)$ é um A-módulo livre sobre S, existe um único A-homomorfismo $h : F \to M$ tal que $h \circ f = g$. Assim,

$$\begin{aligned} h(f(x)) &= g(x) \\ &\neq g(y) \\ &= h(f(y)), \end{aligned}$$

o que implica que $f(x) \neq f(y)$. Logo f é injetora.
Por outro lado, seja $N = ((Im(f))) \subset F$. Considere o diagrama



sendo $f^+ : S \to Im(f)$ uma aplicação tal que $f^+(s) = f(s)$, para todo $s \in S$, I_1 é a inclusão da $Im(f)$ em N e I_N a inclusão de N em F. Como F é livre sobre S, existe um único A-homomorfismo $h : F \to N$ tal que $h \circ f = I_1 \circ f^+$.

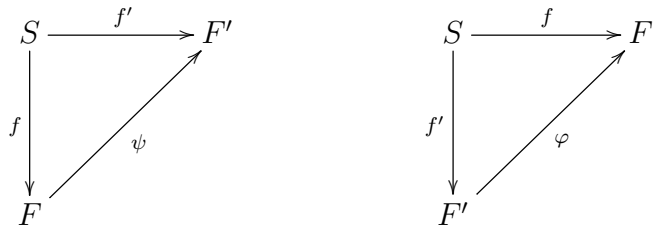
Considere $\beta : F \to F$, o A-homomorfismo dado por $\beta = I_N \circ h$. Notemos que

$$\begin{aligned} \beta \circ f &= (I_N \circ h) \circ f \\ &= I_N \circ (h \circ f) \\ &= I_N \circ (I_1 \circ f^+). \\ &= I_N \circ I_1 \circ f^+. \end{aligned}$$

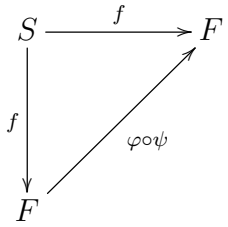
Por outro lado, existe um único A-homomorfismo $\varphi : F \to F$ tal que $\varphi \circ f = I_N \circ I_1 \circ f^+$. Deste modo, $\beta = \varphi$. Como $I_N \circ I_1 \circ f^+ = f$, então $\varphi \circ f = f$. Da unicidade de φ, segue que $\beta = \varphi = Id_F$. Deste modo, $I_N \circ h = Id_F$, o que implica que $I_N : N \to F$ é um A-epimorfismo, donde segue que $Im(I_N) = F$, ou seja, $F = N = ((Im(f)))$. □

Teorema 2.0.3. *Seja $(F; f)$ um A-módulo livre sobre um conjunto não vazio S. Então $(F'; f')$ é um A-módulo livre sobre S se, e somente se, existe um único A-isomorfismo $\psi : F \to F'$ tal que $\psi \circ f = f'$.*

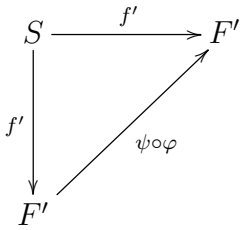
Demonstração. Primeiramente, suponhamos que (F, f) e $(F'; f)$ sejam A-módulos livres sobre S. Então existem únicos A-homomorfismos $\psi : F \to F'$ e $\varphi : F' \to F$, tais que os diagramas abaixo comutam.



Como $\varphi \circ \psi \circ f = \varphi \circ (\psi \circ f) = \varphi \circ f' = f$, segue que o diagrama

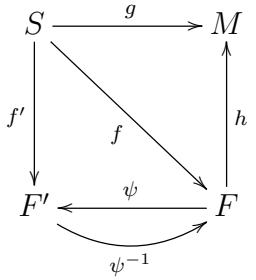


é comutativo. Como F é livre sobre S e $Id_F : F \to F$ é um A-homomorfismo tal que $Id_F \circ f = f$, segue que $\varphi \circ \psi = Id_F$.
Por outro lado, como $\psi \circ \varphi \circ f' = \psi \circ (\varphi \circ f') = \psi \circ f = f'$, segue que o diagrama a seguir é comutativo.



Sabendo que F' é livre sobre S e $Id_{F'} : F' \to F$ é um A-homomorfismo que comuta o diagrama anterior, segue que $\psi \circ \varphi = Id_{F'}$. Logo, ψ é um A-isomorfismo. Notemos que a unicidade de ψ é garantida pelo fato de F ser livre sobre S.

Reciprocamente, suponha que $\psi : F \to F'$ seja um A-isomorfismo tal que $\psi \circ f = f'$. Assim, $f = \psi^{-1} \circ f'$. Sejam M um A-módulo e $g : S \to M$ uma aplicação. Como F é livre sobre S, existe um único $h : F \to M$ tal que $h \circ f = g$.



Tome $\theta : F' \to M$ um A-homomorfismo dado por $\theta = h \circ \psi^{-1}$. Observe que θ é um A-homomorfismo tal que

$$\begin{aligned} \theta \circ f' &= (h \circ \psi^{-1}) \circ f' \\ &= h \circ (\psi^{-1} \circ f') \\ &= h \circ f = g. \end{aligned}$$

Seja $\tilde{\theta} : F' \to M$ um A-homomorfismo tal que $\tilde{\theta} \circ f' = g$. Desta forma,

$$\begin{aligned}(\tilde{\theta} \circ \psi) \circ f &= \tilde{\theta} \circ (\psi \circ f) \\ &= \tilde{\theta} \circ f' \\ &= g.\end{aligned}$$

Da unicidade do A-homomorfismo h, segue que $\tilde{\theta} \circ \psi = h$. Assim, $\tilde{\theta} = h \circ \psi^{-1} = \theta$ e, portanto, $(F'; f')$ é um A-módulo livre sobre S.

□

Teorema 2.0.4 (Existência)**.** *Para todo conjunto não vazio S e todo anel A, existe um A-módulo livre sobre S.*

Demonstração. Seja S um conjunto não vazio qualquer. Considere o conjunto

$$F = \{\varphi : S \to A;\ \varphi(s) = 0_A, \text{ exceto para um nº finito de } s \in S\}.$$

Introduziremos no conjunto F as operações

$$\begin{aligned}+ : F \times F &\longrightarrow F \\ (\varphi, \varepsilon) &\longmapsto (\varphi + \varepsilon)(s) = \varphi(s) + \varepsilon(s), \forall s \in S.\end{aligned}$$

$$\begin{aligned}\cdot : A \times F &\longrightarrow F \\ (\alpha, \varphi) &\longmapsto (\alpha\varphi)(s) = \alpha\varphi(s), \forall s \in S \text{ e } \alpha \in A.\end{aligned}$$

É de fácil verificação que F é um A-módulo. Considere a aplicação $f : S \to F$ atribuindo para $s \in S$ a aplicação dada por

$$\begin{aligned}f : \ S &\longrightarrow F \\ s &\longmapsto f(s) : \ S \longrightarrow A \\ &\qquad\qquad\ t \longmapsto (f(s))(t)\end{aligned}$$

sendo

$$(f(s))(t) = \begin{cases} 1_A, & \text{se} \quad t = s; \\ 0_A, & \text{se} \quad t \neq s. \end{cases}$$

Afirmação:$(F; f)$ é um A-módulo livre sobre S.

