UNIVERSIDADE FEDERAL DO PARÁ

INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS

CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

Sara Raissa Silva Rodrigues

UMA INTRODUÇÃO À TEORIA DE MÓDULOS

BELÉM

2013

UNIVERSIDADE FEDERAL DO PARÁ

INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS

CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

Sara Raissa Silva Rodrigues

UMA INTRODUÇÃO À TEORIA DE MÓDULOS

Trabalho de Conclusão de Curso apresentado para obtenção do grau de Licenciado Pleno em Matemática da Universidade Federal do Pará.

Orientadora: Prof[a]. Dr[a]. Maria de Nazaré Carvalho Bezerra.

BELÉM

2013

CERTIFICADO DE AVALIAÇÃO

Sara Raissa Silva Rodrigues

UMA INTRODUÇÃO À TEORIA DE MÓDULOS

Trabalho de Conclusão de curso apresentado como requisito para obtenção do título de Licenciatura Plena em Matemática, da Universidade Federal do Pará pela seguinte banca examinadora:

Orientadora: Profª. Drª. Maria de Nazaré Carvalho Bezerra.

Faculdade de Matemática, UFPA

Profª. Msc. Joelma Morbach.

Faculdade de Matemática, UFPA

Prof. Dr. Juaci Picanço da Silva.

Faculdade de Matemática, UFPA

Profª. Drª. Rúbia Gonçalves Nascimento.

Faculdade de Matemática, UFPA

DATA DA AVALIAÇÃO: ____ /____ /____

CONCEITO: _____

Dedico este trabalho aos meus pais Ana Maria e Adinilson Fialho (in memoriam).

AGRADECIMENTOS

A Deus, pois sem ele não estaria aqui. Ele que sempre está presente em minha vida, dando-me sabedoria, força e guiando-me em cada passo dado.

À minha mãe Ana Maria, por ser o meu esteio, por estar ao meu lado incondicionalmente, apoiando-me, dando-me forças em qualquer circunstância da vida, ao meu pai Adinilson Fialho, que mesmo ausente, sempre me orientou a nunca desistir dos meus sonhos, ao meu irmão, cunhada, tios, tias, primos, enfim, a todos os meus familiares que me ajudaram e por sempre estarem presente nos momentos felizes e tristes.

À minha orientadora querida e amada Nazaré Bezerra, por ter aceitado me orientar. Por sua grande influência na escolha do tema deste trabalho, por sua excelente e eficiente orientação, por ajudar-me em todos os momentos que precisei durante este curso, dando-me conselhos valiosos, por me escutar, pelas brincadeiras, enfim, obrigada pela sua amizade e por tudo. Faltam-me palavras para dizer o quanto ela é importante e especial na minha vida.

Às minhas queridas e amadas professoras Joelma Morbach e Rúbia Nascimento por terem aceitado fazer parte da banca examinadora e que junto com a professora Nazaré foram como "mães" durante este curso, pois me apoiaram em todos os momentos que precisei, pelos conselhos valiosos, por me escutar, pela cumplicidade, brincadeiras, confiança, amizade, enfim, não consigo expressar toda a gratidão que sinto por elas e o quanto elas são importantes e especiais na minha vida, obrigada por tudo. Estarão todas sempre no meu coração.

Aos amigos irmãos que conquistei durante esses anos de graduação: Ana Lídia, Érico, Francimaria, Renan e Thays, que me ajudaram em todos os momentos que precisei. Posso dizer que tive os melhores amigos. Obrigada pela cumplicidade, amizade, companheirismo e por me aguentarem todos estes anos, enfim, vocês são muito especiais e estarão no meu coração.

À minha professora querida e amada Adma Muriel, pela sua amizade, por ter me influenciado a amar esta ciência, por sempre torcer por mim e por todos os seus ensinamentos, sou muito grata, ela certamente tem um lugar no meu coração.

Ao professor Juaci Picanço, por ter aceitado fazer parte da banca examinadora junto com as professoras Joelma Morbach e Rúbia Nascimento.

À professora Cristina Vaz, por acreditar em mim, pela amizade, compreensão e entendimento em um dos momentos mais difíceis da minha vida.

De um modo geral quero agradecer a todos os meus professores da UFPA que de alguma forma contribuíram para o meu aprendizado, dentre os quais destaco os professores: Augusto César, Erisson Ulisses, Hermínio Gomes, Irene Castro, João Pablo, Manoel Silvino, Marcos Diniz, Maria José e Tânia Valdivia.

Às minhas amigas, Layane, Mayara e Priscyla, por suas amizades, cumplicidade, apoio, por me escutarem nos momentos que precisei conversar e que me acompanham desde o início desta graduação.

À Karen Nobre pelo seu apoio em um dos momentos mais difíceis da minha vida e pela amizade, a Arlena Reis pela amizade e por acreditar em mim, a Nelma Renata e a Elza Líbia por terem sempre me ajudado.

Enfim, obrigada a todos que de certa forma contribuíram para a minha formação acadêmica.

"A Matemática quando bem compreendida nos trás não somente a verdade, mas também um intenso brilho."

Autor desconhecido

RESUMO

Este trabalho faz um estudo introdutório à teoria de módulos, estrutura definida de modo análogo a espaço vetorial, sendo o corpo substituído por um anel. O trabalho apresenta uma grande variedade de exemplos de módulos, mostrando assim a vasta aplicação desta estrutura. Faz-se um aprofundamento no estudo de homomorfismo de módulos com a utilização de diagramas. Por fim define-se módulos livres, comparando propriedades das duas estruturas: espaço vetorial e módulo.

Palavras-chave: Módulos, Módulos Livres.

Sumário

Introdução

Em Álgebra Linear, uma das estruturas centrais é o espaço vetorial, na qual estão definidas duas operações: a adição de vetores e a multiplicação de vetores por escalares, que são elementos de um corpo. Uma pergunta interessante seria: e quando os escalares não pertencem a um corpo e sim a um anel qualquer, que estrutura teria? Será que a mesma existe? A resposta para essas perguntas é afirmativa e tal estrutura chama-se módulos e será o objeto do nosso estudo. Assim, esta substituição de corpo por anel, que exigimos para ser módulo enfraquece tal estrutura, pois perdemos várias propriedades, mas também ganhamos uma riqueza de exemplos que muitos deles serão mencionados ao longo deste estudo.

Neste trabalho faremos um estudo introdutório sobre módulos, estrutura definida de modo análogo a espaço vetorial, na qual em vez de um corpo, temos um anel como o conjunto de escalares. A teoria de módulos tem muitas aplicações, como no estudo de grupos abelianos, na topologia algébrica, teoria de representação de grupos e anéis, álgebra homológica e também na álgebra linear, onde podemos obter resultados clássicos da mesma usando esta teoria.

Muito da teoria de módulos consiste em estender ao máximo possível às propriedades dos espaços vetoriais, mas também temos resultados dos mesmos que em módulos não valem, por exemplo, em geral, não é verdade que todo subconjunto linearmente independente de um módulo livre possa ser ampliado a uma base. Sendo assim, faremos as devidas comparações quando forem necessárias.

Este trabalho reúne alguns conceitos e resultados de módulos, distribuídos ao longo de cinco capítulos, no primeiro deles falaremos de grupos, anéis, homomorfismos dos mesmos e espaço vetorial, destacando alguns exemplos que serão usados mais tarde e principais propriedades, como por exemplo, o teorema do homomorfismo para grupos e anéis que será importantíssimo para o capítulo posterior.

Já no segundo capítulo, definiremos módulos, submódulos, módulos quocientes, mostrando alguns exemplos e principais resultados. No terceiro capítulo trataremos de homomorfismos de módulos, sequências exatas e diagramas comutativos, mostrando alguns exemplos e propriedades, onde destacamos o teorema do homomorfismo para módulos, que será bastante usado nos demais capítulos e também o primeiro e o segundo teorema do isomorfismo.

No quarto capítulo, definiremos produto direto, somas direta externa e interna de módulos e projeção, destacando a propriedade universal para produto direto e soma direta externa e que relação existe entre essas somas.

E por fim, no último capítulo, faremos um estudo de módulos livres, que são aqueles que possuem uma base e fazemos um estudo comparativo das propriedades de espaços vetoriais e de módulos.

Capítulo 1

Preliminares

Neste capítulo veremos alguns resultados importantes de grupos, anéis e espaço vetorial, tais como definições, exemplos e as principais propriedades dos mesmos, os quais são bases para os capítulos posteriores.

1.1 Grupos

Definição 1.1. *Seja G um conjunto não vazio e $*$ uma operação interna em G, dizemos que o par $(G, *)$ é um grupo se verifica as seguintes propriedades:*
(i) *A operação $*$ é associativa, ou seja, quaisquer que sejam $a, b, c \in G$, temos*

$$(a * b) * c = a * (b * c)$$

(ii) *Existe um elemento $e \in G$, chamado elemento neutro de G, tal que para todo $a \in G$, temos*

$$a * e = e * a = a$$

(iii) *Para todo $a \in G$, existe um elemento $a' \in G$, chamado o elemento simétrico de a, tal que*

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

Se, além disso, para todo $a, b \in G$ tivermos a seguinte propriedade

$$a * b = b * a$$

Então, $(G, *)$ recebe o nome de *grupo comutativo* ou *abeliano*.

Proposição 1.1. *Seja $(G, *)$ um grupo, então temos:*

(i) *o elemento neutro de G é único;*

(ii) *o elemento simétrico de G é único;*

(iii) *para todo $a \in G, (a')' = a$;*

(iv) *para todos $(a * b)' = b' * a'$;*

(v) *para quaisquer $a, b, c \in G$ temos:*

$$\textit{Se } a * b = a * c \ (\textit{ou } b * a = c * a), \ \textit{então } b = c.$$

Exemplo 1.1. O par $(\mathbb{Z}, +)$ é um grupo abeliano, chamado o grupo aditivo dos inteiros.

Exemplo 1.2. O par $(\mathbb{R}^*, \cdot)$ é um grupo abeliano, chamado o grupo multiplicativo dos reais.

Exemplo 1.3. O par $(\mathbb{M}_{m\times n}(\mathbb{R}), +)$, onde que $\mathbb{M}_{m\times n}(\mathbb{R})$ é o conjunto das matrizes $m \times n$ com elementos reais, é um grupo abeliano.

Observação 1.1. Para simplificar a notação indicaremos o grupo $(G, *)$ apenas pelo conjunto G.

1.1.1 Subgrupos

Definição 1.2. *Um subconjunto não vazio H de um grupo G é chamado um subgrupo de G, se H é um grupo, com a mesma operação que define G como grupo.*

Proposição 1.2. *Um subconjunto H de um grupo G é um subgrupo de G, se e somente se, verifica-se as seguintes condições:*

(i) *H é não vazio;*

(ii) *para todos $h_1, h_2 \in H$, tem-se $h_1 * h_2 \in H$;*

(iii) *para todo $h \in H$, temos que $h' \in H$.*

Exemplo 1.4. Se G é um grupo, então $\{e\}$ e G são subgrupos, chamados os subgrupos triviais de G.

Exemplo 1.5. Para todo inteiro n, o conjunto $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ é um subgrupo de $(\mathbb{Z}, +)$. E mostra-se que todo subgrupo de $(\mathbb{Z}, +)$ é da forma $n\mathbb{Z}$, para algum inteiro positivo n.

1.1.2 Potência no grupo

Seja $(G, *)$ um grupo com elemento neutro e. Definimos as potências de expoente inteiro de um elemento a de G da seguinte forma:

$$\begin{cases} a^0 &= e \\ a^n &= a^{n-1} \cdot a, \quad n = 1, 2, \ldots \\ a^{-n} &= (a^{-1})^n, \quad n = 1, 2, \ldots \end{cases}$$

Proposição 1.3. *Sejam $(G, *)$ um grupo e a um elemento de G. Então $(a^m)^n = a^{mn}$, para quaisquer inteiros m e n.*

1.1.3 Classes laterais

Sejam G um grupo e H um subgrupo de G, definamos em G a seguinte relação

$$x \sim y \Leftrightarrow x' * y \in H \tag{1.1}$$

a qual é uma relação de equivalência.

Dado $x \in G$, então a classe de equivalência determinada por x é o conjunto

$$xH = \{xh \mid h \in H\}$$

que chamaremos de *classe lateral à esquerda, módulo H, determinada por x*.

O conjunto de todas as classes laterais à esquerda, módulo H é chamado *conjunto quociente* denotado por G/H, isto é,

$$G/H = \{xH \mid x \in G\}.$$

O conjunto das classes laterais à esquerda, módulo H, determina uma partição em G, ou seja,

(a) Se $x \in G$, então $xH \neq \emptyset$;

(b) Se $x, y \in G$, então $xH = yH$ ou $xH \cap yH = \emptyset$;

(c) A união de todas as classes laterais à esquerda é igual a G, isto é,

$$\bigcup_{x \in G} xH = G.$$

Definindo uma relação análoga a (1.1), define-se classe lateral à direita, módulo H. Todas as propriedades válidas para as classes laterais à esquerda, valem também para as classes laterais à direita.

No caso do grupo aditivo $(G, +)$ denotaremos a classe xH por $x + H = \{x + h \mid h \in H\}$.

1.1.4 Grupo Quociente

Proposição 1.4. *Seja H um subgrupo de um grupo G. As seguintes condições são equivalentes:*
(i) Para todo $g \in G$, temos $g'Hg \subset H$;
(ii) Para todo $g \in G$, temos $g'Hg = H$;
(iii) Para todo $g \in G$, temos $gH = Hg$.

Definição 1.3. *Um subgrupo H de um grupo G é chamado um subgrupo normal de G se ele satisfaz a uma (e portanto todas) das condições da Proposição 1.4.*

Escreveremos $H \lhd G$, para dizer que H é um subgrupo normal de G.

Exemplo 1.6. Para qualquer grupo G, os subgrupos triviais $\{e\}$ e G são normais.

Exemplo 1.7. Se G é abeliano, então todo subgrupo de G é normal.

Proposição 1.5. *Sejam G um grupo e H um subgrupo normal de G. Então o conjunto quociente $G/H = \{xH \mid x \in G\}$ com a operação definida por*

$$xH * yH = (xy)H$$

é um grupo.

Definição 1.4. *O grupo $(G/H, *)$ obtido na Proposição 1.5 é chamado o grupo quociente de G por H, denotado por G/H ou $\frac{G}{H}$.*

1.1.5 Homomorfismo de Grupos

Definição 1.5. *Sejam $(G, *)$ e $(J, \cdot)$ dois grupos. Uma função $f : G \longrightarrow J$ é um homomorfismo de grupos se para quaisquer $x, y \in G$ temos*

$$f(x * y) = f(x) \cdot f(y).$$

Os homomorfismos podem apresentar outras propriedades, por serem funções, daí recebem nomes especiais, tais como:

Definição 1.6. *Um homomorfismo $f : G \longrightarrow J$ é dito um:*
(i) *monomorfismo se f é uma função injetora;*
(ii) *epimorfismo se f é uma função sobrejetora;*
(iii) *isomorfismo se f é uma função bijetora.*

Definição 1.7. *Dois grupos G e J são ditos isomorfos se existe um isomorfismo entre eles. Neste caso escrevemos $G \simeq J$.*

Os homomorfismos $f : G \longrightarrow G$ são chamados de *endomorfismos*. Se $f : G \longrightarrow G$ é um isomorfismo, então f é chamado de *automorfismo*.

1.1.6 Núcleo e Imagem de um homomorfismo

Definição 1.8. *Sejam $(G, *)$ e $(J, \cdot)$ dois grupos com elementos neutros e_1 e e_2 respectivamente e $f : G \longrightarrow J$ um homomorfismo de grupos. Então:*
(i) *O conjunto $\{x \in G \mid f(x) = e_2\}$ é chamado o núcleo de f e denotaremos por $ker(f)$;*
(ii) *O conjunto $\{f(x) \mid x \in G\}$ é chamado a imagem de f e denotaremos por $Im(f)$.*

Exemplo 1.8. Sejam $(G, *)$ e $(J, \cdot)$ dois grupos. A aplicação $f : G \longrightarrow J$ definida por $f(x) = e_2$, para todo $x \in G$ é um homomorfismo de grupos, chamado homomorfismo trivial.

Exemplo 1.9. Seja G um grupo arbitrário. A função $Id_G : G \longrightarrow G$ definida por $Id_G(x) = x$, para todo $x \in G$ é um automorfismo de grupos.