De fato, sejam M um A-módulo e $g : S \to M$ uma aplicação. Considere $h : F \to M$ dada por $h(\varphi) = \sum_{t\in S} \varphi(t)g(t)$. Note que a aplicação h está bem definida, pois a soma possui apenas um número finito de parcelas não nulas. Por outro lado, h é um A-homomorfismo, pois

$$\begin{aligned} h(\alpha\varphi + \varphi_1) &= \sum_{t\in S}(\alpha\varphi + \varphi_1)(t)g(t) \\ &= \sum_{t\in S}(\alpha\varphi(t) + \varphi_1(t))g(t) \\ &= \sum_{t\in S}\alpha(\varphi(t)g(t)) + \varphi_1(t)g(t) \\ &= \alpha\sum_{t\in S}\varphi(t)g(t) + \sum_{t\in S}\varphi_1(t)g(t) = \alpha h(\varphi) + h(\varphi_1). \end{aligned}$$

Além disso, para todo $s \in S$, tem-se

$$(h \circ f)(s) = h(f(s)) = \sum_{t\in S}(f(s))(t)g(t) = (f(s))(s)g(s) = g(s),$$

ou seja, $h \circ f = g$.

Suponha que $\psi : F \to M$ seja um A-homomorfismo tal que $\psi \circ f = g$. Notemos que para qualquer $\varphi \in F$, tem-se

$$\begin{aligned} \varphi(t) &= \varphi(t)1_A \\ &= \varphi(t)\sum_{s\in S}(f(s))(t) \\ &= \sum_{s\in S}\varphi(s)(f(s))(t) \\ &= \sum_{s\in S}(\varphi(s)f(s))(t) \\ &= (\sum_{s\in S}\varphi(s)f(s))(t), \end{aligned}$$

para todo $t \in S$, o que implica que $\varphi = \sum_{s\in S}\varphi(s)f(s)$.

Como ψ é um A-homomorfismo tal que $\psi \circ f = g$, então

$$\begin{aligned}
\psi(\varphi) &= \psi(\sum_{s\in S} \varphi(s)f(s)) \\
&= \sum_{s\in S} \varphi(s)\psi(f(s)) \\
&= \sum_{s\in S} \varphi(s)(\psi \circ f)(s) \\
&= \sum_{s\in S} \varphi(s)g(s) \\
&= h(\varphi).
\end{aligned}$$

Portanto $\psi = h$ e, consequentemente, segue que $(F; f)$ um A-módulo livre sobre S. □

Definição 2.0.5. *Sejam M um A-módulo e S um conjunto não vazio. Se M é isomorfo a um A-módulo livre $(F; f)$ sobre S, diremos que M é um A-módulo livre.*

Definição 2.0.6. *Seja M um A-módulo e $X = \{x_1, x_2, ..., x_m\} \subset M$. Diremos que X é linearmente dependente (LD) se existem escalares $\alpha_1, \alpha_2, ..., \alpha_m \in A$, não todas nulas, tais que $\sum_{i=1}^{n} \alpha_i x_i = 0_M$. Caso contrário, diremos que X é linearmente independente (LI).*

Exemplo 2.0.7. *Considere o $\mathbb{Z}$-módulo $\mathbb{Z}_4$. $S = \{\overline{1}\}$ é LD, pois $4.\overline{1} = \overline{0}$ e $4 \neq 0$.*

Exemplo 2.0.8. *Considere o $\mathbb{Z}^{\mathbb{Z}}$. $S_1 = \{1\}$ é LI, pois $a \cdot 1 = 0$ implica $a = 0$. Por outro lado, $S_2 = \{2, 3\}$ é LD, pois $3.2 + (-2).3 = 0$. Em geral, qualquer conjunto com dois ou mais elementos de $\mathbb{Z}$ é um conjunto LD do $\mathbb{Z}^{\mathbb{Z}}$, pois dado $\beta = \{a, b\} \subset \mathbb{Z}$, com $a \neq b$, de $(-b)a + ab = 0$, segue que $\beta = \{a, b\}$ é LD.*

Exemplo 2.0.9. *Considere o $\mathbb{Z}$-módulo $\mathbb{Z} \bigoplus \mathbb{Z}$. Notemos que $S = \{(1, 0), (0, 1)\}$ é LI, pois $a(1, 0) + b(0, 1) = (0, 0)$ implica $(a, b) = (0, 0)$, ou seja, $a = b = 0$.*

Definição 2.0.10. *Sejam M um A-módulo e $S \subset M$. Diremos que S é LI se cada subconjunto finito de S é LI. Caso contrário, diremos que S é LD.*

Exemplo 2.0.11. *Sejam M um A-módulo e $S \subset M$. Se $S = \{0_M\}$, então S é LD.*

Observação 2.0.12. *Sejam M um A-módulo e $X \subset M$. Se um conjunto $Y \subset X$ é LD, então X é LD.*

Observação 2.0.13. *Em um espaço vetorial V, se $S = \{u\}$, com $u \neq 0_V$, então S é LI. Se M é um A-módulo e $S = \{m\} \subset M$, com $m \neq 0_M$, S pode ser LD, basta notar o Exemplo 2.0.7.*

Definição 2.0.14. *Sejam M um A-módulo e $S \subset M$. Se S é LI e gera M, então diremos que S é uma base de M.*

Exemplo 2.0.15. *$S = \{2, 3\}$ gera o $\mathbb{Z}^{\mathbb{Z}}$, pois de $(2, 3) = 1$, existem $x_0, y_0 \in \mathbb{Z}$ tais que $2x_0 + 3y_0 = 1$. Então $m = 2(mx_0) + 3(my_0)$, para todo $m \in \mathbb{Z}$. No entanto, S é LD, conforme mostrado no Exemplo 2.0.8. Deste modo, $S = \{2, 3\}$ não é uma base do $\mathbb{Z}^{\mathbb{Z}}$.*

Exemplo 2.0.16. *Considere $N = (((1, 1), (-1, 1)))$ um submódulo do $\mathbb{Z}$-módulo $\mathbb{Z} \bigoplus \mathbb{Z}$. Notemos que $N \neq \mathbb{Z} \bigoplus \mathbb{Z}$, pois $(1, 0) \notin N$. Como $a(1, 1) + b(-1, 1) = (0, 0)$, tem-se $(a - b, a + b) = (0, 0)$ e, consequentemente, $a - b = 0 = a + b$, ou seja, $a = b = 0$. Logo $S = \{(1, 1), (-1, 1)\}$ é LI. Como S gera N, concluímos que S é uma base de N.*

É interessante notar que nem todo A-módulo M admite uma base. Vejamos alguns exemplos:

Exemplo 2.0.17. *Sejam A um anel e I um ideal próprio à esquerda de A. $\dfrac{A}{I}$ é um A-módulo que não admite uma base, pois para qualquer $S = \{\overline{a}\} \subset \dfrac{A}{I}$ com $\overline{a} \neq \overline{0}$, tem-se que $x\overline{a} = \overline{xa} = \overline{0}$, para $x \in I - \{0_A\}$, o que implica que S é LD.*

Exemplo 2.0.18. *$\mathbb{Q}$ é um $\mathbb{Z}$-módulo que não admite uma base.*

Demonstração. De fato, pelo Exemplo 1.1.14, $\mathbb{Q}$ é um $\mathbb{Z}$-módulo não finitamente gerado. □

Teorema 2.0.19. *Sejam M um A-módulo não nulo e $S \subset M$ não vazio. S é uma base de M se, e somente se, cada elemento $m \in M$ possui uma representação única na forma $m = \sum_{i=1}^{r} \alpha_i x_i$, com $x_i \in S$ e $\alpha_i \in A$, para todo $i \in \{1, 2, ..., r\}$.*

Demonstração. A existência de tal representação é consequência direta da definição de base. Suponhamos que $m = \sum_{i=1}^{r} \alpha_i x_i = \sum_{j=i}^{s} \beta_j y_j$, sendo $x_1, x_2, ..., x_r, y_1, y_2, ..., y_s \in S$, com $x_i \neq x_j$ e $y_i \neq y_j$, para $j \neq i$. Desta forma, $\sum_{i=1}^{r} \alpha_i x_i + \sum_{j=1}^{s} (-\beta_j) y_j = 0$. A independência linear de S nos mostra que para x_i e y_j distintos, tem-se que $\alpha_i = \beta_j = 0$ e quando $x_i = y_j$, tem-se $\alpha_i = \beta_j$. Portanto, m admite uma única representação como combinação linear de elementos de S.

Reciprocamente, por hipótese, segue que S gera M. Como 0_M pode ser expresso de modo único como combinação linear de elementos de S, segue que S é LI. Portanto S é uma base de M. □

Exemplo 2.0.20. *Se A é um anel e $n \in \mathbb{N}^*$, então $A^n = \{A \times A \times ... \times A\}$ é um A-módulo com base $S = \{e_1, e_2, ..., e_n\}$ sendo $e_i = (0_A, 0_A, ..., 0_A, 1_A, 0_A, ..., 0_A)$, onde o i-ésimo termo é igual ao elemento unidade e os demais são todos nulos.*

Demonstração. De fato, como $(a_1, a_2, ..., a_n) \in A^n$ é escrito de modo único como

$$\begin{aligned}(a_1, a_2, ..., a_n) &= a_1(1_A, 0_A, ..., 0_A) + ... + a_n(0_A, 0_A, ..., 1_A) \\ &= \sum_{i=1}^{n} a_i e_i,\end{aligned}$$

o que implica que $S = \{e_1, e_2, ..., e_n\}$ é uma base do A-módulo A^n. □

Teorema 2.0.21. *Se (F, f) é um A-módulo livre sobre S, então $Im(f)$ é uma base de F.*

Demonstração. Vamos considerar o A-módulo (F, f) construído na prova do Teorema 2.0.4. Assim, $\varphi = \sum_{s \in S} \varphi(s) f(s)$, para todo $\varphi \in F$. Do Teorema 2.0.2, segue que $Im(f)$ gera F. Suponhamos que $\sum_{i=1}^{m} \alpha_i f(x_i) = \sum_{i=1}^{m} \beta_i f(x_i)$, onde $f(x_i), f(x_2), ..., f(x_m)$ são elementos distintos dois a dois da $Im(f)$.

Para todo $i \in \{1, 2, ..., m\}$, sejam ε_1, $\varepsilon_2 : S \to A$, aplicações definidas por

$$\varepsilon_1(x) = \begin{cases} 0_A, & \text{se} \quad x \neq x_i; \\ \alpha_i, & \text{se} \quad x = x_i. \end{cases}$$

$$\varepsilon_2(x) = \begin{cases} 0_A, & \text{se} \quad x \neq x_i; \\ \beta_i, & \text{se} \quad x = x_i. \end{cases}$$

Assim, $\varepsilon_1, \varepsilon_2 \in F$ são tais que

$$\begin{aligned}\varepsilon_1 &= \sum_{s \in S} \varepsilon_1(s) f(s) \\ &= \sum_{i=1}^{m} \varepsilon_1(x_i) f(x_i) \\ &= \sum_{i=1}^{m} \alpha_i f(x_i)\end{aligned}$$

e

$$\begin{aligned}\varepsilon_2 &= \sum_{s\in S}\varepsilon_2(s)f(s)\\ &= \sum_{i=1}^{m}\varepsilon_2(x_i)f(x_i)\\ &= \sum_{i=1}^{m}\beta_i f(x_i).\end{aligned}$$

Logo, $\varepsilon_1 = \varepsilon_2$ e, consequentemente, $\alpha_i = \beta_i$, para todo $i \in \{1, 2, ..., m\}$. Portanto, pelo Teorema 2.0.19, $Im(f)$ é uma base de F. □

Teorema 2.0.22. *Seja $f : M \to N$ um A-isomorfismo. Se $X = (x_i)_{i\in I}$ é uma base de M, então $f(X) = (f(x_i))_{i\in I}$ é uma base de N.*

Demonstração. Tome $y \in N = f(M)$ qualquer. Assim, existe $x \in M$ tal que $y = f(x)$. De $x \in M$, existem escalares α_i tais que $x = \sum_{i\in I}\alpha_i x_i$. Desta forma,

$$y = f(x) = f(\sum_{i\in I}\alpha_i x_i) = \sum_{i\in I}\alpha_i f(x_i),$$

o que implica que $(f(x_i))_{i\in I}$ gera N.

Tome $S = \{f(x_1), ..., f(x_n)\} \subset f(X)$ e seja $\alpha_1 f(x_1) + ... + \alpha_n f(x_n) = 0_N$. Deste modo, $f(\alpha_1 x_1 + ... + \alpha_n x_n) = 0_N$, o que implica que $\alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_n x_n \in Ker(f) = \{0_M\}$, ou seja, $\alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_n x_n = 0_M$. Como $S_1 = \{x_1, x_2, ..., x_n\} \subset X$ é LI, segue que $\alpha_1 = \alpha_2 = ... = \alpha_n = 0_A$. Logo, S é LI e, consequentemente, $f(X)$ é LI. Portanto $f(X)$ é uma base de N. □

Teorema 2.0.23. *Um A-módulo M é livre se, e somente se, M admite uma base.*

Demonstração. Suponhamos que M seja um A-módulo livre. Assim, existe $(F; f)$ um A-módulo livre sobre um conjunto não vazio S tal que $F \cong M$. Desta forma, existe um A-isomorfismo $\psi : F \to M$. Como a $Im(f)$ é uma base de F e, pelo Teorema 2.0.22, ψ leva base em base, então M admite uma base.

Reciprocamente, suponhamos que S seja uma base de M. Seja $(F; f)$ um A-módulo livre sobre S. Considere $I_S : S \to M$ a inclusão de S em M. Como $(F; f)$ é um A-módulo livre sobre S, existe um único A-homomorfismo $h : F \to M$ tal que $h \circ f = I_S$. De $h \circ f = I_S$, segue que $Im(h)$ é um submódulo de M, sendo $S \subset Im(h) \subset M$. Como

S gera M, tem-se que $Im(h) = M$, ou seja, h é um A-epimorfismo. Por outro lado, tome $\varphi \in Ker(h) \subset F = ((Im(f)))$. Desta forma, existe $\{s_1, s_2, ..., s_n\} \subset S$ tal que $\varphi = \sum_{i=1}^{n} \varphi(s_i) f(s_i)$. Logo,

$$\begin{aligned} 0_M &= h(\varphi) = h(\sum_{i=1}^{n} \varphi(s_i) f(s_i)) \\ &= \sum_{i=1}^{n} \varphi(s_i) h(f(s_i)) \\ &= \sum_{i=1}^{n} \varphi(s_i)(h \circ f)(s_i) \\ &= \sum_{i=1}^{n} \varphi(s_i) I_S(s_i) \\ &= \sum_{i=1}^{n} \varphi(s_i) s_i. \end{aligned}$$

Como $\{s_1, s_2, ..., s_n\} \subset S$ e S é LI, segue que $\varphi(s_i) = 0_A$, para $i \in \{1, 2, ..., n\}$, o que implica que $\varphi = 0_F$. Logo, $Ker(\varphi) = \{0_F\}$ e, consequentemente, h é um A-monomorfismo. Portanto, h é um A-isomorfismo, o que implica que (M, I_S) é um A-módulo livre sobre S.