1.1.7 Propriedades do Homomorfismo de Grupos

Proposição 1.6. *Sejam $(G, *)$ e $(J, \cdot)$ dois grupos com e_1 o elemento neutro de G, e_2 o elemento neutro de J e $f : G \longrightarrow J$ um homomorfismo de grupos. Então temos:*
(i) $f(e_1) = e_2$;
(ii) *Para todo $x \in G$, tem-se $f(x') = [f(x)]'$;*
(iii) *O núcleo de f é um subgrupo de G e a $Im(f)$ é um subgrupo de J;*
(iv) *f é monomorfismo $\Leftrightarrow ker(f) = \{e_1\}$.*

Teorema 1.1. *(Teorema do Homomorfismo para Grupos): Sejam G e J grupos. Se $f : G \longrightarrow J$ é um homomorfismo de grupos, então*

$$G/ker(f) \simeq Im(f).$$

Em particular, se f é epimorfismo, então

$$G/ker(f) \simeq J.$$

1.2 Anéis

Definição 1.9. *O terno $(A, +, \cdot)$ onde A é um conjunto não vazio munido de duas operações internas, chamadas Adição $(+)$ e Multiplicação $(\cdot)$ é chamado anel se satisfaz as seguintes propriedades:*

(P_1) a adição é associativa, ou seja, para todos $a, b, c \in A$

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

(P_2) existe um elemento $0 \in A$, chamado elemento neutro da adição, tal que para todo $a \in A$, temos

$$a + 0 = 0 + a = a$$

(P_3) para todo $a \in G$, existe um elemento $(-a) \in G$, chamado o inverso aditivo de a, tal que

$$a + (-a) = (-a) + a = 0$$

(P_4) a adição é comutativa, ou seja, para todos $a, b \in A$, temos

$$a + b = b + a$$

(P_5) a multiplicação é associativa, ou seja, para todos $a, b, c \in A$, temos

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

(P_6) a multiplicação é distributiva, à esquerda e a direita, com relação a adição, ou seja, para todos $a, b, c \in A$, temos

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

Observação 1.2. Se $(A, +, \cdot)$ é um anel, então o par $(A, +)$ é um grupo abeliano, assim todas as propriedades vistas para grupos valem também para anéis.

Dizemos que um anel $(A, +, \cdot)$ é:
(i) *comutativo*, se a multiplicação é comutativa, ou seja, para todos $a, b \in A$, temos

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

(ii) *com elemento unidade*, se existe $1 \in A$, com $1 \neq 0$, tal que para todo a, tem-se

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

(iii) *sem divisores de zero*, se o produto de quaisquer dois elementos não nulos de A é um elemento não nulo, ou seja, para todos $a, b \in A$, temos

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

Definição 1.10. *Um anel comutativo, com elemento unidade e sem divisores de zero é chamado um domínio de integridade.*

Definição 1.11. *O anel $(A, +, \cdot)$ é chamado um anel de divisão se é um anel com elemento unidade e para todo $0 \neq a \in A$ existe um $b \in A$, tal que*

$$a \cdot b = b \cdot a = 1$$

Definição 1.12. *O anel $(A, +, \cdot)$ é chamado um corpo se é um anel de divisão comutativo.*

Observação 1.3. Para simplificar a notação indicaremos o anel $(A, +, \cdot)$ apenas pelo conjunto A.

Exemplo 1.10. Os anéis númericos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são anéis de integridade.

Exemplo 1.11. Seja $(G, +)$ um grupo abeliano. Indicaremos por $End(G)$ o conjunto de todos os endomorfismos de G. Neste conjunto podemos introduzir uma estrutura de anel definindo soma e produto de dois endomorfismos $f, g \in End(G)$ por:

- $(f + g)(x) = f(x) + g(x) \quad \forall\, x \in G$
- $(fg)(x) = f(g(x)) \quad \forall\, x \in G$

Vamos mostrar que $End(G)$ é um anel com unidade. Sejam $f, g, h \in End(G)$.

(i) $(f+g)+h = f+(g+h)$.

De fato, $\forall\, x \in G$

$$\begin{aligned}
[(f+g)+h](x) &= (f+g)(x)+h(x) && \text{- definição de soma}\\
&= (f(x)+g(x))+h(x) && \text{- definição de soma}\\
&= f(x)+(g(x)+h(x)) && \text{- associatividade de } G\\
&= f(x)+(g+h)(x) && \text{- definição de soma}\\
&= [f+(g+h)](x) && \text{- definição de soma}
\end{aligned}$$

(ii) $f+g = g+f$.

De fato, $\forall\, x \in G$

$$\begin{aligned}
(f+g)(x) &= f(x)+g(x) && \text{- definição de soma}\\
&= g(x)+f(x) && \text{- comutatividade em } G\\
&= (g+f)(x) && \text{- definição de soma}
\end{aligned}$$

(iii) A função nula $O : G \longrightarrow G$ definida por $O(x) = 0,\ \forall\, x \in G$ é tal que

$$f+O = O+f = f \quad \forall\, f \in End(G)$$

De fato, $\forall\, x \in G$

$$\begin{aligned}
(f+O)(x) &= f(x)+O(x) && \text{- definição de soma}\\
&= f(x)+0 && \text{- definição da } O(x)=0\\
&= f(x) && \text{- elemento neutro de } G
\end{aligned}$$

Como vale a comutatividade, temos $f+O = O+f = f$.

(iv) Dada $f \in End(G)$, a função $g : G \longrightarrow G$ definida por $g(x) = -f(x)$ é tal que

$$f+g = g+f = 0 \quad \forall\, f \in End(G)$$

De fato, $\forall\, x \in G$

$$\begin{aligned}
(f+g)(x) &= f(x)+g(x) && \text{- definição de soma}\\
&= f(x)+(-f(x)) && \text{- definição da } g(x)=-f(x)\\
&= 0 && \text{- elemento simétrico de } G
\end{aligned}$$

Como vale a comutatividade, temos $f + g = g + f = 0$.

Segue, portanto que $(End(G), +)$ é grupo abeliano. Além disso,

(v) $(fg)h = f(gh)$

De fato, $\forall\ x \in G$

$$\begin{aligned}
[(fg)h](x) &= (fg)(h(x)) && \text{- definição de multiplicação}\\
&= f(g(h(x))) && \text{- definição de multiplicação}\\
[f(gh)](x) &= f(gh(x)) && \text{- definição de multiplicação}\\
&= f(g(h(x))) && \text{- definição de multiplicação}
\end{aligned}$$

Daí, $(fg)h = f(gh)$.

(vi) $f(g + h) = fg + fh$ e $(g + h)f = gf + hf$.

De fato, $\forall\ x \in G$

$$\begin{aligned}
[f(g+h)](x) &= f[(g+h)(x)] && \text{- definição de multiplicação}\\
&= f(g(x) + h(x)) && \text{- definição de soma}\\
&= f(g(x)) + f(h(x)) && \text{- pois } g(x), h(x) \in G \text{ e } f \text{ é um homomorfismo}\\
&= (fg)(x) + (fh)(x) && \text{- definição de multiplicação}
\end{aligned}$$

e

$$\begin{aligned}
[(g+h)f)](x) &= (g+h)(f(x)) && \text{- definição de multiplicação}\\
&= g(f(x)) + h(f(x)) && \text{- definição de soma}\\
&= (gf)(x) + (hf)(x) && \text{- definição de multiplicação}
\end{aligned}$$

(vii) A função $I_d : G \longrightarrow G$ definida por $I_d(x) = x,\ \forall\ x \in G$ é tal que

$$f \cdot I_d = I_d \cdot f = f \quad \forall\ f \in End(G)$$

De fato, $\forall\ x \in G$

$$\begin{aligned}
[f \cdot I_d](x) &= f(I_d(x)) && \text{- definição de multiplicação}\\
&= f(x) && \text{- definição de } I_d(x) = x\\
[I_d \cdot f](x) &= I_d(f(x)) && \text{- definição de multiplicação}\\
&= f(x) && \text{- definição de } I_d(x) = x
\end{aligned}$$

Segue então que o $End(G)$ é um anel com unidade, chamado o anel do endomorfismo de G.

1.2.1 Subanéis

Definição 1.13. *Dizemos que um subconjunto não vazio B de um anel $(A, +, \cdot)$ é um subanel de A, se $(B, +, \cdot)$ é também um anel, com relação as mesmas operações que definem A como anel.*

Proposição 1.7. *Um subconjunto não vazio B de um anel A é subanel de A se, e somente se, as seguintes condições são satisfeitas:*
(i) $0 \in B$
(ii) *Para todos* $x, y \in B$, *temos* $x - y \in B$
(iii) *Para todos* $x, y \in B$, *temos* $x \cdot y \in B$

Exemplo 1.12. Dado um anel A o conjunto $Z(A) = \{x \in A \mid x \cdot y = y \cdot x, \ \forall \ y \in A\}$ é um subanel de A, onde $Z(A)$ é chamado o centro de A.

1.2.2 Ideais

Definição 1.14. *Sejam A um anel e I um subanel de A. Dizemos que I é um ideal à esquerda de A se para quaisquer $x \in I$ e $a \in A$, temos $ax \in I$.*

De modo análogo define-se ideal à direita.

Definição 1.15. *Um ideal I chama-se bilateral de A se I é simultaneamente um ideal à esquerda e à direita de A.*

Sejam A um anel comutativo e com elemento unidade, $x_1, x_2, \ldots, x_n$ elementos de A.

O conjunto

$$\{a_1x_1 + a_2x_2 + \cdots + a_nx_n \mid a_1, a_2, \cdots, a_n \in A\}$$

é um ideal de A contendo $x_1, x_2, \ldots, x_n$, chamado ideal *gerado* por $x_1, x_2, \ldots, x_n$ e denotado por $Ax_1 + Ax_2 + \cdots + Ax_n$. Quando $n = 1, Ax_1 = \{ax_1 \mid a \in A\}$ é chamado *ideal principal* gerado por x_1.

1.2.3 Anéis Quocientes

Dados um anel $(A, +, \cdot)$ e um ideal I de A, temos que $(I, +)$ é um subgrupo normal do grupo abeliano $(A, +)$, logo o conjunto quociente

$$A/I = \{a + I \mid a \in A\}$$

com a adição definida por

$$+ : A/I \times A/I \longrightarrow A/I$$

$$(x + I, y + I) \longrightarrow (x + y) + I$$

é um grupo abeliano.

Damos ao grupo quociente $(A/I, +)$ uma estrutura de anel definindo a multiplicação da seguinte forma

$$\cdot : A/I \times A/I \longrightarrow A/I$$

$$(x + I, y + I) \longrightarrow (x \cdot y) + I.$$

No que segue, denotaremos a classe $a + I \in A/I$ por $\overline{a}$.

1.2.4 Homomorfismo de Anéis

Definição 1.16. *Sejam A e B anéis. Uma função $f : A \longrightarrow B$ é um homomorfismo de anéis se para quaisquer $x, y \in G$ temos:*
(i) $f(x + y) = f(x) + f(y)$*;*
(ii) $f(x \cdot y) = f(x) \cdot f(y)$.

Como no caso de homomorfismo de grupo, $f : A \longrightarrow B$ é dito monomorfismo, epimorfismo ou isomorfismo ser for, respectivamente injetora, sobrejetora e bijetora.

Definição 1.17. *Dois anéis A e B são ditos isomorfos se existe um isomorfismo entre eles e escrevemos $A \simeq B$.*

Os homomorfismos $f : A \longrightarrow A$ são chamados de *endomorfismos*. Se $f : A \longrightarrow A$ é um isomorfismo, então f é chamado de *automorfismo*.

1.2.5 Núcleo e Imagem de um homomorfismo

Definição 1.18. *Sejam A e B anéis e $f : A \longrightarrow B$ um homomorfismo de anéis. Então:*
(i) *O conjunto $\{x \in A \mid f(x) = 0_B\}$ é chamado o núcleo de f e denotaremos por $ker(f)$;*
(ii) *O conjunto $\{f(x) \mid x \in A\}$ é chamado a imagem de f e denotaremos por $Im(f)$.*

Teorema 1.2. *(Teorema do Homomorfismo para Anéis): Sejam A e B anéis. Se $f : A \longrightarrow B$ é um homomorfismo de anéis, então*

$$A/ker(f) \simeq Im(f).$$

E se f é epimorfismo, então

$$A/ker(f) \simeq B.$$

1.3 Espaços Vetoriais

Nesta seção veremos a definição de espaço vetorial e algumas propriedades do mesmo, os quais serão bases para o último capítulo.

Definição 1.19. *Um conjunto não vazio V é um espaço vetorial sobre um corpo K se em seus elementos, denominados vetores, estiverem definidas as duas seguintes operações:*
(A) *Cada par $u, v \in V$, temos $u + v \in V$, chamado de soma de u e v, de modo que:*
(A_1) *para todos $u, v, w \in V$, $(u + v) + w = u + (v + w)$ (propriedade associativa).*
(A_2) *para todos $u, v \in V$, $u + v = v + u$ (propriedade comutativa).*
(A_3) *existe um vetor $0 \in V$, chamado vetor nulo, tal que $0 + v = v$, para todo $v \in V$.*
(A_4) *para todo $v \in V$, existe um vetor $-v \in V$, chamado oposto de v, tal que $v + (-v) = 0$.*
(M) *A cada par $\alpha \in K$ e $v \in V$, corresponde um vetor $\alpha v \in V$, chamado produto por escalar de α por v, de modo que:*
(M_1) *para todos $\alpha, \beta \in K$ e $v \in V$, $(\alpha\beta)v = \alpha(\beta v)$.*
(M_3) *para todos $\alpha \in K$ e $u, v \in V$, $\alpha(u + v) = \alpha u + \alpha v$.*
(M_4) *para todos $\alpha, \beta \in V$ e $v \in V$, $(\alpha + \beta)v = \alpha v + \beta v$.*
(M_2) *existe um vetor $1 \in K$, chamado elemento unidade de K, tal que $1v = v$, para todo $v \in V$.*

Definição 1.20. *Seja V um espaço vetorial sobre um corpo K. Um subconjunto não vazio W de V é um subespaço de V se W é também um espaço vetorial considerando as mesmas operações definidas em V.*

Definição 1.21. *Seja V um espaço vetorial sobre um corpo K. Diz-se que um vetor $u \in V$ é uma combinação linear dos vetores $v_1, v_2, \ldots, v_n \in V$ se existem escalares $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$, tais que*

$$u = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n.$$

Dado um subconjunto não vazio S de um espaço vetorial V, denotamos por $\langle S \rangle$ o conjunto de todas as combinações lineares finitas de elementos de S. Assim,

$$\langle S \rangle = \{\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_n u_n \mid n \in \mathbb{N}^*, \alpha_1, \alpha_2, \ldots, \alpha_n \in K, u_1, u_2, \ldots, u_n \in S\}.$$

Definição 1.22. *Seja S um subconjunto não vazio de um espaço vetorial sobre um corpo K. O conjunto $\langle S \rangle$ é chamado subespaço de V gerado por S.*

Definição 1.23. *Seja S um subconjunto de um espaço vetorial V. Se $\langle S \rangle = V$, diz-se que S é um conjunto gerador de V (ou que S gera V).*

Definição 1.24. *Diz-se que um espaço vetorial V sobre um corpo K é finitamente gerado se ele possui um conjunto gerador finito.*

Definição 1.25. *Seja V um espaço vetorial sobre um corpo K. Um subconjunto S de V é dito linearmente dependente (ou l.d.) se existem vetores distintos $u_1, u_2, \ldots, u_n \in S$ e escalares $\alpha_1, \alpha_2, \ldots, \alpha_n$ em K, estes nem todos nulos, tais que*

$$\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_n u_n = 0.$$

Um conjunto que não é linearmente dependente é dito linearmente independente (ou l.i).

Definição 1.26. *Seja V um espaço vetorial sobre um corpo K. Dizemos que um subconjunto $B \subset V$ é uma base de V se:*
(i) B é um gerador de V, isto é, $\langle B \rangle = V$;
(ii) B é um conjunto linearmente independente.

1.3.1 Propriedades de Espaço Vetorial

Proposição 1.8. *Sejam V um espaço vetorial. Um subconjunto $S = \{u_1, u_2, \ldots, u_n\}$ de vetores não nulos de V é linearmente dependente se, e somente se, um dos vetores de S é combinação linear dos precedentes.*

Proposição 1.9. *Seja V um espaço vetorial de dimensão finita n. Então todo gerador S de V contém uma base de V.*

Proposição 1.10. *Seja V um espaço vetorial finitamente gerado. Todo subconjunto não vazio de V linearmente independente é parte de uma base de V.*

Proposição 1.11. *Seja W um subespaço de um espaço vetorial V de dimensão finita. Então $dimW \leq dimV$ e se $dimW = dimV$, então $W = V$.*

Proposição 1.12. *Todo espaço vetorial finitamente gerado tem uma base.*

Capítulo 2

Módulo

Neste capítulo definiremos módulos que é uma importante generalização de espaço vetorial, no qual o corpo é substituído por um anel, também trabalharemos as definições de submódulos e módulos quocientes, apresentando vários exemplos dos mesmos.

Definição 2.1. *Seja A um anel não necessariamente comutativo. Um grupo abeliano $(M, +)$ dotado de uma multiplicação por escalar*

$$A \times M \longrightarrow M$$
$$(a, m) \longmapsto am$$

é dito um A-módulo à esquerda *se satisfaz os seguintes axiomas, para quaisquer $a_1, a_2 \in A$ e $m_1, m_2 \in M$:*
(i) $a_1(a_2m_1) = (a_1a_2)m_1$*;*
(ii) $a_1(m_1 + m_2) = a_1m_1 + a_1m_2$*;*
(iii) $(a_1 + a_2)m_1 = a_1m_1 + a_2m_1$.