□

Corolário 2.0.24. *Sejam M, N A-módulos e $f : M \to N$ um A-isomorfismo. M é livre se, e somente se, N é livre.*

Demonstração. Decorre imediatamente dos teoremas 2.0.22 e 2.0.23. □

Exemplo 2.0.25. *O $\mathbb{Z}$-módulo $\mathbb{Q}$ não é livre, pois não admite uma base.*

Exemplo 2.0.26. *Não existe $\mathbb{Z}$-isomorfismo $f : \mathbb{Z} \to \mathbb{Q}$.*

Com efeito, suponha que $f : \mathbb{Z} \to \mathbb{Q}$ seja um $\mathbb{Z}$-isomorfismo. Como $\mathbb{Z}^{\mathbb{Z}}$ é um $\mathbb{Z}$-módulo livre, então $\mathbb{Q} = f(\mathbb{Z})$ é um $\mathbb{Z}$-módulo livre, o que é um absurdo, pois $\mathbb{Q}$ é um $\mathbb{Z}$-módulo que não admite uma base. Portanto não existe tal $\mathbb{Z}$-isomorfismo.

Corolário 2.0.27. *Se $\{a_i;\, i \in I\}$ é uma base do A-módulo M, então*

1) $M = \bigoplus_{i \in I} ((a_i))$.

2) $((a_i)) \cong A^A$, *para todo* $i \in I$.

Demonstração. Como $X = (a_i)_{i\in I}$ é uma base de M, para cada $m \in M$, tem-se $m = \sum_{i\in I} \alpha_i a_i$, onde $\alpha_i = 0$, para todo $i \in I$, exceto para um número finito de índices i. Como $\alpha_i a_i \in ((a_i))$, para todo $i \in I$, concluímos que $M = \bigoplus_{i\in I}((a_i))$.

Por outro lado, como X é uma base de M, então cada subconjunto unitário $\{a_i\}$ é LI. Deste modo, a aplicação $f_i : A^A \to ((a_i))$, dada por $f_i(\alpha) = \alpha a_i$ é um A-isomorfismo. Portanto $A^A \cong ((a_i))$, para todo $i \in I$. □

Exemplo 2.0.28. *Se A é um anel e I é um ideal próprio à esquerda, então o A-módulo $\frac{A}{I}$ não é livre.*

Exemplo 2.0.29. *$S = \{\mu\}$ é uma base do A^A se, e somente se, μ é um elemento inversível do anel A.*

De fato, como S é uma base de A^A, existe $\alpha \in A$ tal que $\alpha\mu = 1_A$. Logo, μ é um elemento inversível do anel A.

Reciprocamente, suponha que μ seja um elemento inversível de A. Assim, $S = \{\mu\}$ é LI, pois $a\mu = 0_A$, implica em $(a\mu)\mu^{-1} = 0_A$ e, consequentemente, $a = 0_A$. Por outro lado, dado $a \in A$ qualquer, tem-se que $a = (a\mu^{-1})\mu$, o que implica que S gera A^A. Portanto, $S = \{\mu\}$ é uma base de A^A.

Exemplo 2.0.30. *Com base no Exemplo 2.0.29, $S = \{1\}$ e $S = \{-1\}$ são as únicas bases do $\mathbb{Z}$-módulo $\mathbb{Z}^{\mathbb{Z}}$.*

Em geral, não é verdade que todo subconjunto LI, de um A-módulo livre, possa ser completado até formar uma base. Como exemplo para ilustrar esse fato, tome o $\mathbb{Z}^{\mathbb{Z}}$. Sabemos que ele é livre e que o conjunto $\{2\}$ é LI. No entanto, ele não é base e nem pode ser ampliado para uma base, pois todo conjunto com dois ou mais elementos do $\mathbb{Z}^{\mathbb{Z}}$ é linearmente dependente (Exemplo 2.0.8). Um outro fato interessante é que nem todo conjunto gerador contém uma base. Novamente podemos tomar como exemplo o $\mathbb{Z}^{\mathbb{Z}}$ e o conjunto $\{2, 3\}$. Pelo Exemplo 2.0.8, $\{2, 3\}$ gera todo módulo, porém ele não contém nenhuma base, pois $\{2\}$ e $\{3\}$ não são bases de $\mathbb{Z}^{\mathbb{Z}}$.

Observação 2.0.31. *Nem sempre um submódulo de um A-módulo livre é livre. Por exemplo, o $\mathbb{Z}_4^{\mathbb{Z}_4}$ é um módulo livre com base $\{\overline{1}\}$, cujo submódulo $S = \{\overline{0}, \overline{2}\}$ não é livre, pois todo subconjunto unitário de S é LD.*

Observação 2.0.32. *Seja M um A-módulo livre e $S \subsetneq M$ um submódulo livre de M. Nem sempre é verdade que o número de elementos de uma base de S é menor do que o número de elementos de uma base de M. Por exemplo, o $\mathbb{Z}$-módulo $\mathbb{Z} \bigoplus \mathbb{Z}$ e o seu submódulo $S = (((1,1),(-1,1)))$ são livres, sendo $\{(1,0),(0,1)\}$ uma base de $\mathbb{Z} \bigoplus \mathbb{Z}$ e $\{(1,1),(-1,1)\}$ uma base de S. Note que $S \subsetneq \mathbb{Z} \bigoplus \mathbb{Z}$, pois $(1,0)$, $(0,1) \notin S$.*

Observação 2.0.33. *Se V e W são espaços vetoriais de dimensão finita sobre o mesmo corpo K, tais que $dim(V) = dim(W)$ e $\psi : V \to W$ é uma transformação linear, então ψ é injetora se, e somente se, ψ é sobrejetora. Esse fato, em geral, é falso para A-módulos livres com bases finitas. Como exemplo, considere o A-homomorfismo $\psi : \mathbb{Z}^{\mathbb{Z}} \to \mathbb{Z}^{\mathbb{Z}}$ dado por $\psi(m) = 2m$. $\{1\}$ é uma base do $\mathbb{Z}^{\mathbb{Z}}$, ψ é injetora mas não é sobrejetora.*

Corolário 2.0.34. *Se M é um A-módulo tal que $M \cong \bigoplus_{i \in I} A^A$, então M é um A-módulo livre.*

Demonstração. Para cada $i \in I$, considere a aplicação

$$\begin{aligned} \mu_i : A &\longrightarrow \bigoplus_{i \in I} A^A \\ a &\longmapsto (x_j)_{j \in I}, \end{aligned}$$

sendo

$$x_j = \begin{cases} 0_A, & \text{se} \quad j \neq i; \\ a, & \text{se} \quad j = i. \end{cases}$$

Considere $B = \{(\mu_i(1_A))_{i \in I}\}$.

Afirmação: B é uma base de $\bigoplus_{i \in I} A^A$.

De fato, tome $z \in \bigoplus_{i \in I} A^A$ qualquer. Assim, $z = (x_i)_{i \in I}$, onde $x_i \in A$ e $x_i = 0_A$, para todo $i \in I$, exceto para um número finito de índices i.

$$\begin{aligned} z &= (x_i)_{i \in I} \\ &= \sum_{i \in I} \mu_i(x_i) \\ &= \sum_{i \in I} x_i \mu_i(1_A), \end{aligned}$$

o que implica que B gera $\bigoplus_{i \in I} A^A$. Por outro lado, considere $\{\mu_1(1_A), ..., \mu_n(1_A)\}$ um subconjunto finito de B e escalares $a_1, ..., a_n \in A$ tais que $a_1\mu_1(1_A) + ... + a_n\mu_n(1_A) = 0_A$.