Observação 2.1. De forma análoga definimos *A-módulo à direita*, considerando a multiplicação à direita por elementos do anel.

Se A é um anel com elemento unidade 1 e

$$1m = m, \ \ \forall\, m \in M$$

então M é dito um A-módulo unitário.

Em nosso estudo, tomaremos sempre módulos à esquerda sobre anéis com unidade. E quando não houver perigo de confusão, usaremos simplesmente a expressão A-*módulo*.

Exemplo 2.1. Seja $M = \{0\}$. Definamos as operações

(i) $0 + 0 = 0$

(ii) $a0 = 0,\ \forall\, a \in A$

M é chamado o A-módulo nulo denotado por 0.

Exemplo 2.2. Todo espaço vetorial sobre um corpo K é um K-módulo.

De fato, como um corpo é um anel com unidade, então a definição de espaço vetorial coincide com a de módulo.

Exemplo 2.3. Todo grupo abeliano $(G, +)$ pode ser considerado como um módulo sobre o anel $\mathbb{Z}$ dos números inteiros, definindo uma multiplicação por escalar da seguinte forma:

$$\cdot : \mathbb{Z} \times G \longrightarrow G$$

$$(n, a) \longrightarrow n \cdot a = a^n.$$

Com a^n definido como na Seção 1.1.2 do Capítulo 1.

De fato, para quaisquer $n_1, n_2 \in \mathbb{Z}$ e $a_1, a_2 \in G$, tem-se

(i) $n_1(n_2a_1) = (n_1n_2)a_1$.

$$\begin{aligned}
n_1(n_2a_1) &= n_1(a^{n_2}) && \text{- definição de multiplicação por escalar de } G \\
&= (a^{n_2})^{n_1} && \text{- definição de multiplicação por escalar de } G \\
&= a^{n_2n_1} && \text{- propriedade de potência} \\
&= a^{n_1n_2} && \text{- pois } \mathbb{Z} \text{ é comutativo} \\
&= (n_1n_2)a && \text{- definição de multiplicação por escalar de } G
\end{aligned}$$

(ii) $n_1(a_1 + a_2) = n_1a_1 + n_1a_2$.

$$\begin{aligned}
n_1(a_1 + a_2) &= (a_1 + a_2)^{n_1} && \text{- definição de multiplicação por escalar de } G \\
&= a_1^{n_1} + a_2^{n_1} && \text{- associando e comutando os elementos de } G \\
&= n_1a_1 + n_1a_2 && \text{- definição de multiplicação por escalar de } G
\end{aligned}$$

(iii) $(n_1 + n_2)a_1 = n_1a_1 + n_2a_1$.

$$\begin{aligned}(n_1+n_2)a_1 &= a_1^{(n_1+n_2)} && \text{- definição de multiplicação por escalar de } G\\ &= a_1^{n_1} + a_1^{n_2} && \text{- agrupando os termos } G\\ &= n_1a_1 + n_2a_1 && \text{- definição de multiplicação por escalar de } G\end{aligned}$$

(iv) $1_{\mathbb{Z}}a_1 = a_1$.

$$\begin{aligned}1_{\mathbb{Z}}a_1 &= a_1^1 && \text{- definição de multiplicação por escalar de } G\\ &= a_1\end{aligned}$$

Segue de $(i), (ii), (iii)$ e (iv) que G é um $\mathbb{Z}$-módulo unitário.

Exemplo 2.4. Seja I um ideal à esquerda de um anel A. Então I admite uma estrutura de A-módulo com a soma induzida pela soma de A e a multiplicação por escalar definida pela multiplicação de A.

$(I, +)$ é um grupo abeliano, por I ser um subanel de A. Além disso, para quaisquer $a_1, a_2 \in A$ e $x, y \in I$, como $I \subset A$ segue que $x, y \in A$ e sabendo que A é anel tem-se

(i) $a_1(a_2x) = (a_1a_2)x$ - associatividade da multiplicação em A

(ii) $a_1(x + y) = a_1x + a_1y$ - distributividade em A

(iii) $(a_1 + a_2)x = a_1x + a_2x$ - distributividade em A

(iv) $1_Ax = x$ - unidade de A

Portanto, segue de $(i), (ii), (iii)$ e (iv) que I é um A-módulo.

Em particular do Exemplo 2.4 todo anel pode ser considerado como um módulo sobre si mesmo. Escrevemos ${}_AA$ quando estivermos considerando A como módulo sobre si mesmo e apenas A, como anel.

Exemplo 2.5. Damos a um grupo abeliano $(G, +)$ uma estrutura de $End(G)$-módulo, associando a cada par $(f, x) \in End(G) \times G \longrightarrow G$ o elemento $fx = f(x) \in G$.

Já mostramos que $(End(G), +)$ é um grupo abeliano e para quaisquer $f, g \in End(G)$ e $x, y \in G$, temos

(a) $f(gx) = (fg)x$.

$$\begin{aligned} f(gx) &= f(g(x)) && \text{- definição de multiplicação por escalar} \\ &= (fg)(x) && \text{- definição de multiplicação em } (End(G)) \\ &= (fg)x && \text{- definição de multiplicação por escalar} \end{aligned}$$

(b) $f(x+y) = fx + fy$.

$$\begin{aligned} f(x+y) &= f(x) + f(y) && \text{- pois } f \text{ é um homomorfismo} \\ &= fx + fy && \text{- definição de multiplicação por escalar} \end{aligned}$$

(c) $(f+g)x = fx + gx$.

$$\begin{aligned} (f+g)x &= (f+g)(x) && \text{- definição de multiplicação por escalar} \\ &= f(x) + g(x) && \text{- definição de soma em } (End(G)) \\ &= fx + gx && \text{- definição de multiplicação por escalar} \end{aligned}$$

(d) $I_d x = x$.

De fato, $\forall\, x \in G$

$$\begin{aligned} I_d x &= I_d(x) && \text{- definição de multiplicação por escalar} \\ &= x && \text{- definição de } I_d(x) = x \end{aligned}$$

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

Exemplo 2.6. Seja A um anel e X um conjunto qualquer. Indicaremos por A^X o conjunto de todas as funções de domínio X a valores em A. A^X admite uma estrutura de A-módulo, definindo a soma de funções, como no exemplo anterior e a multiplicação à esquerda por elementos de A que associa a cada par $(a, f) \in A \times A^X$ a função $a \cdot f \in A^X$ definida por:

$$(af)(x) = af(x), \quad \forall\, x \in X.$$

De fato, $(A^X, +)$ é um grupo abeliano, conforme já mostrado no Exemplo 2.5. Vamos mostrar as propriedades da multiplicação por escalar. Sejam $a_1, a_2 \in A$ e $f, g \in A^X$.

(i) $a_1(a_2 f) = (a_1 a_2) f$.

De fato, $\forall\, x \in X$

$$\begin{aligned}
[a_1(a_2 f)](x) &= a_1(a_2 f)(x) && \text{- definição de multiplicação por escalar}\\
&= a_1(a_2 f(x)) && \text{- definição de multiplicação por escalar}\\
&= (a_1 a_2) f(x) && \text{- associatividade em } A, \text{ pois } f(x) \in A\\
&= [(a_1 a_2) f](x) && \text{- definição de multiplicação por escalar}
\end{aligned}$$

(ii) $a_1(f + g) = a_1 f + a_1 g$.

De fato, $\forall\, x \in X$

$$\begin{aligned}
[a_1(f+g)](x) &= a_1(f+g)(x) && \text{- definição de multiplicação por escalar}\\
&= a_1[f(x) + g(x)] && \text{- definição de soma}\\
&= a_1 f(x) + a_1 g(x) && \text{- distributividade em } A, \text{ pois } f(x), g(x) \in A\\
&= (a_1 f)(x) + (a_1 g)(x) && \text{- definição de multiplicação por escalar}\\
&= (a_1 f + a_1 g)(x) && \text{- definição de soma}
\end{aligned}$$

(iii) $(a_1 + a_2) f = a_1 f + a_2 f$.

De fato, $\forall\, x \in X$

$$\begin{aligned}
[(a_1 + a_2) f](x) &= (a_1 + a_2) f(x) && \text{- definição de multiplicação por escalar}\\
&= a_1 f(x) + a_2 f(x) && \text{- distributividade em } A, \text{ pois } a_1, a_2, f(x) \in A\\
&= (a_1 f) x + (a_2 f) x && \text{- definição de multiplicação por escalar}\\
&= (a_1 f + a_2 f)(x) && \text{- definição de soma}
\end{aligned}$$

(iv) $1_A f = f$.

De fato, $\forall\, x \in X$

$$\begin{aligned}
(1_A f)(x) &= 1_A f(x) && \text{- definição de multiplicação por escalar}\\
&= f(x) && \text{- elemento unidade, pois } f(x) \in A
\end{aligned}$$

Segue de $(i), (ii), (iii)$ e (iv) que A^X é um A-módulo unitário.

Exemplo 2.7. Seja M um A-módulo, I um ideal bilateral de A e A/I o anel quociente.

Definamos uma multiplicação à esquerda de A/I, como segue

$$\cdot : A/I \times M \longrightarrow M$$

$$(\overline{a}, m) \longrightarrow \overline{a}m = am.$$

Para que esta operação esteja bem definida é necessário que para quaisquer $a, b \in A$ e qualquer $m \in M$, se $\overline{a} = \overline{b}$, então

$$\overline{a}m = \overline{b}m \Rightarrow am = bm \Rightarrow (a-b)m = 0.$$

Em particular, tomando $b = 0$, temos que $am = 0, \forall\, a \in A, \forall\, m \in M$. Assim o conjunto

$$IM := \{\alpha m \mid \alpha \in I, m \in M\} = \{0\}.$$

Claramente vê-se que esta condição é também suficiente para que a operação não dependa do representante escolhido para a classe.

Além disso, para todo $\overline{a_1}, \overline{a_2} \in A/I$ e $m_1, m_2 \in M$ temos

(i) $\overline{a_1}(\overline{a_2}m_1) = (\overline{a_1 a_2})m_1$.

De fato,

$$\begin{aligned}
\overline{a_1}(\overline{a_2}m_1) &= \overline{a_1}(a_2 m_1) && \text{- definição de multiplicação por escalar}\\
&= a_1(a_2 m_1) && \text{- definição de multiplicação por escalar}\\
&= (a_1 a_2)m_1 && \text{- pois } M \text{ é um } A\text{-módulo}\\
&= (\overline{a_1 a_2})m_1 && \text{- definição de multiplicação por escalar}
\end{aligned}$$

(ii) $\overline{a_1}(m_1 + m_2) = \overline{a_1}m_1 + \overline{a_1}m_2$.

De fato,

$$\begin{aligned}
\overline{a_1}(m_1 + m_2) &= a_1(m_1 + m_2) && \text{- definição de multiplicação por escalar}\\
&= a_1 m_1 + a_1 m_2 && \text{- pois } M \text{ é um } A\text{-módulo}\\
&= \overline{a_1}m_1 + \overline{a_1}m_2 && \text{- definição de multiplicação por escalar}
\end{aligned}$$

(iii) $(\overline{a_1} + \overline{a_2})m_1 = \overline{a_1}m_1 + \overline{a_2}m_1$.

De fato,

$$\begin{aligned}
(\overline{a_1} + \overline{a_2})m_1 &= (\overline{a_1 + a_2})m_1 && \text{- definição de soma de classes} \\
&= (a_1 + a_2)m_1 && \text{- definição de multiplicação por escalar} \\
&= a_1m_1 + a_2m_1 && \text{- pois } M \text{ é um } A\text{-módulo} \\
&= \overline{a_1}m_1 + \overline{a_2}m_1 && \text{- definição de multiplicação por escalar}
\end{aligned}$$

(iv) $\overline{1_A}m_1 = m_1$.

De fato,

$$\begin{aligned}
\overline{1_A}m_1 &= 1_Am_1 && \text{- definição de multiplicação por escalar} \\
&= m_1 && \text{- pois } M \text{ é um } A\text{-módulo}
\end{aligned}$$

Portanto, segue de $(i), (ii), (iii)$ e (iv) que M é um A/I-módulo unitário.

Exemplo 2.8. Dado um grupo abeliano G e um inteiro m, o grupo G admite uma estrutura de $\mathbb{Z}_m$-módulo se, e somente se, para todo $g \in G$ tem-se que $mg = 0$.

De fato, se o grupo G admite uma estrutura $\mathbb{Z}_m$-módulo, então para todo $g \in G$ tem-se que $mg = 0$. Suponhamos que G admita uma estrutura $\mathbb{Z}_m$-módulo, sabemos que $\mathbb{Z}_m \simeq \mathbb{Z}/m\mathbb{Z}$, assim G tem uma estrutura de $\mathbb{Z}/m\mathbb{Z}$-módulo, usando o Exemplo 2.7, concluímos que $m\mathbb{Z}G = \{0\}$, onde

$$m\mathbb{Z}G = \{ng \mid n \in m\mathbb{Z} \text{ e } g \in G\}$$

e a multiplicação de elementos de $m\mathbb{Z}G$ é definida como no Exemplo 2.3.

Assim, $m \in m\mathbb{Z}$, pois $m = m1$, considere $g \in G$. Logo, $mg \in m\mathbb{Z}G$, daí segue que $mg = 0 \ \forall\, g \in G$, pois $m\mathbb{Z}G = \{0\}$.
Agora se $\forall\, g \in G$ tem-se que $mg = 0$, então G é um $\mathbb{Z}_m$-módulo.

De fato, se $mg = 0 \ \forall g \in G$, então pelo Exemplo 2.7, a operação

$$\mathbb{Z}/m\mathbb{Z} \times G \longrightarrow G$$

$$(\overline{a}, g) \longrightarrow ag$$

está bem definida. Sendo assim, verificaremos se G é um $\mathbb{Z}/m\mathbb{Z}$-módulo, para isto usaremos a definição de multiplicação do Exemplo 2.3. Com efeito, pelo Exemplo 2.7 segue que G é um $\mathbb{Z}$-módulo.

2.1 Submódulos

Definição 2.2. *Dizemos que um subconjunto não vazio N de um A-módulo M é um A-submódulo ou um submódulo de M, se as seguintes condições são satisfeitas:*
(i) $(N,+)$ *é um subgrupo aditivo de* $(M,+)$*;*
(ii) *Para todo* $a \in A$ *e todo* $n \in N$*, tem-se que* $an \in N$.

Proposição 2.1. *Um subconjunto não vazio N de um A-módulo M é um submódulo se, e somente se, as seguintes condições são satisfeitas:*
(i) *Para todos* $n_1, n_2 \in N$*, tem-se* $n_1 + n_2 \in N$*;*
(ii) *Para todos* $a \in A$ *e* $n \in N$*, tem-se* $an \in N$.

Demonstração:

$(\Rightarrow)$ Supondo N submódulo, as condições (i) e (ii) são verificadas, pois N é um A-módulo.

$(\Leftarrow)$ Se as condições (i) e (ii) são satisfeitas, então N é um submódulo.

A condição (ii) já mostra que N é fechado em relação a multiplicação por escalar. Resta mostrarmos que N é um subgrupo aditivo de M. De fato,
(i) $0 \in N$, pois $0 = 0n \in N$, pelo item (ii).
(ii) Para todos $n_1, n_2 \in N$ tem-se $n_1 + n_2 \in N$, pelo item (i).
(iii) Para todo $n \in N$, o simétrico $-n \in N$.
Com efeito, para todo $n \in N$, temos que

$$-n = (-1)n = -(1n) \in N \text{ por } (ii).$$

Portanto, segue que N é um submódulo de M. □

Exemplo 2.9. Seja V um espaço vetorial sobre um corpo K. Um subconjunto $S \subseteq V$ é um submódulo, se e somente se, S é um subespaço de V.

De fato, como todo corpo é um anel, a definição de subespaço coincide com a de submódulo. Reciprocamente, como V é um K-módulo e $S \subseteq V$ é um submódulo, onde os escalares pertencem ao corpo K, segue que a definição de submódulo coincide com a de subespaço.

Exemplo 2.10. Os $\mathbb{Z}$-submódulos de um grupo abeliano $(G,+)$ são precisamente os seus subgrupos.

De fato, se $H \subseteq G$ é um submódulo, então segue da definição que $(H, +)$ é subgrupo de $(G, +)$. E se H é um subgrupo de G, então para todos $n \in \mathbb{Z}$ e $h \in H$ tem-se $nh = h^n \in H$, pois H é subgrupo de G.

Exemplo 2.11. Seja A um anel. Os A-submódulos de ${}_A A$ são os ideais à esquerda.

Exemplo 2.12. Se N_1 e N_2 são submódulos de um A-módulo M, o conjunto

$$N_1 + N_2 := \{n_1 + n_2 \mid n_1 \in N_1 \text{ e } n_2 \in N_2\}$$

também é um submódulo de M, chamado submódulo soma de N_1 e N_2.

Vamos mostrar que o conjunto $N_1 + N_2$ é submódulo de M.
(i) $N_1 + N_2 \neq \emptyset$, pois $0 \in N_1$ e $0 \in N_2$, logo $0 = 0 + 0 \in N_1 + N_2$.
(ii) Se $n, n' \in N_1 + N_2$, então $n + n' \in N_1 + N_2$.

De fato, se $n, n' \in N_1 + N_2$, então $n = n_1 + n_2$ e $n' = n_1' + n_2'$, onde $n_1, n_1' \in N_1$ e $n_2, n_2' \in N_2$.

$$\begin{aligned} n + n' &= (n_1 + n_2) + (n_1' + n_2') && \text{- substituição de } n \text{ e } n' \\ &= (n_1 + n_1') + (n_2 + n_2') && \text{- associatividade e comutatividade de } M \\ &= n_3 + n_4 && \text{- onde } n_3 = n_1 + n_1' \in N_1 \text{ e } n_4 = n_1' + n_2' \in N_2 \end{aligned}$$

Portanto, $n + n' \in N_1 + N_2$.
(iii) Se $a \in A$ e $n \in N_1 + N_2$, então $an \in N_1 + N_2$.

De fato, se $n \in N_1 + N_2$, então $n = n_1 + n_2$, onde $n_1 \in N_1$ e $n_2 \in N_2$.

$$\begin{aligned} an &= a(n_1 + n_2) && \text{- substituição de } n \\ &= an_1 + an_2 && \text{- pois } M \text{ é um } A\text{-módulo} \\ &= n_3 + n_4 && \text{- pois } N_1, N_2 \text{ são submódulos, logo } n_3 = an_1 \in N_1 \text{ e } n_4 = an_2 \in N_2 \end{aligned}$$

Segue de $(i), (ii)$ e (iii) que $N_1 + N_2$ é um submódulo.

Exemplo 2.13. Seja M um A-módulo e $\{N_i\}_{i \in I}$ uma família de submódulos de M. Então $\bigcap_{i \in I} N_i$ é um submódulo de M.

De fato,

(i) $\bigcap_{i\in I} N_i \neq \emptyset$, pois como N_i é submódulo para todo $i \in I$, temos $0 \in N_i$, para cada $i \in I$, logo $0 \in \bigcap_{i\in I} N_i$.

(ii) Se $n, n' \in \bigcap_{i\in I} N_i$, então $n + n' \in \bigcap_{i\in I} N_i$.

De fato, se $n, n' \in \bigcap_{i\in I} N_i$, então $n, n' \in N_i$, para todo $i \in I$, logo $n + n' \in N_i$ para todo $i \in I$, pois N_i é submódulo. Assim, $n + n' \in \bigcap_{i\in I} N_i$.

(iii) Se $a \in A$ e $n \in \bigcap_{i\in I} N_i$, então $an \in \bigcap_{i\in I} N_i$.

Se $n \in \bigcap_{i\in I} N_i$, então $n \in N_i$ para todo $i \in I$, como N_i é submódulo, segue que $an \in N_i$, para todo $i \in I$, logo $an \in \bigcap_{i\in I} N_i$.

Segue de $(i), (ii)$ e (iii) que $\bigcap_{i\in I} N_i$ é um submódulo.

Exemplo 2.14. Seja S um subconjunto não vazio de um A- módulo M, o conjunto

$$(S) = \left\{ \sum_{i=1}^{n} a_i s_i \mid n \in \mathbb{N}, a_i \in A, s_i \in S \right\}$$

é um submódulo de M, chamado o submódulo gerado por S.

(i) $(S) \neq \emptyset$, pois $S \subseteq (S)$, isto é, $0 = 0s_1 \in (S)$.

(ii) Se $x, y \in (S)$, então $x + y \in (S)$.

De fato, se $x, y \in (S)$, então $x = \sum_{i=1}^{n} a_i s_i$ e $y = \sum_{j=1}^{m} a_j s_j$, com $a_i, a_j \in A$ e $s_i, s_j \in S$.

$$x + y = \sum_{i=1}^{n} a_i s_i + \sum_{j=1}^{m} a_j s_j \in (S).$$

Onde $x + y$ é uma soma finita de elementos de S multiplicado pelos elementos do anel.

(iii) Se $a \in A$ e $x \in (S)$, então $ax \in (S)$.

$$ax = a \sum_{i=1}^{n} a_i s_i = \sum_{i=1}^{n} a(a_i s_i) = \sum_{i=1}^{n} (aa_i) s_i = \sum_{i=1}^{n} b_i s_i \in (S).$$

onde $b_i = aa_i \in A$

Segue de $(i), (ii)$ e (iii) que (S) é um submódulo.

Em particular se $S = \{m\}$, então

$$(S) = \left\{ \sum_{i=1}^{n} a_i m \right\} \Rightarrow (S) = \{am \mid a \in A\}$$

Onde (S) é chamado de *submódulo cíclico* gerado por m, denotado por (m).

Exemplo 2.15. Se I é um ideal à esquerda de um anel A e m um elemento de um A-módulo M, então o conjunto

$$Im = \{\alpha m \mid \alpha \in I\}$$

é um submódulo de M.

De fato, vamos mostrar que

(i) $Im \neq \emptyset$, pois como I é ideal, temos $0 \in I$, logo $0 = 0m \in Im$.

(ii) Se $\alpha_1 m, \alpha_2 m \in Im$, então $\alpha_1 m + \alpha_2 m \in Im$.

Com efeito,

$$\begin{aligned} \alpha_1 m + \alpha_2 m &= (\alpha_1 + \alpha_2)m && \text{- pois } m \in A\text{-módulo e } \alpha_1, \alpha_2 \in I \subseteq A \\ &= \alpha m && \text{- pois } \alpha = \alpha_1 + \alpha_2 \in I, \text{ por } I \text{ ser ideal} \end{aligned}$$

Portanto, $\alpha_1 m + \alpha_2 m \in Im$

(iii) Se $a \in A$ e $\alpha m \in Im$, então $a(\alpha m) \in Im$.

De fato,

$$\begin{aligned} a(\alpha m) &= (a\alpha)m && \text{- pois } a, m \in A \text{ e } m \in A\text{-módulo } M \\ &= \alpha_1 m && \text{- } \alpha_1 = a\alpha \in I, \text{ por } I \text{ ser ideal} \end{aligned}$$

Segue de $(i), (ii)$ e (iii) que Im é um submódulo de M.

Definição 2.3. *Sejam A um anel e M um A-módulo, o conjunto*

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

é chamado anulador *do módulo M.*

De forma análoga defini-se anulador de um subconjunto de M.

Em particular, se $Anl(M) = \{0\}$, dizemos que M é um A-módulo fiel.

Proposição 2.2. *Seja A um anel e M um A-módulo. Então $Anl(M)$ é um ideal bilateral de A e M é um $A/Anl(M)$-módulo fiel.*

Demonstração:

Mostraremos que $Anl(M)$ é um ideal bilateral de A.

(i) $Anl(M) \neq \emptyset$, pois $0 = 0m,\ \forall\, m \in M$, logo $0 \in Anl(M)$.

(ii) Se $a_1, a_2 \in Anl(M)$, então $(a_1 - a_2) \in Anl(M)$.

Inicialmente observamos que se $a \in Anl(M)$, então $-a \in Anl(M)$. De fato,

$$(-a)m = -(am) = 0,\ \forall\, m \in M,\ \text{logo}\ -a \in Anl(M).$$

Assim, se $a_1, a_2 \in Anl(M)$, então $\forall\, m \in M$, temos

$$\begin{aligned} [a_1 + (-a_2)]m &= a_1m + (-a_2)m && \text{- pois } M \text{ é } A\text{-módulo} \\ &= 0 + 0 && \text{- pois } a_1, (-a_2) \in Anl(M) \\ &= 0 \end{aligned}$$

Logo, $a_1 + (-a_2) \in Anl(M)$.

(iii) Se $a \in A$ e $a_1 \in Anl(M)$, então $aa_1 \in Anl(M)$.

De fato, $\forall\, m \in M$

$$\begin{aligned} (aa_1)m &= a(a_1m) && \text{- pois } M \text{ é } A\text{-módulo} \\ &= a0 && \text{- pois } a_1 \in Anl(M), \text{ então } a_1m = 0 \\ &= 0 \end{aligned}$$

Logo, $(aa_1) \in Anl(M)$.

(iv) Se $a \in A$, $a_1 \in Anl(M)$, então $a_1a \in Anl(M)$.

De fato, $\forall\ m \in M$

$$\begin{aligned} (a_1a)m &= a_1(am) && \text{- pois } M \text{ é } A\text{-módulo} \\ &= 0 && \text{- pois } a_1 \in Anl(M) \text{ e } am \in M \end{aligned}$$

Logo, $(a_1a) \in Anl(M)$.

Segue de $(i), (ii), (iii)$ e (iv) que $Anl(M)$ é um ideal bilateral de A.

Determinaremos agora $Anl(M)$ quando M é visto como $A/Anl(M)$-módulo.

Por definição,

$$\begin{aligned} Anl(M) &= \{a + Anl(M) \in A/Anl(M) \mid (a + Anl(M))m = 0,\ \forall\, m \in M\} \\ &= \{a + Anl(M) \in A/Anl(M) \mid am = 0,\ \forall\, m \in M\} \\ &= \{a + Anl(M) \in A/Anl(M) \mid a \in Anl(M)\} \end{aligned}$$

Lembrando que para todo $a \in A$

$$\begin{aligned} a + Anl(M) &= \{a + a_1 \mid a_1 \in Anl(M)\} = \{a + a_1 \mid am = 0 \text{ e } a_1 m = 0, \forall\, m \in M\} \\ &= \{a_2 \mid a_2 = a + a_1 \in A \text{ e } a_2 m = 0, \forall\, m \in M\} \\ &= \{a_2 \mid a_2 \in A \text{ e } a_2 m = 0, \forall\, m \in M\} \\ &= \{a_2 \in A \mid a_2 m = 0, \forall\, m \in M\} = Anl(M) \end{aligned}$$

Então,

$$a + Anl(M) = Anl(M) = 0 + Anl(M)$$

Portanto,

$$Anl(M) = 0 + Anl(M).$$

Logo,

$$Anl(M) = \{0 + Anl(M)\}$$

e assim M é um $A/Anl(M)$-módulo fiel.

2.2 Módulo Quociente

Veremos agora o conceito de módulo quociente. Se N é um submódulo do A-módulo M, como $(M, +)$ é grupo abeliano segue que $N \lhd M$, logo podemos considerar o grupo quociente de M por N, isto é, M/N.

Sabemos que o grupo quociente é o grupo das classes laterais, isto é,

$$M/N = \{\overline{x} \mid x \in M\} \text{ onde } \overline{x} = \{x + n \mid n \in N\}$$

com a operação definida por

$$\overline{x} + \overline{y} = \overline{x + y}$$

Proposição 2.3. *Se $(M,+)$ é um A-módulo e N é um submódulo de M, então o grupo quociente M/N com o produto escalar*

$$\cdot : A \times M/N \longrightarrow M/N$$

$$(a, \overline{x}) \longrightarrow a \cdot \overline{x} = \overline{ax}$$

é um A-módulo, chamado A-módulo quociente de M/N.

Demonstração:

- Vamos mostrar primeiramente que a operação está bem definida.
  De fato, se $\overline{x} = \overline{y}$, temos $(x-y) \in N$, e então $a \cdot (x-y) \in N$ para qualquer $a \in A$, pois N é submódulo. Como N é também um A-módulo, tem-se

  $$a \cdot (x-y) \in N \Rightarrow (a \cdot x) - (a \cdot y) \in N \Rightarrow \overline{a \cdot x} = \overline{a \cdot y}.$$

  Assim, a operação está bem definida.

- Mostraremos que o M/N é um A-módulo.
  De fato, como $(M/N,+)$ é um grupo quociente, resta mostrarmos que M/N verifica as propriedades de multiplicação por escalar da definição de módulos.
  Com efeito, sejam $\overline{x_1}, \overline{x_2} \in M/N$ e $a_1, a_2 \in A$, assim

  (i) $a_1(a_2\overline{x_1}) = (a_1a_2)\overline{x_1}$.

  $$\begin{aligned} a_1(a_2\overline{x_1}) &= a_1(\overline{a_2x_1}) && \text{- definição de multiplicação por escalar} \\ &= \overline{a_1(a_2x_1)} && \text{- definição de multiplicação por escalar} \\ &= \overline{(a_1a_2)x_1} && \text{- pois } M \text{ é um } A\text{-módulo} \\ &= (a_1a_2)\overline{x_1} && \text{- definição de multiplicação por escalar} \end{aligned}$$

  (ii) $a_1(\overline{x_1} + \overline{x_2}) = a_1\overline{x_1} + a_1\overline{x_2}$.

  $$\begin{aligned} a_1(\overline{x_1} + \overline{y_2}) &= a_1(\overline{x_1 + x_2}) && \text{- definição de soma de classes} \\ &= \overline{a_1(x_1 + x_2)} && \text{- definição de multiplicação por escalar} \\ &= \overline{a_1x_1 + a_1x_2} && \text{- pois } M \text{ é um } A\text{-módulo} \\ &= \overline{a_1x_1} + \overline{a_1x_2} && \text{- definição de soma de classes} \\ &= a_1\overline{x_1} + a_1\overline{y_2} && \text{- definição de multiplicação por escalar} \end{aligned}$$

(iii) $(a_1 + a_2)\overline{x_1} = a_1\overline{x_1} + a_2\overline{x_1}$.

$$\begin{aligned}
(a_1 + a_2)\overline{x_1} &= \overline{(a_1 + a_2)x_1} && \text{- definição de multiplicação por escalar} \\
&= \overline{a_1x_1 + a_2x_1} && \text{- pois } M \text{ é um } A\text{-módulo} \\
&= \overline{a_1x_1} + \overline{a_2x_1} && \text{- definição de soma de classes} \\
&= a_1\overline{x_1} + a_2\overline{x_1} && \text{- definição de multiplicação por escalar}
\end{aligned}$$

(iv) $1_A \cdot \overline{x_1} = \overline{x_1}$.

$$\begin{aligned}
1_A \cdot \overline{x_1} &= \overline{1_A \cdot x_1} && \text{- definição de multiplicação por escalar} \\
&= \overline{x_1} && \text{- pois } M \text{ é um } A\text{-módulo}
\end{aligned}$$

Portanto, segue de $(i), (ii), (iii)$ e (iv) que M/N é um A-módulo. □

Capítulo 3

Homomorfismo de Módulos

Neste capítulo trataremos de homomorfismo de módulos, destacando suas principais propriedades, depois definiremos sequência exata que é apenas uma relação entre homomorfismos e por fim veremos a noção de diagramas comutativos.

Definição 3.1. *Sejam M e N dois A-módulos. Uma função $f : M \longrightarrow N$ chama-se um homomorfismo de A-módulos ou um A-homomorfismo, se para todos $m_1, m_2 \in M$ e todo $a \in A$ verificam-se:*
(i) $f(m_1 + m_2) = f(m_1) + f(m_2)$;
(ii) $f(am_1) = af(m_1)$.

Analogamente ao que ocorre com homomorfismo de grupos e anéis, $f : M \longrightarrow N$ é dito A-monomorfismo, A-epimorfismo ou A-isomorfismo ser f é, respectivamente injetora, sobrejetora e bijetora.

3.1 Núcleo e Imagem de um A-homomorfismo

Definição 3.2. *Sejam M e N dois A-módulos e $f : M \longrightarrow N$ um A-homomorfismo. Então:*
(i) *O conjunto $\{m \in M \mid f(m) = 0_N\}$ é chamado o núcleo de f e denotaremos por $ker(f)$;*
(ii) *O conjunto $\{f(m) \mid m \in M\}$ é chamado a imagem de f e denotaremos por $Im(f)$.*

Se $f : M \longrightarrow N$ é um A-homomorfismo, então f é um homomorfismo do grupo $(M, +)$ em $(N, +)$ logo valem todas as propriedades de homomorfismo de grupos.

Proposição 3.1. *Sejam M e N dois A-módulos e $f : M \longrightarrow N$ um A-homomorfismo, então $ker(f)$ e $Im(f)$ são submódulos de M e N, respectivamente.*

Demonstração:

(i) $ker(f)$ é um submódulo de M.

De fato, já sabemos que o $ker(f)$ é um subgrupo de $(M, +)$. Além disso, seja $a \in A$ e $m \in ker(f)$ arbitrários, então

$$\begin{aligned} f(am) &= af(m) && \text{- pois } f \text{ é um } A\text{-homomorfismo} \\ &= a0_N && \text{- pois } m \in ker(f) \\ &= 0_N \end{aligned}$$

Assim, $am \in ker(f)$, portanto $ker(f)$ é um submódulo de M.

(ii) $Im(f)$ é um submódulo de N.