Seja $z = (z_i)_{i\in I} \in \bigoplus_{i\in I} A^A$, dado por

$$z_i = \begin{cases} 0_A, & \text{se} \quad i \notin \{1, 2, ..., n\}; \\ a_i, & \text{se} \quad i \in \{1, 2, ..., n\}. \end{cases}$$

Assim,

$$\begin{aligned} z &= \sum_{i\in I} z_i\mu_i(1_A) \\ &= \sum_{i=1}^{n} a_i\mu_i(1_A) \\ &= 0_A. \end{aligned}$$

Desta forma, $a_i = 0_A$, para $i \in \{1, 2, 3, ..., n\}$, o que implica que $\{\mu_1(1_A), ..., \mu_n(1_A)\}$ é LI. Logo B é LI e, consequentemente, B é uma base de $\bigoplus_{i\in I} A^A$. Como $M \cong \bigoplus_{i\in I} A^A$ e $\bigoplus_{i\in I} A^A$ é um A-módulo livre, pelo Teorema 2.0.22, concluímos que M é um A-módulo livre. □

Teorema 2.0.35. *Um A-módulo M é livre se, e somente se, $M \cong \bigoplus_{i\in I} A^A$.*

Demonstração. Decorre dos corolários 2.0.27 e 2.0.34. □

Teorema 2.0.36. *Sejam M um A-módulo livre e $X = \{x_i;\ i \in I\}$ uma base de M. Se N é um A-módulo e $(b_i)_{i\in I}$ é uma família de elementos de N, então existe um único A-homomorfismo $f : M \to N$ tal que $f(x_i) = b_i$, para todo $i \in I$.*

Demonstração. Como X é uma base de M, pelo Corolário 2.0.27, item (a), $M = \bigoplus_{i\in I}((x_i))$. Dado $m \in M$ qualquer, podemos escrever, de modo único, $m = \sum_{i\in I} \alpha_i x_i$. Deste modo, considere $f : M \to N$ uma aplicação dada por $f(\sum_{i\in I} \alpha_i x_i) = \sum_{i\in I} \alpha_i b_i$. A aplicação f está bem definida, pois dado $x = \sum_{i\in I} \alpha_i x_i \in \bigoplus_{i\in I}((x_i))$, onde $\alpha_i = 0$, para todo $i \in I$, exceto para um número finito de índices i, o que implica que $\sum_{i\in I} \alpha_i b_i$ é finita.

Notemos que $x_i = \sum_{j\in I} \alpha_j x_j$, sendo $\alpha_j = \begin{cases} 1_A, & \text{se} \quad j = i; \\ 0_A, & \text{se} \quad j \neq i. \end{cases}$. Deste modo,

$$f(x_i) = f(\sum_{j\in I} \alpha_j x_j) = \sum_{j\in I} \alpha_j b_j = b_i.$$

Além disso, f é um A-homomorfismo, pois dado $x = \sum_{i\in I} \alpha_i x_i$, $y = \sum_{i\in I} \beta_i x_i$ e $\alpha \in A$ quaisquer, tem-se

$$\begin{aligned} f(\alpha x + y) &= f(\alpha \sum_{i\in I} \alpha_i x_i + \sum_{i\in I} \beta_i x_i) \\ &= f(\sum_{i\in I} (\alpha\alpha_i + \beta_i) x_i) \\ &= \sum_{i\in I} (\alpha\alpha_i + \beta_i) b_i \\ &= \alpha \sum_{i\in I} \alpha_i b_i + \sum_{i\in I} \beta_i b_i = \alpha f(x) + f(y). \end{aligned}$$

Suponhamos que $g : M \to N$ seja um A-homomorfismo tal que $g(x_i) = b_i$, para todo $i \in I$. Assim, dado $x = \sum_{i\in I} \alpha_i x_i \in M$, tem-se

$$\begin{aligned} g(x) &= g(\sum_{i\in I} \alpha_i x_i) \\ &= \sum_{i\in I} g(\alpha_i x_i) \\ &= \sum_{i\in I} \alpha_i g(x_i) \\ &= \sum_{i\in I} \alpha_i b_i = f(x). \end{aligned}$$

Portanto, $f(x) = g(x)$, para todo $x \in M$ e, consequentemente, $f = g$. □

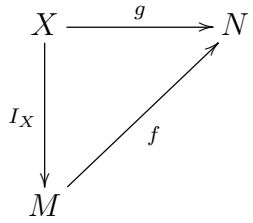
Corolário 2.0.37. *Sejam $X = (x_i)_{i\in I}$ um subconjunto não vazio de um A-módulo M e $I_X : X \to M$ a inclusão natural. Então X é uma base de M se, e somente se, (M, I_X) é um A-módulo livre sobre X.*

Demonstração. Suponha que $X = (x_i)_{i\in I}$ é uma base do A-módulo M. Considere N um A-módulo e $g : X \to N$ uma aplicação tal que $g(x_i) = b_i \in N$, para todo $i \in I$. Pelo Teorema 2.0.36, existe um único A-homomorfismo $f : M \to N$ tal que $f(x_i) = b_i$, para todo $i \in I$. Desta forma, para todo $x_i \in X$, segue que

$$\begin{aligned} b_i &= f(x_i) \\ &= f(I_X(x_i)) \\ &= (f \circ I_X)(x_i), \end{aligned}$$

o que implica que $f : M \to N$ é o único A-homomorfismo tal que o diagrama abaixo

comuta.

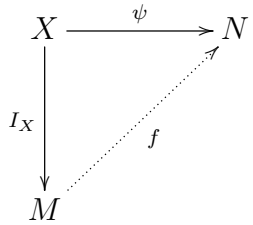


Portanto (M, I_X) é um A-módulo livre sobre X.

Reciprocamente, suponha que (M, I_X) seja um A-módulo livre sobre X. Assim, pelo Teorema 2.0.21, $Im(I_X) = X$ é uma base de M. □

Corolário 2.0.38. *Sejam M e N A-módulos. Se X é uma base do A-módulo M e $\psi : X \to N$ é uma aplicação, então existe um único A-homomorfismo $f : M \to N$ tal que $f|_X = \psi$.*

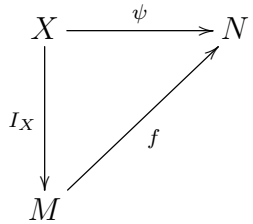
Demonstração. Se X é uma base de M, então pelo Corolário 2.0.37, (M, I_X) é um A-módulo livre sobre X. Assim, dado o diagrama abaixo



existe um único A-homomorfismo $f : M \to N$ tal que o diagrama comuta, isto é, $f \circ I_X = \psi$. Deste modo, $f(x_i) = \psi(x_i)$, para todo $x_i \in X$, ou seja, $f|_X = \psi$. □

Corolário 2.0.39. *Sejam M e N A-módulos. Se X é um subconjunto não vazio de M, $\psi : X \to N$ é uma aplicação e existe um único A-homomorfismo $f : M \to N$ tal que $f|_X = \psi$ então, X é uma base de M.*

Demonstração. De $f|_X = \psi$, tem-se $f(x_i) = \psi(x_i)$, o que implica que $(f \circ I_X)(x_i) = \psi(x_i)$, para todo $x_i \in X$, ou seja, $f \circ I_X = \psi$. Assim, f é o único A-homomorfismo que comuta o diagrama a seguir.