De fato, já sabemos que a $Im(f)$ é um subgrupo de $(N, +)$. Além disso, seja $a \in A$ e $n \in Im(f)$, então existe $m \in M$ talque $f(m) = n$, daí $am \in M$, logo temos:

$$\begin{aligned} f(am) &= af(m) && \text{- pois } f \text{ é um } A\text{-homomorfismo} \\ &= an && \text{- pois } f(m) = n \end{aligned}$$

Assim, $an \in Im(f)$, pois $an \in N$ e existe $am \in M$ tal que $f(am) = an$.

Portanto, $Im(f)$ é um submódulo de N. □

Proposição 3.2. *Seja $f : M \longrightarrow N$ um A-homomorfismo. Então f é um A-monomorfismo, se e somente se, $ker(f) = \{0_M\}$.*

Demonstração:

Decorre diretamente do fato de $f : (M, +) \longrightarrow (N, +)$ ser um homomorfismo de grupos. □

Exemplo 3.1. Se A é um corpo, os A-homomorfismos são as transformações lineares entre espaços vetoriais sobre A.

De fato, como todo espaço vetorial sobre um corpo K é um K-módulo, então a definição de transformação linear coincide com a de A-homomorfismo.

Exemplo 3.2. Os homomorfismos de grupos abelianos são precisamente os $\mathbb{Z}$-homomorfismos.

De fato, Sejam M, N dois $\mathbb{Z}$-módulos e $f : M \longrightarrow N$ um $\mathbb{Z}$-homomorfismo, então em particular f é um homomorfismo de grupos abelianos. Reciprocamente, se M e N são dois grupos abelianos e $f : M \longrightarrow N$ um homomorfismo de grupo. Como todo grupo abeliano pode ser considerado como um $\mathbb{Z}$-módulo, segue que M e N são dois $\mathbb{Z}$-módulos, resta mostrarmos que $\forall\, k \in \mathbb{Z}$ e $\forall\, m \in M$, temos

$$f(km) = kf(m) \tag{3.1}$$

Vamos mostrar (3.1).

- Se $k \geq 0$, então mostraremos por indução sobre k.

  (i) $k = 0$

  $f(0m) = f(0) = 0 = 0 \cdot f(m)$ (Verdadeiro)

  (ii) Seja $k \geq 1$, suponhamos que vale para k, isto é

  $$f(km) = kf(m)$$

  Então, mostraremos que vale para $k + 1$, ou seja,

  $$f[(k+1)m] = (k+1)f(m)$$

  $$\begin{aligned} f[(k+1)m] &= f(km + m) && \text{- pois } m \in M \text{ e } M \text{ é um } \mathbb{Z}\text{-módulo} \\ &= f(km) + f(m) && \text{- pois } f \text{ é um homomorfismo de grupo} \\ &= kf(m) + f(m) && \text{- usando a hipótese de indução} \\ &= (k+1)f(m) && \text{- pois } f(m) \in N \text{ e } N \text{ é um } \mathbb{Z}\text{-módulo} \end{aligned}$$

  Portanto, segue que $f(km) = kf(m)$ vale $\forall\, k \geq 0$.

- Se $k < 0$, então $-k > 0$. Assim,

  $$\begin{aligned} 0 &= f(0) && \text{- propriedade de homomorfismo de grupos} \\ &= f[(k + (-k))m] && \text{- pois } m \in M \text{ e } M \text{ é um } \mathbb{Z}\text{-módulo} \\ &= f[km + (-k)m] && \text{- pois } m \in M \text{ e } M \text{ é um } \mathbb{Z}\text{-módulo} \\ &= f(km) + f[(-k)m] && \text{- pois } f \text{ é um homomorfismo de grupo} \\ &= f(km) + (-k)f(m) && \text{- pois } -k > 0 \text{ e } f(km) = kf(m) \text{ vale } \forall\, k \geq 0 \end{aligned}$$

Somando $kf(m)$ em ambos os lados a última igualdade, obtemos

$$kf(m) = f(km)$$

Portanto, a igualdade acima vale $\forall\, k \in \mathbb{Z}$ e $\forall\, m \in M$.

Exemplo 3.3. A função trivial $f : M \longrightarrow N$ definida por $f(m) = 0, \forall\ m \in M$ é um A-homomorfismo, chamado homomorfismo nulo, a qual será denotado por 0.

- De fato, vamos mostrar que f é um A-homomorfismo.

  (i) Sejam $m_1, m_2 \in M$, temos

$$\begin{aligned} f(m_1 + m_2) &= 0 && \text{- definição da } f \\ &= 0 + 0 && \text{- elemento neutro} \\ &= f(m_1) + f(m_2) && \text{- definição da } f \end{aligned}$$

  (ii) Seja $a \in A$ e $m \in M$, temos

$$\begin{aligned} f(am) &= 0 && \text{- definição da } f \\ &= a \cdot 0 && \text{- propriedade de grupo } a \cdot 0 = 0\ \forall\, a \in A \\ &= af(m) && \text{- pois } f(m) = 0 \text{ e } m \in M \end{aligned}$$

Exemplo 3.4. Seja N um submódulo de um A-módulo M. Então a função inclusão $i : N \hookrightarrow M$ definida por $i(x) = x,\ \forall\, x \in N$ é um A-homomorfismo. Em particular, a função $Id_M : M \longrightarrow M$ também é um A-homomorfismo.

De fato, $\forall\, n_1, n_2 \in N$ e $a \in A$, tem-se
$(i)\ f(n_1 + n_2) = f(n_1) + f(n_2)$

$$\begin{aligned} f(n_1 + n_2) &= n_1 + n_2 && \text{- definição da } f \\ &= f(n_1) + f(n_2) && \text{- definição da } f \end{aligned}$$

$(ii)\ f(an) = af(n)$

$$\begin{aligned} f(an) &= an && \text{- definição da } f \\ &= af(n) && \text{- definição da } f \end{aligned}$$

Segue de (i) e (ii) que a função inclusão é um A-homomorfismo. Em particular este resultado, vale se $N = M$, daí, temos a função Id_M sendo um A-homomorfismo.

Exemplo 3.5. Seja N um submódulo de um A-módulo M. Definimos o homomorfismo canônico ou projeção canônica à aplicação $\pi : M \longrightarrow M/N$, definida por $\pi(m) = \overline{m}, \forall\, m \in M$.

- Vamos mostrar que a projeção canônica é um epimorfismo, cujo o núcleo é N.
  (i) Sejam $m_1, m_2 \in M$, temos

$$\begin{aligned} \pi(m_1 + m_2) &= \overline{m_1 + m_2} && \text{- definição de } \pi \\ &= \overline{m_1} + \overline{m_2} && \text{- definição de soma de classes} \\ &= \pi(m_1) + \pi(m_2) && \text{- definição de } \pi \end{aligned}$$

  (ii) Sejam $a \in A$ e $m \in M$, temos

$$\begin{aligned} \pi(am) &= \overline{am} && \text{- definição de } \pi \\ &= a\overline{m} && \text{- definição de multiplicação por escalar de classes} \\ &= a\pi(m) && \text{- definição de } \pi \end{aligned}$$

  Segue de (i) e (ii) que a projeção canônica é um A-homomorfismo e

$$\begin{aligned} Im(\pi) &= \{\pi(m) \mid m \in M\} \\ &= \{\overline{m} \mid m \in M\} \\ &= M/N \end{aligned}$$

  Portanto, $Im(\pi) = M/N$, logo π é um epimorfismo, com

$$\begin{aligned} ker(\pi) &= \{m \in M \mid \pi(m) = \overline{0}\} \\ &= \{m \in M \mid \overline{m} = \overline{0}\} \\ &= \{m \in M \mid m \in N\} \\ &= N \end{aligned}$$

Exemplo 3.6. Seja M um A-módulo. Para cada elemento $a \in A$ definimos uma função $L_a : M \longrightarrow N$ por $L_a(m) = am, \forall\, m \in M$. Uma função desse tipo chama-se **homotetia**. Se $a \in Centro(A) = C(A)$ que é o seguinte conjunto

$$C(A) = \{a \in A \mid ax = xa, \forall\, x \in A\}$$

então, L_a é um A-homomorfismo.

De fato, $\forall\ m_1, m_2 \in M$ e $a \in A$, temos

$(i)\ L_a(m_1 + m_2) = L_a(m_1) + L_a(m_2)$

$$\begin{aligned} L_a(m_1 + m_2) &= a(m_1 + m_2) && \text{- definição de } L_a \\ &= am_1 + am_2 && \text{- pois } M \text{ é um } A\text{-módulo} \\ &= L_a(m_1) + L_a(m_2) && \text{- definição de } L_a \end{aligned}$$

$(ii)\ L_a(a_1 m) = a_1 L_a(m)$

$$\begin{aligned} L_a(a_1 m) &= a(a_1 m) && \text{- definição de } L_a \\ &= (aa_1)m && \text{- pois } M \text{ é um } A\text{-módulo} \\ &= (a_1 a)m && \text{- pois } a \in C(A) \\ &= a_1(am) && \text{- pois } M \text{ é um } A\text{-módulo} \\ &= a_1 L_a(m) && \text{- definição de } L_a \end{aligned}$$

Segue de (i) e (ii) que a homotetia é um A-homomorfismo.

Em particular, se A é comutativo, toda homotetia é um A-homomorfismo, pois todo elemento de A comuta com os demais, assim $A = C(A)$.

3.2 Propriedades do A-homomorfismo

Vejamos as propriedades dos A-homomorfismos.

Proposição 3.3. *Valem as seguintes afirmações:*

(i) *Sejam* $M \xrightarrow{f} M' \xrightarrow{g} M''$ *A-homomorfismos. Então* $g \circ f : M \longrightarrow M''$ *também é um A-homomorfismo.*

(ii) *Se* $M \xrightarrow{f} M' \xrightarrow{g} M'' \xrightarrow{h} M'''$ *são A-homomorfismos, então*

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

(iii) *Se* $M \xrightarrow{f_1} M', M \xrightarrow{f_2} M', M' \xrightarrow{g_1} M''$ *e* $M' \xrightarrow{g_2} M''$ *são A-homomorfismos, então*

$$g_1 \circ (f_1 + f_2) = g_1 \circ f_1 + g_1 \circ f_2$$

Vale também,

$$(g_1 + g_2) \circ f_1 = g_1 \circ f_1 + g_2 \circ f_1$$

(iv) *Dado um A-homomorfismo $f : M \longrightarrow N$, então*

$$Id_N \circ f = f \quad e \quad f \circ Id_M = f$$

(v) *Dados A-homomorfismos $M \xrightarrow{f} M'$ e $M' \xrightarrow{g} M$ tais que $g \circ f = Id_M$, então f é um monomorfismo e g um epimorfismo.*

Demonstração:

(i) Vamos mostrar que $g \circ f : M \longrightarrow M''$ também é um A-homomorfismo.

- Sejam $m_1, m_2 \in M$, então

$$\begin{aligned}
(g \circ f)(m_1 + m_2) &= g[f(m_1 + m_2)] && \text{- definição de composição de função} \\
&= g[f(m_1) + f(m_2)] && \text{- pois } f \text{ é um } A\text{-homomorfismo} \\
&= g[f(m_1)] + g[f(m_2)] && \text{- pois } g \text{ é um } A\text{-homomorfismo} \\
&= (g \circ f)(m_1) + (g \circ f)(m_2) && \text{- definição de composição de função}
\end{aligned}$$

- Sejam $a \in A$ e $m \in M$, temos

$$\begin{aligned}
(g \circ f)(am) &= g[f(am)] && \text{- definição de composição de função} \\
&= g[af(m)] && \text{- pois } f \text{ é um } A\text{-homomorfismo} \\
&= ag[f(m)] && \text{- pois } g \text{ é um } A\text{-homomorfismo} \\
&= a(g \circ f)(m) && \text{- definição de composição de função}
\end{aligned}$$

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

(ii) Vamos mostrar que $h \circ (g \circ f) = (h \circ g) \circ f$.

De fato, já foi mostrado no Capítulo 1, Exemplo 1.11 item (v).

(iii) Vamos mostrar que $g_1 \circ (f_1 + f_2) = g_1 \circ f_1 + g_1 \circ f_2$ e $(g_1 + g_2) \circ f_1 = g_1 \circ f_1 + g_2 \circ f_1$.

- Seja $m \in M$

$$\begin{aligned}
[g_1 \circ (f_1 + f_2)](m) &= g_1[(f_1 + f_2)(m)] && \text{- definição de composição de função} \\
&= g_1(f_1(m) + f_2(m)) && \text{- definição de soma de função} \\
&= g_1(f_1(m)) + g_1(f_2(m)) && \text{- pois } g \text{ é um } A\text{-homomorfismo} \\
&= (g_1 \circ f_1)(m) + (g_1 \circ f_2)(m) && \text{- definição de composição de função}
\end{aligned}$$

Portanto, $g_1 \circ (f_1 + f_2) = g_1 \circ f_1 + g_1 \circ f_2$.

- Seja $m \in M$

$$\begin{aligned}
[(g_1 + g_2) \circ f_1](m) &= (g_1 + g_2)(f_1(m)) && \text{- definição de composição de função} \\
&= g_1(f_1(m)) + g_2(f_1(m)) && \text{- definição de soma de função} \\
&= (g_1 \circ f_1)(m) + (g_2 \circ f_1)(m) && \text{- definição de composição de função}
\end{aligned}$$

Portanto, $(g_1 + g_2) \circ f_1 = g_1 \circ f_1 + g_2 \circ f_1$.

(iv) Vamos mostrar que $Id_N \circ f = f \quad \text{e} \quad f \circ Id_M = f$.

- Para todo $m \in M$, temos

$$\begin{aligned}
(Id_N \circ f)(m) &= Id_N(f(m)) && \text{- definição de composição de função} \\
&= f(m) && \text{- definição da identidade } Id_N(x) = x
\end{aligned}$$

Portanto, $Id_N \circ f = f$.

- Do outro lado, tem-se

$$\begin{aligned}
(f \circ Id_M)(m) &= f(Id_M(m)) && \text{- definição de composição de função} \\
&= f(m) && \text{- definição da identidade } Id_M(x) = x
\end{aligned}$$

Portanto, $f \circ Id_M = f$.

(v) Vamos mostrar que f é um monomorfismo e g um epimorfismo.

- f é um monomorfismo.

De fato, sejam $m_1, m_2 \in M$ tais que $f(m_1) = f(m_2)$. Aplicando a g em ambos os lados da igualdade, obtemos

$$g(f(m_1)) = g(f(m_2)) \Rightarrow \underbrace{(g \circ f)(m_1) = (g \circ f)(m_2)}_{\text{definição de composta}} \Rightarrow \underbrace{Id_M(m_1) = Id_M(m_2)}_{\text{hipótese}} \Rightarrow m_1 = m_2$$

Logo, f é um monomorfismo.

- g é um epimorfismo.

  De fato, seja $m \in M$, temos que $Id_M(m) = m$, então por hipótese, tem-se

  $$(g \circ f)(m) = m \Rightarrow g(f(m)) = m$$

  Chamando $f(m) = y \in M'$, temos $g(y) = m$.

  Portanto, g é um epimorfismo. □

Proposição 3.4. *Um A-homomorfismo $f : M \longrightarrow N$ é um A-isomorfismo, se e somente se, existe um A-homomorfismo $g : N \longrightarrow M$ tal que*

$$g \circ f = Id_M \quad e \quad f \circ g = Id_N. \tag{3.2}$$

Demonstração:

$(\Rightarrow)$ Suponhamos que f é isomorfismo, então f é bijetora, logo existe uma função inversa $g : N \longrightarrow M$ tal que $g \circ f = Id_M$ e $f \circ g = Id_N$. Resta mostrarmos que g é um A-homomorfismo. Com efeito,

(i) Mostraremos que $g(n_1 + n_2) = g(n_1) + g(n_2)$.

De fato, sejam $n_1, n_2 \in N$, como f é um epimorfismo, então existem $m_1, m_2 \in M$ tais que $f(m_1) = n_1$ e $f(m_2) = n_2$. Agora,

$$\begin{aligned} g(n_1) + g(n_2) &= g(f(m_1)) + g(f(m_2)) && \text{- substituição de } n_1 \text{ e } n_2 \\ &= (g \circ f)(m_1) + (g \circ f)(m_2) && \text{- definição de composta} \\ &= Id_M(m_1) + Id_M(m_2) && \text{- por hipótese } g \circ f = Id_M \\ &= m_1 + m_2 \quad (I) \end{aligned}$$

Como f é um A-homomorfismo, temos que

$$\begin{aligned} f(m_1 + m_2) &= f(m_1) + f(m_2) && \text{- pois } f \text{ é um } A\text{-homomorfismo} \\ &= n_1 + n_2 && \text{- pois } f(m_1) = n_1 \text{ e } f(m_2) = n_2 \end{aligned}$$

Aplicando g em ambos os membros da igualdade, temos

$g(f(m_1 + m_2)) = g(n_1 + n_2)$

$(g \circ f)(m_1 + m_2) = g(n_1 + n_2)$ - definição de composta

$Id_M(m_1 + m_2) = g(n_1 + n_2)$ - por hipótese $g \circ f = Id_M$

$m_1 + m_2 = g(n_1 + n_2) \qquad (II)$

Igualando (I) e (II) segue que $g(n_1 + n_2) = g(n_1) + g(n_2)$.

(ii) Mostraremos que $g(an) = ag(n)$.

De fato, seja $a \in A$ e $n \in N$, como f é um epimorfismo, existe um $m \in M$ tal que $f(m) = n$. Daí, aplicando a g, temos

$g(f(m)) = g(n)$

$(g \circ f)(m) = g(n)$ - definição de composta

$Id_M(m) = g(n)$ - por hipótese $g \circ f = Id_M$

$m = g(n)$ - definição de Id_M

$am = ag(n) \qquad (III)$ - multiplicando a na igualdade

Como f é um A-homomorfismo, tem-se

$$\begin{aligned} f(am) &= af(m) \\ &= an \qquad \text{- pois } f(m) = n \end{aligned}$$

Aplicando g em ambos os membros da igualdade, temos

$$\begin{aligned} g(an) &= g(f(am)) \\ &= (g \circ f)(am) \qquad \text{- definição de composta} \\ &= Id_M(am) \qquad \text{- por hipótese } g \circ f = Id_M \\ &= am \quad (IV) \qquad \text{- definição de } Id_M \end{aligned}$$

Igualando (III) e (IV) segue que $g(an) = ag(n)$.

Portanto, segue de (i) e (ii) que g é um A-homomorfismo.

$(\Leftarrow)$ Se existe $g : N \longrightarrow M$, tal que (3.2) ocorre, então f é bijetora, logo é um isomorfismo. □

Notação: Denotaremos $M \simeq N$ para indicar que M é isomorfo à N.

Teorema 3.1. *(Homomorfismo para módulos): Sejam M e N A-módulos. Se $f : M \longrightarrow N$ é um A-homomorfismo, então $M/ker(f) \simeq Im(f)$.*

Demonstração:

Para mostrarmos que $M/ker(f) \simeq Im(f)$, vamos construir um isomorfismo entre esses módulos. Para isto, vamos considerar as aplicações f, π e i, as relações entre elas pode ser visualizada no seguinte diagrama:

$$\begin{array}{ccc} M & \xrightarrow{\quad f \quad} & N \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ M/ker(f) & \xrightarrow{\quad g \quad} & Im(f) \end{array}$$

Assim, queremos a função g, então vamos defini-la da seguinte forma:

$$g : M/ker(f) \longrightarrow Im(f)$$

$$\overline{m} \longrightarrow f(m).$$

- Vamos verificar se g está bem definida.

  De fato, se

  $\overline{m_1} = \overline{m_2} \Rightarrow m_1 - m_2 \in ker(f) \Rightarrow f(m_1 - m_2) = 0 \Rightarrow f(m_1) - f(m_2) = 0 \Rightarrow f(m_1) = f(m_2).$

  Portanto, g está bem definida.

- Mostraremos que g é um A-homomorfismo.

  (i) Sejam $\overline{m_1}, \overline{m_2} \in M/ker(f)$, então

  $$\begin{aligned} g(\overline{m_1} + \overline{m_2}) &= g(\overline{m_1 + m_2}) && \text{- definição de soma de classes} \\ &= f(m_1 + m_2) && \text{- definição de } g \\ &= f(m_1) + f(m_2) && \text{- pois } f \text{ é um } A\text{-homomorfismo} \\ &= g(\overline{m_1}) + g(\overline{m_2}) && \text{- definição de } g \end{aligned}$$

  (ii) Sejam $\alpha \in A$ e $\overline{m_1} \in M/ker(f)$, então

  $$\begin{aligned} g(\alpha\overline{m_1}) &= g(\overline{\alpha m_1}) && \text{- definição de multiplicação por escalar de classe} \\ &= f(\alpha m_1) && \text{- definição de } g \\ &= \alpha f(m_1) && \text{- pois } f \text{ é um } A\text{-homomorfismo} \\ &= \alpha g(\overline{m_1}) && \text{- definição de } g \end{aligned}$$

  Portanto, segue de (i) e (ii) que g é um A-homomorfismo.

- g é injetora.

  Com efeito, sejam $m_1, m_2 \in M$ tais que $f(m_1) = f(m_2)$, então

  $f(m_1) = f(m_2) \Rightarrow f(m_1) - f(m_2) = 0 \Rightarrow f(m_1 - m_2) = 0 \Rightarrow m_1 - m_2 \in Ker(f) \Rightarrow \overline{m_1} = \overline{m_2}.$

- g é sobrejetora.

  De fato,

$$\begin{aligned} Im(g) &= \{g(\overline{m}) \mid \overline{m} \in M/kerf(f)\} \\ &= \{f(m) \mid m \in M\} \\ &= Im(f) \end{aligned}$$

  Segue então, que g é bijetora, logo g é um isomorfismo. □

Corolário 3.1. *Se $f : M \longrightarrow N$ é um A-epimorfismo, então $M/Ker(f) \simeq N$.*

Demonstração:

De fato, no teorema anterior mostramos que $M/Ker(f) \simeq Im(f)$, como por hipótese f é um A-epimorfismo, segue que $Im(f) = N$ e assim temos $M/Ker(f) \simeq N$. □

Corolário 3.2. *Seja A um anel. Todo A-módulo cíclico é isomorfo a um módulo quociente de A por um ideal à esquerda de A. Reciprocamente, se I é um ideal à esquerda de A, então A/I é um A-módulo cíclico.*

Demonstração:

Seja $M = (m)$ um A-módulo cíclico. Podemos definir um A-homomorfismo $f :_A A \longrightarrow M$ da seguinte forma:

$$f(a) = am, \quad \forall\, a \in A.$$

- Dados $a, b \in_A A$ e $m \in M$, tem-se:

  (i) $f(a + b) = f(a) + f(b)$.

$$\begin{aligned} f(a+b) &= (a+b)m && \text{- definição de } f \\ &= am + bm && \text{- pois } M \text{ é um } A\text{-módulo} \\ &= f(a) + f(b) && \text{- definição de } f \end{aligned}$$

  (ii) $a_1 f(a) = f(a_1 a)$.

$$\begin{aligned} a_1 f(a) &= a_1(am) && \text{- definição de } f \\ &= (a_1 a)m && \text{- pois } M \text{ é um } A\text{-módulo} \\ &= f(a_1 a) && \text{- definição de } f \end{aligned}$$

  Portanto, segue de (i) e (ii) que f é um A-homomorfismo.

- f é sobrejetora.

$$\begin{aligned} Im(f) &= \{f(a) \mid a \in {}_AA\} \\ &= \{am \mid a \in A\} \\ &= M \end{aligned}$$

Logo, $Im(f) = M$.

Assim, temos que f é um A-epimorfismo e usando o Corolário 3.1, temos $M \simeq A/ker(f)$.

Agora, como $ker(f)$ é um submódulo de ${}_AA$, pelo exemplo 2.11 de submódulo, temos que $ker(f)$ é um ideal à esquerda de A.

Reciprocamente, se I é um ideal à esquerda de A, então temos

$$\begin{aligned} A/I &= \{\overline{a} \mid a \in A\} \\ &= \{a\overline{1} \mid a \in A\} \\ &= (\overline{1}) \end{aligned}$$

Logo A/I é um A-módulo cíclico, gerado por $\overline{1}$. □

- **Classificaremos os grupos cíclicos a partir do Corolário 3.2**.

Como todo ideal de $\mathbb{Z}$ é principal da forma (m) com $m \in \mathbb{Z}$, temos que todo grupo cíclico é isomorfo a um quociente da forma $\mathbb{Z}/(m)$. Se $m = 0$, por exemplo o ideal nulo $I = \{0\}$ é principal, pois $I = 0A = \{0a \mid a \in A\}$, neste caso o grupo cíclico é isomorfo a $\mathbb{Z}$.

Teorema 3.2. *(Primeiro Teorema do Isomorfismo): Seja M um A-módulo e P e N dois submódulos tais que $P \subset N$. Então*

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

Demonstração:

Consideremos $f : M/P \longrightarrow M/N$ definida por $f(m + P) = m + N, \forall\, m \in M$. A função está bem definida, pois se $m_1, m_2 \in M$ são tais que

$$m_1 + P = m_2 + P \Rightarrow m_1 - m_2 \in P \subset N \Rightarrow m_1 - m_2 \in N \Rightarrow m_1 + N = m_2 + N.$$

- f é um A-homomorfismo, pois $\forall\, m_1, m_2 \in M, a \in A$, tem-se:

(i) $f[(m_1+P)+(m_2+P)] = f(m_1+P)+f(m_2+P)$

$$\begin{aligned} f[(m_1+P)+(m_2+P)] &= f[(m_1+m_2)+P] && \text{- definição de soma de classes} \\ &= (m_1+m_2)+N && \text{- definição de } f \\ &= (m_1+N)+(m_2+N) && \text{- definição de soma de classes} \\ &= f(m_1+P)+f(m_2+P) && \text{- definição de } f \end{aligned}$$

(ii) $f(a(m+P)) = f(m+P)$

$$\begin{aligned} f(a(m+P)) &= f(am+P) && \text{- definição de multiplicação por escalar de classes} \\ &= am+N && \text{- definição de } f \\ &= a(m+N) && \text{- definição de multiplicação por escalar de classes} \\ &= af(m+P) && \text{- definição de } f \end{aligned}$$

Portanto, segue de (i) e (ii) que f é um A-homomorfismo.

E como,

$$\begin{aligned} Im(f) &= \{f(m+P) \mid m+P \in M/P\} \\ &= \{m+N \mid m \in M\} \\ &= M/N \end{aligned}$$

Portanto, f é um epimorfismo.

Assim, pelo Corolário 3.1, temos

$$M/N \simeq \frac{M/P}{ker(f)}.$$

Agora,

$$\begin{aligned} ker(f) &= \{m+P \in M/P \mid f(m+P) = 0+N\} \\ &= \{m+P \in M/P \mid m+N = 0+N\} \\ &= \{m+P \in M/P \mid m \in N\} \\ &= N/P \end{aligned}$$

Portanto,

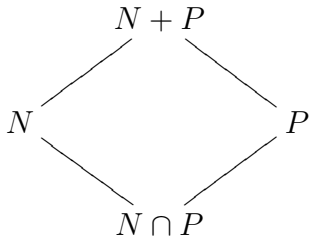
$$M/N \simeq \frac{M/P}{N/P}.$$

□

Teorema 3.3. *(Segundo Teorema do Isomorfismo): Sejam N e P submódulos de um A-módulo M. Então tem-se que*

$$\frac{N}{N \cap P} \simeq \frac{N+P}{P}.$$

A relação entre os submódulos do enunciado pode ser visualizada no seguinte diagrama:



Demonstração:

Consideremos $f : N \longrightarrow \dfrac{N+P}{P}$ definida por $f(n) = n + P$, $\forall\, n \in N$.

- Vamos mostrar que f é um A-homomorfismo.

  (i) Sejam $n_1, n_2 \in N$, mostraremos que $f(n_1 + n_2) = f(n_1) + f(n_2)$.

  De fato,

$$\begin{aligned} f(n_1+n_2) &= (n_1+n_2)+P && \text{- definição de } f \\ &= (n_1+P)+(n_2+P) && \text{- definição de soma de classes} \\ &= f(n_1)+f(n_2) && \text{- definição de } f \end{aligned}$$

  (ii) Sejam $a \in A$ e $n_1 \in N$, mostraremos que $f(an_1) = af(n_1)$.

  De fato,

$$\begin{aligned} f(an_1) &= (an_1)+P && \text{- definição de } f \\ &= a(n_1+P) && \text{- definição de multiplicação por escalar de classes} \\ &= af(n_1) && \text{- definição de } f \end{aligned}$$

  Portanto, segue de (i) e (ii) que f é um A-homomorfismo.

- Vamos mostrar que f é um epimorfismo.

  De fato,

$$\begin{aligned} Im(f) &= \{f(n) \mid n \in N\} \\ &= \{n + P \mid n \in N\} \\ &= \{(n + p) + P = n + P \mid n \in N \text{ e } p \in P\} \\ &= \{(n + p) + P \mid n \in N \text{ e } p \in P\} \\ &= \frac{N + P}{P} \end{aligned}$$

Portanto, f é um epimorfismo e pelo Corolário 3.1, temos

$$\frac{N}{ker(f)} \simeq \frac{N + P}{P}.$$

Por fim, observamos que dado $n \in N, n \in ker(f) \Leftrightarrow n + P = 0 + P \Leftrightarrow n - 0 = n \in P$.

Com efeito, se

$$n \in ker(f) \Leftrightarrow f(n) = 0 \Leftrightarrow n + P = 0 + P \Leftrightarrow n - 0 = n \in P.$$

Portanto, $n \in ker(f) \Leftrightarrow n \in P$.

Agora, se

$$n \in ker(f) \Leftrightarrow n \in N \text{ e } n \in P \Leftrightarrow n \in N \cap P.$$

Portanto, $ker(f) = N \cap P$.

Substituindo $ker(f)$, temos

$$\frac{N}{N \cap P} \simeq \frac{N + P}{P}.$$

O resultado acima é chamado, *isomorfismo de Noether*. □

3.3 Sequências Exatas

A noção de sequência exata que trataremos nesta seção é apenas uma linguagem que permite expressar certas relações entre homomorfismos por meio de diagramas.

Definição 3.3. *Sejam F, G, H três A-módulos, $f : F \longrightarrow G$ e $g : G \longrightarrow H$ A-homomorfismos. Dizemos que o diagrama*

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

é uma sequência de 2^a ordem em G se $Im(f) \subset ker(g)$.

Em particular, se $Im(f) = ker(g)$, dizemos que o diagrama é uma sequência exata em G.

Observação 3.1. A condição $Im(f) \subset ker(g)$ da definição acima é equivalente a afirmar que $g \circ f = 0$.

Demonstração:

($\Rightarrow$) Se $Im(f) \subset ker(g)$, então $g \circ f = 0$.

De fato, seja $x \in F$, temos

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) && \text{- definição de composta} \\ &= 0 && \text{- pois } f(x) \in ker(g) \text{ e } g(f(x)) = 0 \end{aligned}$$

Portanto, $g \circ f = 0$.

($\Leftarrow$) Se $g \circ f = 0$, então $Im(f) \subset ker(g)$.

Seja $y \in Im(f)$, então existe $x \in F$ tal que $f(x) = y$. Aplicando a g em ambos os lados da igualdade, temos

$$g(f(x)) = g(y) \Rightarrow (g \circ f)(x) = g(y) \Rightarrow \underbrace{O(x)}_{Hiptese} = g(y) \Rightarrow g(y) = 0$$

Assim, tem-se $y \in Im(f) \subset G$ e $g(y) = 0$, logo $y \in ker(g)$.

Definição 3.4. *Sejam $\{\ldots, M_{i-1}, M_i, M_{i+1}, \ldots\}$ uma família eventualmente infinita de A-módulos e $\{\ldots, f_i : M_i \longrightarrow M_{i+1}, \ldots\}$ uma família de A-homomorfismos. Dizemos que o diagrama*

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

é uma sequência exata, se é exata em M_i,para todo i, isto é, se

$$Im(f_{i-1}) = ker(f_i), \text{ para todo } i.$$

Exemplo 3.7. Sejam $0 = \{0\}$ o A-módulo nulo e $f : M \longrightarrow N$ um A-homomorfismo. A sequência $0 \xrightarrow{0} E \xrightarrow{f} F$ é exata, se e somente se, f é um monomorfismo.

De fato, como 0 é o A-homomorfismo nulo, temos que $Im(0) = ker(0) = \{0\}$. Assim,

f é monomorfismo $\Leftrightarrow ker(f) = \{0\} = Im(g) \Leftrightarrow$ a sequência é exata.

Exemplo 3.8. A sequência $E \xrightarrow{f} F \xrightarrow{0} 0$ é exata, se e somente se, f é um epimorfismo.

De fato, temos que 0 é o A-homomorfismo nulo, pois $0(x) = 0$, para todo $x \in F$, assim vamos determinar:

$$\begin{aligned} Im(0) &= \{0(x) \mid x \in F\} \\ &= \{0\} \end{aligned}$$

$$\begin{aligned} ker(0) &= \{x \in F \mid 0(x) = 0\} \\ &= F \end{aligned}$$

Temos também que $0 \circ f : E \longrightarrow 0$, definida por $(0 \circ f)(x) = 0$ é o homomorfismo nulo. Assim, f é um epimorfismo $\Leftrightarrow Im(f) = F = ker(0) \Leftrightarrow$ a sequência é exata.

Exemplo 3.9. Dos exemplos citados acima segue imediatamente que a sequência

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

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

De fato,

$$f \text{ é um isomorfismo} \Leftrightarrow \begin{cases} f & \text{é monomorfismo} \Leftrightarrow \text{a sequência } 0 \longrightarrow E \xrightarrow{f} F \text{ é exata} \\ f & \text{é epimorfismo} \Leftrightarrow \text{a sequência } E \xrightarrow{f} F \longrightarrow 0 \text{ é exata} \end{cases}$$

$\Leftrightarrow$ a sequência $0 \longrightarrow E \xrightarrow{f} F \longrightarrow 0$ é exata.