Logo (M, I_X) é um A-módulo livre sobre X e, pelo Corolário 2.0.37, X é uma base de M. □

Corolário 2.0.40. *Seja $f : M \to N$ um A-homomorfismo onde $X = (x_i)_{i\in I}$ é uma base de M. Se $f(x_i) = 0_N$, para todo $i \in I$, então $f = 0$.*

Demonstração. Como o A-homomorfismo nulo $0 : M \to N$ é tal que $0(x_i) = 0_N$, para todo $x_i \in X$, do Teorema 2.0.36, segue que $f = 0$. □

Corolário 2.0.41. *Se $f, g : M \to N$ são A-homomorfismos, $X = (x_i)_{i\in I}$ uma base de M e $f(x_i) = g(x_i)$, para todo $x_i \in X$, então $f = g$.*

Demonstração. Considere o A-homomorfismo $f - g$. Como $(f - g)(x_i) = 0$, para todo $x_i \in X$, então $f - g = 0$, ou seja, $f = g$. □

Observação 2.0.42. *Dado um A-módulo M arbitrário, é possível determinar um conjunto de geradores de M, pois na pior das hipóteses, podemos tomar como gerador o próprio M. No entanto, como vimos anteriormente, nem todo A-módulo é livre.*

Teorema 2.0.43. *Todo A-módulo M é isomorfo a um quociente de um A-módulo livre.*

Demonstração. Sejam M um A-módulo, $\{x_i\}_{i\in I}$ um conjunto de geradores de M e $X = \{e_i\}_{i\in I}$ uma base de $\bigoplus_{i\in I} A^A$. Considere $\psi : X \to M$ dada por $\psi(e_i) = x_i$, para todo $i \in I$. Pelo Corolário 2.0.38, existe único A-homomorfismo $f : \bigoplus_{i\in I} A^A \to M$ tal que $f|_X = \psi$. Notemos que f é um A-epimorfismo, pois dado $y \in M$, tem-se $y = \sum_{i\in I} \alpha_i x_i$, com $x_i \in A$ e segue que

$$y = \sum_{i\in I} \alpha_i x_i = \sum_{i\in I} \alpha_i f(e_i) = \sum_{i\in I} f(\alpha_i e_i) = f(\sum_{i\in I} \alpha_i e_i).$$

Portanto, pelo Teorema 1.3.15, $M \cong \dfrac{\bigoplus_{i\in I} A^A}{Ker(f)}$. □

Teorema 2.0.44. *Todo A-módulo finitamente gerado é imagem de algum A-módulo livre cujas as bases são todas finitas.*

Demonstração. 0 Seja $M = ((x_1, x_2, ..., x_n))$. Considere o A-módulo $A^n = A \times A \times ... \times A$. A^n é um A-módulo livre e $X = \{e_1, e_2, ..., e_n\}$ é uma base de A^n. Considere a aplicação

$$\begin{aligned} \psi : X &\longrightarrow M \\ e_i &\longmapsto x_i. \end{aligned}$$

Do Corolário 2.0.38, podemos estender ψ a um A-homomorfismo $\tilde{\psi} : A^n \to M$. $\tilde{\psi}$ é um A-epimorfismo, pois dado $m \in M$ qualquer, existem escalares $\alpha_1, \alpha_2, ..., \alpha_n$ tais que $m = \sum_{i=1}^{n} \alpha_i x_i$. Logo,

$$\begin{aligned} m &= \sum_{i=1}^{n} \alpha_i x_i \\ &= \sum_{i=1}^{n} \alpha_i \psi(e_i) \\ &= \sum_{i=1}^{n} \alpha_i \tilde{\psi}(e_i) \\ &= \sum_{i=1}^{n} \tilde{\psi}(\alpha_i e_i) \\ &= \tilde{\psi}(\sum_{i=1}^{n} \alpha_i e_i). \end{aligned}$$

Portanto, M é imagem de um A-módulo livre de bases finitas. □

Teorema 2.0.45. *Todo A-módulo livre finitamente gerado admite uma base finita.*

Demonstração. Seja M um A-módulo livre com uma base X. Considere $m_1, m_2, ..., m_r$ elementos em M tais que $M = ((m_1, m_2, ..., m_r))$. Como X é uma base de M, para cada m_i, com $i \in \{1, 2, ..., n\}$, existe um subconjunto finito $X_i \subset X$ tal que $m_i \in ((X_i))$. Daí resulta que $X_0 = \bigcup_{i=1}^{n} X_i$ gera M, ou seja, $M = ((X_0))$. Como $X_0 \subset X$ e X_i é finito para cada $i \in \{1, 2, 3, ..., n\}$, segue que X_0 é finito e LI. Portanto, X_0 é uma base finita de M. □

Teorema 2.0.46. *M é um A-módulo finitamente gerado se, e somente se, M é isomorfo a um quociente de A^n, para algum inteiro $n > 0$.*

Demonstração. Seja $m_1, m_2, m_3..., m_n \in M$ tais que $M = ((m_1, m_2, m_3..., m_n))$. Defina $f : A^n \to M$ dada por $f(a_1, a_2, ..., a_n) = a_1 m_1 + a_2 m_2 + ... + a_n m_n$. Assim, f é um A-epimorfismo e $\dfrac{A^n}{Ker(f)} \cong M$.

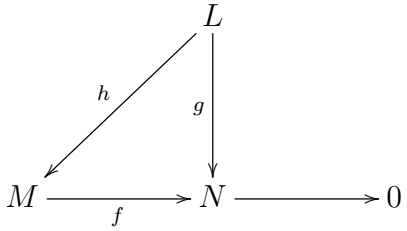
Reciprocamente, seja N um submódulo de A^n, tal que $\psi : \dfrac{A^n}{N} \to M$ seja um A-isomorfismo. Considere $f : A^n \to M$ um A-homomorfismo dada por $f = \psi \circ \pi$, onde $\pi : A^n \to \dfrac{A^n}{N}$ é a projeção canônica. Tome $m \in M = Im(f)$ qualquer. Desta forma,

existe $(a_1, a_2, ..., a_n) \in A^n$ tal que $f(a_1, a_2, ..., a_n) = m$. Deste modo

$$\begin{aligned} m &= f(a_1, a_2, ..., a_n) \\ &= f(a_1e_1 + ... + a_ne_n) \\ &= a_1f(e_1) + a_2f(e_2) + ... + a_nf(e_n), \end{aligned}$$

o que implica que $M = ((f(e_1), f(e_2), ..., f(e_n)))$. Portanto, M é um A-módulo finitamente gerado. □

Teorema 2.0.47. *Seja L um A-módulo livre. Dados M e N A-módulos, $f : M \to N$ um A-epimorfismo e um A-homomorfismo $g : L \to N$, sempre existe um homomorfismo $h : L \to M$ tal que $h \circ f = g$.*



Demonstração. Seja $X = (x_i)_{i \in I}$ uma base de L. Considere $y_i = g(x_i)$, com $x_i \in X$. Como f é um A-epimorfismo, existem $m_i \in M$ tal que $f(m_i) = y_i$, para todo $i \in I$. Definamos $\tilde{h} : X \to M$ dada por $\tilde{h}(x_i) = m_i$. Assim, pelo Corolário 2.0.38, existe um único A-homomorfismo $h : L \to M$ tal que $h \mid_X = \tilde{h}$. Tome $m \in L$ qualquer. Deste modo, existe um subconjunto finito $\{x_1, x_2, ..., x_r\} \subset X$ tal que $m = \alpha_1x_1 + \alpha_2x_2 + ... + \alpha_rx_r$. Daí

$$\begin{aligned} h(m) &= \alpha_1h(x_1) + \alpha_2h(x_2) + ... + \alpha_rh(x_r) \\ &= \alpha_1m_1 + \alpha_2m_2 + ... + \alpha_rm_r \end{aligned}$$