Exemplo 3.10. A sequência $0 \xrightarrow{0} M \xrightarrow{f} 0$ é exata, se e somente se, $M = \{0\}$.

De fato, como 0 é o A-homomorfismo nulo, tem-se que $Im(0) = \{0\} = ker(0)$. Agora temos $f : M \longrightarrow 0$, definida por $f(x) = 0$, para todo $x \in M$, logo f é o A-homomorfismo nulo, assim a $Im(f) = \{0\}$ e o $ker(f) = M$. Então,

$$M = \{0\} \Leftrightarrow ker(f) = Im(g) \Leftrightarrow \text{ a sequência é exata}$$

Exemplo 3.11. A sequência $0 \longrightarrow 2\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_2 \longrightarrow 0$, onde i é a inclusão e π é a projeção, é uma sequência exata.

De fato, sabemos que i é um monomorfismo, logo a sequência é exata em $2\mathbb{Z}$. Também, temos que π é um epimorfismo, logo ela é exata em $\mathbb{Z}_2$. Resta mostrarmos que a sequência é exata em $\mathbb{Z}$. Como,

$$\begin{aligned} Im(i) &= \{i(x) \mid x \in 2\mathbb{Z}\} \\ &= \{x \mid x \in 2\mathbb{Z}\} \\ &= 2\mathbb{Z} \end{aligned}$$

e

$$\begin{aligned} ker(\pi) &= \{x \in \mathbb{Z} \mid \pi(x) = \overline{0}\} \\ &= \{x \in \mathbb{Z} \mid \overline{x} = \overline{0}\} \\ &= \{x \in \mathbb{Z} \mid x \in 2\mathbb{Z}\} \\ &= 2\mathbb{Z} \end{aligned}$$

Portanto, $Im(i) = ker(\pi)$, logo $0 \longrightarrow 2\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_2 \longrightarrow 0$ é exata.

Definição 3.5. *Chamamos de sequência exata curta a toda sequência exata da forma*

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

Exemplo 3.12. Em geral, se E é um submódulo de um A-módulo F e indicamos por $i : E \longrightarrow F$ a inclusão e por $\pi : F \longrightarrow F/E$ a projeção canônica, então a sequência

$$0 \longrightarrow E \xrightarrow{i} F \xrightarrow{\pi} F/E \longrightarrow 0$$

é uma sequência exata curta.

De fato, sabemos que i é um monomorfismo, logo a sequência é exata em E e π é um epimorfismo, logo a sequência é exata em F/E é exata. Resta mostrarmos que a sequência $E \xrightarrow{i} F \xrightarrow{\pi} F/E$ é exata, para isto vamos determinar:

$$\begin{aligned} Im(i) &= \{i(x) \mid x \in E\} \\ &= \{x \mid x \in E\} \\ &= E \end{aligned}$$

$$\begin{aligned} ker(\pi) &= \{x \in F \mid \pi(x) = \overline{0}\} \\ &= \{x \in F \mid \overline{x} = \overline{0}\} \\ &= \{x \in F \mid x \in E\} \\ &= E \end{aligned}$$

Portanto, $Im(i) = ker(\pi)$, logo a sequência $E \xrightarrow{i} F \xrightarrow{\pi} F/E$ é exata. Segue então que a sequência $0 \longrightarrow E \xrightarrow{i} F \xrightarrow{\pi} F/E \longrightarrow 0$ é exata.

Mas geralmente, tem-se que toda sequência exata curta é da forma do Exemplo 3.12 para submódulos E' e F'.

De fato, seja

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

uma sequência exata curta, consideremos $E' = Im(f)$ e $f : E \longrightarrow F$ um A-homomorfismo. Pelo teorema do homomorfismo para módulos, temos

$$E/ker(f) \simeq Im(f).$$

Agora como a sequência $0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G \longrightarrow 0$ é exata, segue que f é um monomorfismo, então $ker(f) = \{0\}$, substituindo, o $ker(f)$, obtemos

$$E/\{0\} \simeq Im(f).$$

Considerando a função identidade $f : E \longrightarrow E$ e usando novamente o teorema do homomorfismo para módulos, segue

$$E/ker(f) \simeq Im(f).$$

Como a função identidade é injetora, temos que $ker(f) = \{0\}$ e a

$$Im(f) = \{f(x) \mid x \in E\} = \{x \mid x \in E\} = E.$$

Portanto,

$$E/\{0\} \simeq E.$$

Assim, tem-se

$$E \simeq E/\{0\} \simeq Im(f) = E'.$$

Logo,

$$E \simeq E'.$$

Agora, como a sequência $0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G \longrightarrow 0$ é exata, segue que g é um epimorfismo. Logo, pelo Corolário 3.1 tem-se

$$G \simeq F/ker(g).$$

como $Im(f) = ker(g)$, concluímos

$$G \simeq F/Im(f).$$

Então,

$$G \simeq F/E'.$$

Portanto, temos a seguinte sequência exata

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

onde os módulos são ordenadamente isomorfos aos da sequência original.

Exemplo 3.13. Dado um homomorfismo de A-módulos $f : E \longrightarrow F$ a seguinte sequência é exata

$$0 \longrightarrow ker(f) \xrightarrow{i} E \xrightarrow{f} F \xrightarrow{\pi} F/Im(f) \longrightarrow 0.$$

De fato, sabemos que i é um monomorfismo, logo a sequência é exata em $ker(f)$. Também, temos que π é um epimorfismo, logo a sequência é exata em $F/Im(f)$. E como $Im(i) = ker(f)$, então a sequência é exata em E. Por fim, resta mostrarmos que a sequência é exata em F, para isto determinemos $ker(\pi)$.

$$\begin{aligned} ker(\pi) &= \{x \in F \mid \pi(x) = \overline{0}\} \\ &= \{x \in F \mid \overline{x} = \overline{0}\} \\ &= \{x \in F \mid x \in Im(f)\} \\ &= Im(f) \qquad\qquad\qquad\qquad \text{– pois } F \subset Im(f) \end{aligned}$$

Logo, $Im(f) = ker(\pi)$, logo a sequência é exata em F. Portanto, segue que a sequência

$$0 \longrightarrow ker(f) \xrightarrow{i} E \xrightarrow{f} F \xrightarrow{\pi} F/Im(f) \longrightarrow 0$$

é exata.

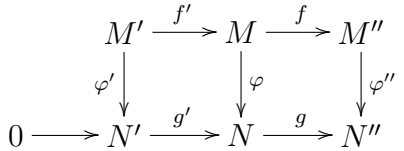
3.4 Diagramas Comutativos

Definição 3.6. *Dizemos que uma família de A-módulos $\mathcal{M}$ e uma família de A-homomorfismos $\mathcal{G}$ forma um diagrama comutativo, se para todo par de A-módulos $M, N \in \mathcal{M}$ e todo par de A-homomorfismos $f, g \in \mathcal{G}$ tais que $f : M \longrightarrow N$ e $g : M \longrightarrow N$, então $f = g$.*

Exemplo 3.14. Consideremos os seguintes diagramas

Dizemos que o primeiro diagrama é comutativo se $\theta = \psi \circ \varphi$ e o segundo, se $g \circ f = k \circ h$.

Proposição 3.5. *Seja*



um diagrama comutativo, onde as linhas são sequências exatas. Se φ' e φ'' são monomorfismos, então φ é monomorfismo.

Demonstração:

Seja $m \in M$ tais que $\varphi(m) = 0$. Mostraremos que $m = 0$.

De fato, aplicando g em $\varphi(m) = 0$, temos

$$
\begin{aligned}
\varphi(m) = 0 \quad &\Rightarrow \quad g(\varphi(m)) = g(0) \\
&\Rightarrow \quad g(\varphi(m)) = 0 && \text{- pois } g \text{ é um homomorfismo} \\
&\Rightarrow \quad (g \circ \varphi)(m) = 0 && \text{- definição de composta} \\
&\Rightarrow \quad (\varphi'' \circ f)(m) = 0 && \text{- pois o diagrama é comutativo, ou seja, } g \circ \varphi = \varphi'' \circ f \\
&\Rightarrow \quad \varphi''(f(m)) = 0 && \text{- definição de composta} \\
&\Rightarrow \quad f(m) \in Ker(\varphi'') = \{0\} && \text{- pois } \varphi'' \text{ é um monomorfismo} \\
&\Rightarrow \quad f(m) = 0 \\
&\Rightarrow \quad m \in ker(f) = Im(f') && \text{- pois a sequência é exata}
\end{aligned}
$$

Como $m \in Im(f')$, temos que existe $m' \in M'$ tal que $f'(m') = m$. Aplicando φ na igualdade, obtemos

$$
\begin{aligned}
f'(m') = m \quad &\Rightarrow \quad \varphi(f'(m')) = \varphi(m) \\
&\Rightarrow \quad (\varphi \circ f')(m') = 0 && \text{- pois } \varphi(m) = 0 \\
&\Rightarrow \quad (g' \circ \varphi')(m') = 0 && \text{- pois o diagrama é comutativo, ou seja, } \varphi \circ f' = g' \circ \varphi' \\
&\Rightarrow \quad m' \in ker(g' \circ \varphi') = \{0\} && \text{- pois } g' \text{ é um monomorfismo, pois a sequência é exata} \\
&\Rightarrow \quad m' = 0
\end{aligned}
$$

Logo, temos

$$f'(m') = m \Rightarrow f'(0) = m \Rightarrow m = 0.$$

Portanto, φ é monomorfismo. □

Proposição 3.6. *Seja*

$$\begin{array}{ccccccc} & & M' & \xrightarrow{f'} & M & \xrightarrow{f} & M'' \longrightarrow 0 \\ & & \downarrow{\scriptstyle \varphi'} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi''} \\ 0 & \longrightarrow & N' & \xrightarrow{g'} & N & \xrightarrow{g} & N'' \end{array}$$

um diagrama comutativo, onde as linhas são sequências exatas.

(i) *Se φ' e φ'' são epimorfismos, então φ é epimorfismo;*

(ii) *Se φ' e φ'' são isomorfismos, então φ é isomorfismo.*

Demonstração:

(i) Queremos mostrar que $N = Im(\varphi)$, ou seja, $\forall\ n \in N$, existe $m \in M$ tal que $n = \varphi(m)$. Assim, tomando $n \in M$ temos que $g(n) = n' = \varphi''(m'')$ para algum $m'' \in M'$, pois φ'' é epimorfismo e como $Im(f) = ker(0) = M''$, pois a sequência é exata em M'', então existe $m \in M$ tal que $f(m) = m''$, assim

$$\begin{array}{rcll} g(n) & = & \varphi''(f(m)) & \\ & = & (\varphi'' \circ f)(m) & \text{- definição de composta} \\ & = & (g \circ \varphi)(m) & \text{- pois } \varphi'' \circ f = g \circ \varphi \\ & = & g(\varphi(m)) & \text{- definição de composta} \end{array}$$

Assim,

$$g(\varphi(m)) - g(n) = 0 \Rightarrow g(\varphi(m) - n) = 0 \Rightarrow \varphi(m) - n \in ker(g) = Im(g').$$

Então, $\varphi(m) - n = g'(n')$ para algum $n' \in N'$ e como φ' é epimorfismo, temos que existe $m' \in M'$ tal que $\varphi'(m') = n'$. Assim,

$$\varphi(m) - n = g'(n') \Rightarrow \varphi(m) - n = g'(\varphi'(m')) \Rightarrow \varphi(m) - n = (g' \circ \varphi')(m').$$

Como o diagrama comuta, temos

$$\varphi(m) - n = (g' \circ \varphi')(m') \Rightarrow \varphi(m) - n = (\varphi \circ f')(m') \Rightarrow \varphi(m) - n = \varphi(f'(m')) \Rightarrow$$

$\varphi(m) - \varphi(f'(m')) = n \Rightarrow \varphi(m - f'(m')) = n.$

Fazendo $m_1 = m - f'(m') \in M$, temos

$$\varphi(m_1) = n, \text{ para algum } m_1 \in M.$$

Logo, φ é epimorfismo.

(ii) Segue do item (i) que se φ' e φ'' são epimorfismo, então φ também é. Resta mostrarmos que se φ' e φ'' são monomorfismo, então φ também é.

De fato, seja $m \in M$ tal que $\varphi(m) = 0$, vamos mostrar que $m = 0$. Com efeito,

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

Assim, $f(m) \in ker(\varphi'')$, como φ'' é monomorfismo, temos

$$f(m) = 0 \Rightarrow m \in ker(f) = Im(f') \Rightarrow m' \in M' \text{ tal que } m = f'(m').$$

Logo,

$$\varphi(m) = \varphi(f'(m')) \Rightarrow 0 = \varphi(f'(m')) \Rightarrow (\varphi \circ f')(m') = 0 \Rightarrow m' \in ker(\varphi \circ f') = ker(g' \circ \varphi') = \{0\}.$$

Portanto, $m = 0$. □

Proposição 3.7. *Seja*

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \xrightarrow{f_4} & M_4 \\ \downarrow{\scriptstyle h_1} & & \downarrow{\scriptstyle h_2} & & \downarrow{\scriptstyle h_3} & & \downarrow{\scriptstyle h_4} & & \downarrow{\scriptstyle h_5} \\ N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 & \xrightarrow{g_3} & N_4 & \xrightarrow{g_4} & N_5 \end{array}$$

um diagrama comutativo, onde as linhas são sequências exatas. Temos que

(i) *Se* h_1 *é epimorfismo e* h_4 *é monomorfismo, então* $ker(h_3) = f_2(ker(h_2))$;

(ii) *Se* h_2 *é epimorfismo e* h_4 *é monomorfismo, então* $g_3^{-1}(Im(h_4)) = (Im(h_3))$.

Demonstração:

(i) Seja $x \in M_3$ tal que $x \in ker(h_3)$, então $h_3(x) = 0$. Como o diagrama comuta, isto é, $h_4 \circ f_3 = g_3 \circ h_3$, temos

$(h_4 \circ f_3)(x) = (g_3 \circ h_3)(x) \Rightarrow h_4(f_3(x)) = g_3(h_3(x)) \Rightarrow h_4(f_3(x)) = g_3(0) \Rightarrow h_4(f_3(x)) = 0 \Rightarrow$ $f_3(x) \in ker(h_4) \Rightarrow f_3(x) = 0$, pois por hipótese h_4 é monomorfismo, logo $x \in ker(f_3)$. Assim, como a sequência é exata, tem-se

$$ker(h_3) \subset ker(f_3) = Im(f_2) \Rightarrow \exists\, y \in M_2 \text{ tal que } x = f_2(y).$$

Já que $g_2 \circ h_2 = h_3 \circ f_2$, então

$$g_2(h_2(y)) = h_3(f_2(y)) \Rightarrow g_2(h_2(y)) = h_3(x) \Rightarrow g_2(h_2(y)) = 0 \Rightarrow h_2(y) \in ker(g_2) = Im(g_1).$$

Dessa forma, $h_2(y) = g_1(z)$, para algum $z \in N_1$. Além disso, $h_2 \circ f_1 = g_1 \circ h_1$ e como h_1 é epimorfismo, obtemos

$$z = h_1(s), \text{ para algum } s \in M_1 \Rightarrow h_2(f_1(s)) = g_1(h_1(s)) \Rightarrow h_2(f_1(s)) = g_1(z) \Rightarrow h_2(f_1(s)) = h_2(y).$$

Logo,

$$h_2(f_1(s) - y) = 0 \Rightarrow f_1(s) - y \in ker(h_2) \Rightarrow f_1(s) - y = w \in ker(h_2) \Rightarrow y = f_1(s) - w.$$

Portanto,

$$x = f_2(y) = f_2(f_1(s) - w) = f_2(f_1(s)) - f_2(w) = -f_2(w).$$

Assim,

$$ker(h_3) \subset f_2(ker(h_2)).$$

Por outro lado, seja

$$f_2(m_2) \in f_2(ker(h_2)) \Rightarrow m_2 \in ker(h_2) \Rightarrow h_2(m_2) = 0.$$

e como $h_3 \circ f_2 = g_2 \circ h_2$, então

$$h_3(f_2(m_2)) = g_2(h_2(m_2)) = 0 \Rightarrow f_2(m_2) \in ker(h_3).$$

Assim, $f_2(ker(h_2)) \subset ker(h_3)$ e logo, $f_2(ker(h_2)) = ker(h_3)$.

(ii) Temos que

$$g_3^{-1}(Im(h_4)) = \{n_3 \in N_3 \mid g_3(n_3) = h_4(m_4)\}.$$

Assim, seja $n_3 \in Im(h_3)$, então existe $m_3 \in M_3$ tal que $n_3 = h_3(m_3)$ e como $g_3 \circ h_3 = h_4 \circ f_3$, tem-se

$$g_3(h_3(m_3)) = h_4(f_3(m_3)) = g_3(n_3).$$

Chamando $m_4 = f_3(m_3)$, temos

$$h_4(m_4) = g_3(n_3) \Rightarrow n_3 \in g_3^{-1}(Im(h_4)).$$

Portanto, $Im(h_3) \subset g_3^{-1}(Im(h_4))$.