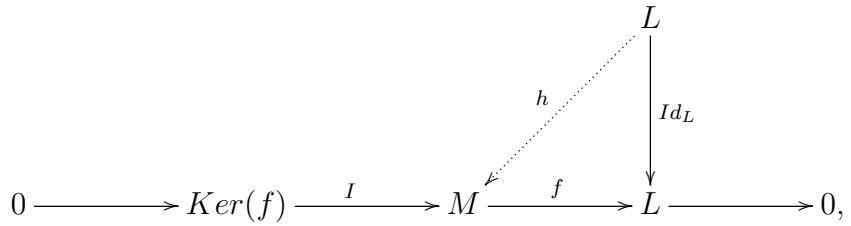
o que implica que,

$$\begin{aligned} (f \circ h)(m) &= \alpha_1f(m_1) + \alpha_2f(m_2) + ... + \alpha_rf(m_r) \\ &= \alpha_1y_1 + \alpha_2y_2 + ... + \alpha_ry_r \\ &= \alpha_1g(x_1) + \alpha_2g(x_2) + ... + \alpha_rg(x_r) \\ &= g(\alpha_1x_1 + \alpha_2x_2 + ... + \alpha_rx_r) \\ &= g(m), \end{aligned}$$

e, portanto, que $f \circ h = g$. □

Teorema 2.0.48. *Se $f : M \to L$ é um A-epimorfismo e L é um A-módulo livre, então $M \cong Ker(f) \bigoplus L$.*

Demonstração. Considere o diagrama abaixo



onde $I : Ker(f) \to M$ é a inclusão. Como L é livre, do Teorema 2.0.47, existe $h : L \to M$ tal que $f \circ h = Id_L$. Deste modo, pelo Teorema 1.6.9, $Ker(f)$ é um somando direto de M. Logo, existe um submódulo M_1 de M tal que $M = Ker(f) \bigoplus M_1$ e, pelo Teorema 1.5.21, segue que $M_1 \cong \dfrac{M}{Ker(f)} \cong L$. Portanto, $M \cong Ker(f) \bigoplus L$. □

Exemplo 2.0.49. *Não existem $\mathbb{Z}$-epimorfismos, não nulos, de $\mathbb{Q}$ sobre um $\mathbb{Z}$-módulo livres.*

Com efeito, suponha que $f : \mathbb{Q} \to L$ seja um $\mathbb{Z}$-epimorfismo, sendo L um $\mathbb{Z}$-módulo livre, com $L \neq \{0\}$. Pelo Teorema 2.0.48, $Ker(f)$ é um somando direto de $\mathbb{Q}$. Como $\mathbb{Q}$ é um $\mathbb{Z}$-módulo irredutível, então $Ker(f) = \{0\}$ ou $Ker(f) = \mathbb{Q}$. Se $Ker(f) = \mathbb{Q}$, então $f = 0$, o que é um absurdo. Se $Ker(f) = \{0\}$, então f é injetora e, portanto, f é um A-isomorfismo. Deste modo, $\mathbb{Q} \cong \mathbb{L}$, o que implica que $\mathbb{Q}$ é um $\mathbb{Z}$-módulo livre, o que é um absurdo. Portanto, tal A-epimorfismo f não existe.

Corolário 2.0.50. *Seja a sequência exata de A-módulo*

$$0 \longrightarrow M \xrightarrow[f]{} N \xrightarrow[g]{} L \longrightarrow 0\ .$$

Se L é livre, a sequência cinde.

Demonstração. Como $g : N \to L$ é um A-epimorfismo e L é um A-módulo livre, então, pelo Teorema 2.0.48, $Ker(g)$ é um somando direto de N. Portanto, a sequência exata de A-módulos cinde. □

Corolário 2.0.51. *Se M é um A-módulo livre e N um submódulo de M tal que $\dfrac{M}{N}$ seja um A-módulo livre, então N é um somando direto de M e todos os seus suplementares são submódulos livres.*

Demonstração. Considere a sequência exata de A-módulos

$$0 \longrightarrow N \xrightarrow[i]{} M \xrightarrow[\pi]{} \frac{M}{N} \longrightarrow 0\,,$$

onde $i : N \to M$ é a inclusão. Como $\frac{M}{N}$ é um A-módulo livre, pelo Corolário 2.0.50, a sequência cinde, ou seja, $N = Ker(\pi)$ é um somando direto de M. Deste modo, existe M_1, submódulo de M, tal que $M = N \bigoplus M_1$. Pelo Teorema 1.5.21, segue que $M_1 \cong \frac{M}{N}$. Como $\frac{M}{N}$ é um A-módulo livre, do Corolário 2.0.24, segue que M_1 é um A-módulo livre. □

Observação 2.0.52. *Nem sempre um somando direto de um A-módulo livre é livre. Por exemplo, o anel $A = \mathbb{Z} \times \mathbb{Z}$ é um A-módulo livre com base $\{(1,1)\}$. Considere $N = (((1,0)))$ um submódulo de A^A. Notemos que $N_1 = (((0,1)))$ é um submódulo de A^A tal que $A^A = N \bigoplus N_1$. No entanto, N não é um somando direto livre de A^A pois $\{(1,0)\}$ é LD, visto que $(0,5)\cdot(1,0) = (0,0)$, onde $(0,5) \neq (0,0)$.*

Teorema 2.0.53. *Se M é um A-módulo livre com uma base infinita, então qualquer outra base de M é infinita.*

Demonstração. Sejam $(e_i)_{i\in I}$ e $(f_j)_{j\in J}$ bases de M, onde I é um conjunto infinito. Suponhamos que J seja finito. Sem perda de generalidade, considere $J = \{1,2,3,...,m\}$. Assim, para cada $j \in J$, existem elementos $a_{j,k} \in A$ e $i_{j,k}$, sendo $k \in \{1,2,...,n_j\}$, tais que $f_j = \sum_{k=1}^{n_j} a_{j,k} e_{i_{j,k}}$. Isto significa que $E = \{e_{i_{1,1}}, ..., e_{i_{1,n_1}}, e_{i_{2,1}}, ..., e_{i_{2,n_2}}, ..., e_{i_{m,nm}}\}$ é um conjunto finito que gera M. Em particular, cada $e_i \notin E$ é uma combinação linear de elementos E, o que contradiz o fato de $(e_i)_{i\in I}$ ser LI. Logo, J é um conjunto infinito. □

Observação 2.0.54. *Vimos que se M é um A-módulo livre que admite uma base finita $\{e_1, e_2, ..., e_n\}$, então $M \cong A^n$. Será que qualquer outra base de M tem a mesma quantidade de elementos?*

Exemplo 2.0.55. *Considere o $\mathbb{R}^{\mathbb{R}}$ e $\mathbb{R}^\infty = \bigoplus_{i=1}^{\infty} \mathbb{R}^{\mathbb{R}}$. Tome $A = End(\mathbb{R}^\infty)$, o conjunto dos $\mathbb{R}$-endomorfismos $f : \mathbb{R}^\infty \to \mathbb{R}^\infty$. Seja $\mathbb{N} = \{1,2,3,...\}$ e defina as seguintes operações em A:*

$$\begin{aligned} (f+g)((\alpha_n)_{n\in\mathbb{N}} &= f((a_n)_{n\in\mathbb{N}}) + g((a_n)_{n\in\mathbb{N}}), \\ (fg)((a_n)_{n\in\mathbb{N}}) &= (f\circ g)((a_n)_{n\in\mathbb{N}}). \end{aligned}$$

É de fácil verificação que $(A,+,\cdot)$ é um anel com elemento unidade. Notemos que $\mathbb{R}^\infty$

é um $\mathbb{R}$-módulo livre, pois $X = \{e_n;\ n \in \mathbb{N}^*\}$, onde $e_n = (x_k)_{k\in\mathbb{N}} = \begin{cases} 0, & se \quad k \neq n; \\ 1, & se \quad k = n. \end{cases}$ é uma base de $\mathbb{R}^\infty$.

Considere $\tilde{f}_1,\ \tilde{f}_2 : X \to \mathbb{R}^\infty$, aplicações dadas por

$$\tilde{f}_1(e_n) = \begin{cases} e_{\frac{n}{2}}, & se \quad n \text{ é par}; \\ 0_n, & se \quad n \text{ é ímpar}. \end{cases}$$

$$\tilde{f}_2(e_n) = \begin{cases} 0_n, & se \quad n \text{ é par}; \\ e_{\frac{n+1}{2}}, & se \quad n \text{ é ímpar}. \end{cases},$$

onde $0_n = (x_n)_{n\in\mathbb{N}}$, com $x_n = 0$, para todo $n \in \mathbb{N}$. Como X é uma base de $\mathbb{R}^\infty$, existem $\mathbb{R}$-endomorfismos $f_1, f_2 : \mathbb{R}^\infty \to \mathbb{R}^\infty$ tais que $f_1 \mid_X = \tilde{f}_1$ e $f_2 \mid_X = \tilde{f}_2$.

Afirmação: *$\{f_1, f_2\}$ é uma base de A^A.*

De fato, tome $g \in A^A$ qualquer. Considere as aplicações $\tilde{\theta}_1,\ \tilde{\theta}_2 : X \to \mathbb{R}^\infty$, dadas por $\tilde{\theta}_1(e_n) = g(e_{2n})$ e $\tilde{\theta}_2(e_n) = g(e_{2n-1})$. Assim, pelo Corolário 2.0.38, existem $\mathbb{R}$-endomorfismos $\theta_1,\ \theta_2 : \mathbb{R}^\infty \to \mathbb{R}^\infty$ tais que $\theta_1 \mid_X = \tilde{\theta}_1$ e $\theta_2 \mid_X = \tilde{\theta}_2$. De

$$\begin{aligned} (\theta_1 \circ f_1 + \theta_2 \circ f_2)(e_{2n}) &= \theta_1(f_1(e_{2n})) + \theta_2(f_2(e_{2n})) \\ &= \theta_1(f_1(e_{2n})) \\ &= \theta_1(e_n) = g(e_{2n}) \end{aligned}$$

e

$$\begin{aligned} (\theta_1 \circ f_1 + \theta_2 \circ f_2)(e_{2n-1}) &= \theta_1(f_1(e_{2n-1})) + \theta_2(f_2(e_{2n-1})) \\ &= \theta_2(f_2(e_{2n-1})) \\ &= \theta_2(e_n) = g(e_{2n-1}), \end{aligned}$$

segue que $(\theta_1 \circ f_1 + \theta_2 \circ f_2)(e_n) = g(e_n)$, para todo $n \in \mathbb{N}$. Pelo Corolário 2.0.41, $\theta_1 \circ f_1 + \theta_2 \circ f_2 = g$, o que implica que $\{f_1, f_2\}$ gera A^A.

Por outro lado, sejam $\theta_1,\ \theta_2 \in A$ tais que $\theta_1 \circ f_1 + \theta_2 \circ f_2 = 0$. Desta forma, para

todo $n \in \mathbb{N}$ *tem-se que*

$$\begin{aligned} 0_n &= (\theta_1 \circ f_1 + \theta_2 \circ f_2)(e_{2n}) \\ &= \theta_1(f_1(e_{2n})) + \theta_2(f_2(e_{2n})) \\ &= \theta_1(f_1(e_{2n})) \\ &= \theta_1(e_n). \end{aligned}$$

e

$$\begin{aligned} 0_n &= (\theta_1 \circ f_1 + \theta_2 \circ f_2)(e_{2n-1}) \\ &= \theta_1(f_1(e_{2n-1})) + \theta_2(f_2(e_{2n-1})) \\ &= \theta_2(f_2(e_{2n-1})) \\ &= \theta_2(e_n), \end{aligned}$$

o que implica que $\theta_1(e_n) = \theta_2(e_n) = 0_n$*, para todo* $n \in \mathbb{N}$ *e, pelo Corolário 2.0.41, segue que* $\theta_1 = \theta_2 = 0$*. Logo,* $\{f_1, f_2\}$ *é LI e, consequentemente,* $\{f_1, f_2\}$ *é uma base de* A^A*. Portanto,* $\{f_1, f_2\}$ *e* $\{Id_A\}$ *são bases de* A^A*.*

Conclusão

Este trabalho teve como objetivo o desenvolvimento de um material introdutório, em língua portuguesa, de Módulos Livres. Percebemos que ao generalizarmos o conjunto das escalares de um espaço vetorial, ou seja, exigindo que seja apenas um anel, surge uma nova teoria que não preserva todos os resultados obtidos para espaços vetoriais. Um dos resultados mais expressivos é o fato de que nem todo módulo possui uma base. Devido a isso, definimos os módulos livres.

Verificamos que todo módulo livre garante a existência de um conjunto linearmente independente que o gera. Por outro lado, constatamos que nem todo conjunto linearmente independente pode ser completado até formar uma base de um módulo. A única garantia que temos é que se uma base de um módulo livre for finita, então todas as outras também serão. Por fim, mostramos que todo módulo livre, finitamente gerado, possui uma base finita no entanto, esse fato não garante que quaisquer duas bases possuam o mesmo número de elementos.

A Teoria de Módulos serve como base para o estudo de áreas mais avançadas da Álgebra abstrata, como a Álgebra Homológica, Teoria das Categorias e Topologia Álgebrica.

Referências

ADKINS, W. A.; WEINTRAUB, S. H. **Algebra**: An Approach via Module Theory. Nova York: Springer, 1999.

BLYTH, T. S. **Module Theory: An Approach to Linear Algebra**. 2. ed. Oxford: Oxford University Press, 1990.

DORIER, J. A General Outline of the Genesis of Vector Space Theory. **Historia Mathematica**, Amesterdã, v. 22, n. 3, p. 227-261, 1995.

ELIZONDO, L.V. **Notas del curso de Álgebra Moderna III**, 01 de mar. de 2005. 69 f. Notas de Aula.

FERREIROS, J. **Labyrinth of Thought: A History of Set Theory and Its Role in Modern Mathematics**. 2. ed. Basileia: Birkhauser, 2007.

GUCCIONE, J. A.; GUCCIONE, J. J. **ÁLGEBRA**: Grupos Anillos y Módulos, 2011. 84 f. Notas de Aula.

HAWKES, T. O.; HARTLEY, B. **Rings, Module and Algebra Linear**. 1. ed. Londres: Chapman and Hall/CRC, 1970.

JACOBSON, N. **Basic Algebra**. 1. ed. Nova York: W.H.Freeman & Co Ltd, 1974.

LAM, T. Y. **A First Course in Noncommutative Rings**. 2. ed. Nova York: Springer, 2001.

LANG, S. **Algebra**: Graduate Texts in Mathematics. 3. ed. Nova York: Springer, 2005.

MILIES, C. P. **Anéis e módulos**. São Paulo: Instituto de Matemática e Estatística da Universidade de São Paulo, 1972.

MILIES, C. P. Breve História da Álgebra Abstrata. In: BIENAL DA SOCIEDADE BRASILEIRA DE MATEMÁTICA, 2., 2004, Salvador. **Anais eletrônicos...** Disponível em: <http://www.bienasbm.ufba.br/M18.pdf>. Acesso em: 17 de out. 2018.

MUSILI, C. **Introduction to Rings and Modules**. 2. ed. Nova Deli: Narosa Publishing House, 2001.

ROMAN, S. **Advanced Linear Algebra**. 3. ed. Nova York: Springer, 2007.

WAGSTAFF, S. S. **Rings, Modules, and Linear Algebra**, 1 de out. de 2011. 167 f. Notas de Aula.