Agora, se $n_3 \in g_3^{-1}(Im(h_4))$, então $g_3(n_3) = h_4(m_4)$. Como h_5 é monomorfismo, tem-se

$$g_4(g_3(n_3)) = g_4(h_4(m_4)) = h_5(f_4(m_4)) = 0 \Rightarrow f_4(m_4) = 0.$$

Logo,

$$m_4 \in ker(f_4) = Im(f_3) \Rightarrow m_4 = f_3(m_3), \text{ para algum } m_3 \in M_3.$$

Daí,

$$g_3(n_3) = h_4(m_4) = h_4(f_3(m_3)) = g_3(h_3(m_3)) \Rightarrow g_3(n_3 - h_3(m_3)) = 0 \Rightarrow$$

$$(n_3 - h_3(m_3)) = y \in ker(g_3) = Im(g_2).$$

Portanto,

$$n_3 - h_3(m_3) = g_2(h_2(m_2)) = h_3(f_2(m_2)) \Rightarrow n_3 = h_3(f_2(m_2) + m_3) \Rightarrow n_3 \in Im(h_3).$$

Logo, $g_3^{-1}(Im(h_4)) = (Im(h_3))$. □

Capítulo 4

Produto Direto e Somas

Neste capítulo daremos uma noção de produto direto, somas direta externa e interna, destacando a propriedade universal para produto direto e soma direta externa, que relação existe entre essas somas e por fim trataremos de projeção.

4.1 Produto Direto

Dados dois A-módulos M e N, podemos obter um novo A-módulo considerando o conjunto

$$P = \{(m, n) \mid m \in M \text{ e } n \in N\}$$

definindo as seguintes operações:

$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2)$$

$$\alpha(m_1, n_1) = (\alpha m_1, \alpha n_1)$$

$\forall\, \alpha \in A, \forall\, (m_1, n_1), (m_2, n_2) \in P$.

Quando consideramos famílias, eventualmente infinitas, de A-módulos, a construção anterior pode ser generalizada em dois sentidos.

Seja $\{M_i\}_{i \in I}$ uma família de A-módulos, onde I é um conjunto arbitrário de índices (finitos ou infinitos) e $M = \prod_{i \in I} M_i$ o produto cartesiano dos M_i, isto é,

$$M = \{(m_1, m_2, \ldots, m_n, \ldots) \mid m_i \in M_i,\ \forall\, i \in I\}.$$

Em M podemos introduzir uma estrutura de A-módulo definindo as seguintes operações para todo $\alpha \in A$ e $m_i, m_i' \in M_i$ para todo i.

$$(m_i)_{i\in I} + (m_i')_{i\in I} = (m_i + m_i')_{i\in I}$$

$$\alpha(m_i)_{i\in I} = (\alpha m_i)_{i\in I}$$

Definição 4.1. *O A-módulo M construído acima é chamado produto direto da família $\{M_i\}_{i\in I}$.*

Para cada $i \in I$, dizemos que o A-módulo M_i do produto direto M da família $\{M_i\}_{i\in I}$ é um fator de M.

Se I for um conjunto finito do tipo $I = \{1, 2, \ldots, n\}$ denotaremos o produto direto da seguinte forma

$$\prod_{i\in I} M_i = M_1 \times M_2 \times \ldots \times M_n.$$

Cada módulo M_i com $i \in I$, pode ser canônicamente imerso no produto direto M. Para isto, basta considerarmos as funções

$$i_k : M_k \longrightarrow M$$

$$m_k \longrightarrow i_k(m_k) = (x_i)_{i\in I} = \begin{cases} x_i = m_k & \text{se } i = k; \\ x_i = 0 & \text{se } i \neq k. \end{cases}$$

As funções assim definidas são monomorfismos que chamaremos *inclusões naturais*.

Como,

$$\begin{aligned} ker(i_k) &= \{m_k \in M_k \mid i_k(m_k) = 0\} \\ &= \{m_k \in M_k \mid (0, 0, \ldots, m_k, \ldots) = (0, 0, \ldots, 0, \ldots)\} \\ &= \{0\} \end{aligned}$$

logo, i_k é monomorfismo.

e também definamos

$$\pi_k : M \longrightarrow M_k$$

$$(m_i)_{i\in I} \longrightarrow \pi(m_i)_{i\in I} = m_k$$

As funções assim definidas são epimorfismos que chamaremos *projeções sobre as componentes*.

Como,

$$\begin{aligned} Im(\pi_k) &= \{\pi_k(m_i)_{i\in I} \mid (m_i)_{i\in I} \in M\} \\ &= \{m_k \in M_k\} \\ &= M_k \end{aligned}$$

logo, π_k é epimorfismo.

Proposição 4.1. *Sejam π_k as projeções sobre as componentes e i_k as inclusões naturais. Então temos:*

(i) $\pi_k \circ i_k = Id_{M_k},\ \forall\, k \in I$;

(ii) $\pi_k \circ i_h = 0,\ \forall\, h, k \in I$ *tal que* $h \neq k$.

Demonstração:

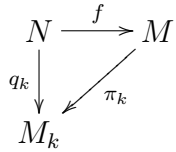
(i) Para todo $k \in I$ e todo $m_k \in M_k$, temos

$$\begin{aligned} (\pi_k \circ i_k)(m_k) &= \pi_k(i_k(m_k)) && \text{- definição de composta} \\ &= \pi_k(0, 0, \ldots, m_k, 0 \ldots) && \text{- definição de } i_k \\ &= m_k && \text{- definição de } \pi_k \\ &= Id_{M_k}(m_k) && \text{- definição de } Id_{M_k} \end{aligned}$$

(ii) Para todo $h, k \in I$ tais que $h \neq k$ e todo $m_h \in M_h$, temos

$$\begin{aligned} (\pi_k \circ i_h)(m_h) &= \pi_k(i_h(m_h)) && \text{- definição de composta} \\ &= \pi_k(0, \ldots, 0, \ldots, m_h, \ldots) && \text{- definição de } i_k \\ &= 0 && \text{- definição de } \pi_k \end{aligned}$$

Proposição 4.2. *Sejam $\{Mi\}_{i\in I}$ uma família de A-módulos, $M = \prod_{i\in I} M_i$ o produto direto desta família e $\{\pi_k : M \longrightarrow M_k\}_{k\in I}$ a família das projeções sobre as componentes. Dado um A-módulo N e uma família de A-homomorfismo $\{q_k : N \longrightarrow M_k\}_{k\in I}$, existe um único A-homomorfismo $f : N \longrightarrow M$ tal que o diagrama comuta, para todo $k \in I$.*



Demonstração:

- *Existência.*

  Consideremos $f : N \longrightarrow M$ definida por $f(n) = (q_i(n))_{i\in I}, \forall\, n \in N$. Vamos mostrar que f é um A-homomorfismo.

  Dados $n_1, n_2 \in N$ e $a \in A$, tem-se

  (i) $f(n_1 + n_2) = f(n_1) + f(n_2)$.

  $$\begin{aligned} f(n_1+n_2) &= (q_i(n_1+n_2))_{i\in I} && \text{- definição de } f \\ &= (q_i(n_1)+q_i(n_2))_{i\in I} && \text{- pois } q_i \text{ é } A\text{-homomorfismo} \\ &= (q_i(n_1))_{i\in I} + (q_i(n_2))_{i\in I} && \text{- definição de soma de } M \\ &= f(n_1)+f(n_2) && \text{- definição de } f \end{aligned}$$

  (ii) $f(an_1) = af(n_1)$.

  $$\begin{aligned} f(an_1) &= (q_i(an_1))_{i\in I} && \text{- definição de } f \\ &= (aq_i(n_1))_{i\in I} && \text{- pois } q_i \text{ é } A\text{-homomorfismo} \\ &= a(q_i(n_1))_{i\in I} && \text{- definição de multiplicação por escalar de } M \\ &= af(n_1) && \text{- definição de } f \end{aligned}$$

  Portanto, segue de (i) e (ii) que f é um A-homomorfismo.

  $\star$ Vamos mostrar que $\pi_k \circ f = q_k, \forall\, k \in I$.

  De fato, seja $n \in N$, temos que

  $$\begin{aligned} (\pi_k \circ f)(n) &= \pi_k(f(n)) && \text{- definição de composta} \\ &= \pi_k(q_i(n))_{i\in I} && \text{- definição de } f \\ &= q_k(n) && \text{- definição de } \pi_k \end{aligned}$$

  Portanto, $\pi_k \circ f = q_k$.

- *Unicidade*.

  Suponhamos que exista um A-homomorfismo $g : N \longrightarrow M$ que associa a todo $n \in N$ o elemento $(g_i(n))_{i\in I}$ em M e tal que $\pi_k \circ g = q_k, \forall\, k \in I$. Mostraremos que $f = g$.

  Com efeito, aplicando π_k em $g(n) = (g_i(n))_{i\in I}$, tem-se

  $$g(n) = (g_i(n))_{i\in I} \Rightarrow \pi_k(g(n)) = \pi_k(g_i(n))_{i\in I} \Rightarrow (\pi_k \circ g)(n) = g_k(n) \Rightarrow q_k(n) = g_k(n)$$

Portanto, $q_k = g_k$. Assim,

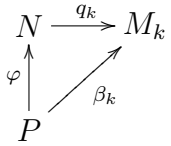
$$g(n) = (g_i(n))_{i\in I} \Rightarrow g(n) = (q_i(n))_{i\in I} \Rightarrow g(n) = f(n).$$

Logo, $f = g$.

Então concluímos que o A-homomorfismo f é único e que $\pi_k \circ f = q_k, \forall\, k \in I$. □

A existência e unicidade do A-homomorfismo f na proposição, é a menos de isomorfismo uma característica exclusiva do produto direto, tal propriedade é conhecida como *Propriedade Universal* do Produto Direto.

Proposição 4.3. *Sejam $\{M_i\}_{i\in I}$ uma família de A-módulos, $M = \prod_{i\in I} M_i$ o produto direto desta família e N um A-módulo arbitrário. Então, $N \simeq M$, se e somente se, existe uma família de A-homomorfismos $\{q_k : N \longrightarrow M_k\}_{k\in I}$ que tem a seguinte propriedade: dado qualquer A-módulo P e uma família de A-homomorfismos $\{\beta_k : P \longrightarrow M_k\}_{k\in I}$, então existe um único A-homomorfismo $\varphi : P \longrightarrow N$ tal que o diagrama*



é comutativo, para todo $k \in I$.

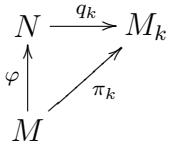
Demonstração:

($\Rightarrow$) Se $N \simeq M$, então existe uma família de A-homomorfismos $\{q_k : N \longrightarrow M_k\}_{k\in I}$ que tem a propriedade dada na Proposição 4.2.

Consideremos $N = M$ e $\{\pi_k : N \longrightarrow M_k\}_{k\in I}$ as projeções sobre as componentes, então o par $(M, \{\pi_k\})$ tem a propriedade universal, como mostrado na Proposição 4.2.

($\Leftarrow$) Se existe um par $(N, \{q_k\})$ que tem a propriedade universal, então $N \simeq M$.

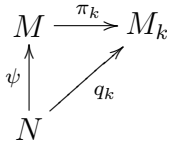
Consideremos, $P = M$ e $\{\pi_k : N \longrightarrow M_k\}_{k\in I}$ as projeções naturais, pela hipótese existe um A-homomorfismo $\varphi : M \longrightarrow N$ tal que o diagrama



comuta, isto é,

$$q_k \circ \varphi = \pi_k,\ \forall\, k \in I.$$

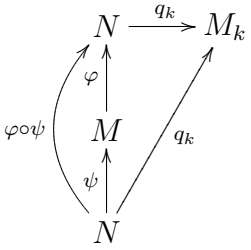
Pela Proposição 4.2, existe um A-homomorfismo $\psi : N \longrightarrow M$ tal que o diagrama



comuta, isto é,

$$\pi_k \circ \psi = q_k, \ \forall \ k \in I.$$

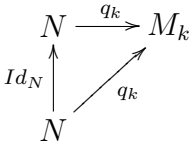
Juntando os diagramas, temos



Da comutatividade dos diagramas, temos que $q_k \circ \varphi = \pi_k$ e $\pi_k \circ \psi = q_k$, assim

$$\pi_k \circ \psi = q_k \Rightarrow (q_k \circ \varphi) \circ \psi = q_k \Rightarrow q_k \circ (\varphi \circ \psi) = q_k. \tag{4.1}$$

Por outro lado, a Id_N torna o diagrama



comutativo, isto é,

$$q_k \circ Id_N = q_k, \ \forall \ k \in I. \tag{4.2}$$

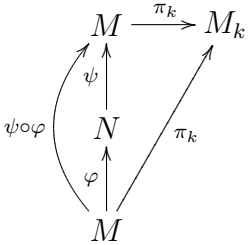
Igualando (4.1) e (4.2), obtemos

$$q_k \circ (\varphi \circ \psi) = q_k \circ Id_N.$$

Pela unicidade do A-homomorfismo, concluímos

$$\varphi \circ \psi = Id_N.$$

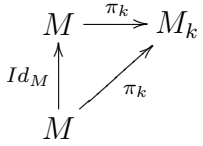
De modo análogo, tem-se



Da comutatividade dos diagramas, temos que $q_k \circ \varphi = \pi_k$ e $\pi_k \circ \psi = q_k$, assim

$$q_k \circ \varphi = \pi_k \Rightarrow (\pi_k \circ \psi) \circ \varphi = \pi_k \Rightarrow \pi_k \circ (\psi \circ \varphi) = \pi_k. \tag{4.3}$$

Como $(M, \{\pi_k\})$ tem a propriedade universal, segue que existe um único A-homomorfismo $Id : M \longrightarrow M$ tal que o diagrama



comuta, isto é,

$$\pi_k \circ Id_M = \pi_k, \ \forall \ k \in I. \tag{4.4}$$

Igualando (4.3) e (4.4), obtemos

$$\pi_k \circ (\psi \circ \varphi) = \pi_k \circ Id_M.$$

Pela unicidade do A-homomorfismo, concluímos

$$\psi \circ \varphi = Id_M.$$

Portanto, temos que o A-homomorfismo $\varphi : M \longrightarrow N$ é um A-isomorfismo, pois existe um A-homomorfismo $\psi : N \longrightarrow M$ tal que

$$\varphi \circ \psi = Id_N \quad \text{e} \quad \psi \circ \varphi = Id_M.$$

Logo, $N \simeq M$. □

Então, a menos de isomorfismo só o produto direto tem a propriedade universal.

4.2 Soma Direta Externa

Definição 4.2. *Sejam $\{M_i\}_{i \in I}$ uma família de A-módulos e $M = \prod_{i \in I} M_i$ o produto direto desta família. Um elemento $(m_i)_{i \in I} \in M$ chama-se **família quase nula**, se $m_i = 0$, exceto para um número finito de índices.*

Vamos denotar por $\sum_{i \in I} M_i$ o conjunto das famílias quase nulas de M, isto é,

$$\sum_{i \in I} M_i = \{(m_1, m_2, \ldots, m_n, 0, 0, \ldots) \mid n \in \mathbb{N} \text{ e } m_i \in M_i\}.$$

Observamos que este conjunto é um submódulo de M, pois temos que $\sum_{i\in I} M_i \subset M$, pois basta considerarmos a partir de uma quantidade finita de índices, $0 \in M_i, \forall\, i \in I$, também temos:

(i) $(0)_{i\in I} \in \sum_{i\in I} M_i$, pois $m_i = 0$ exceto para um nº finito de índices, em que este número é zero.

(ii) O fechamento com relação a soma de famílias quase nulas de M, ou seja, para todos $(m_i)_{i\in I}$, $(m_i')_{i\in I} \in \sum_{i\in I} M_i$, tem-se

$$(m_i)_{i\in I} + (m_i')_{i\in I} = (m_i + m_i')_{i\in I} \in \sum_{i\in I} M_i.$$

(iii) O fechamento com relação a multiplicação por escalar de famílias quase nulas de M, ou seja, para todo $(m_i)_{i\in I} \in \sum_{i\in I} M_i$ e todo $\alpha \in A$, tem-se

$$\alpha(m_i)_{i\in I} = (\alpha m_i)_{i\in I} \in \sum_{i\in I} M_i.$$

Portanto, $\sum_{i\in I} M_i$ é um A-módulo, chamado *soma direta externa* da família $\{M_i\}_{i\in I}$.

Se o conjunto de índices for finito, $I = \{1, 2, \ldots, n\}$, denotaremos a soma direta externa por

$$\sum_{i\in I} M_i = M_1 + M_2 + \ldots + M_n.$$

Observação 4.1. *Se o conjunto de índices I for finito, então* $\sum_{i\in I} M_i = \prod_{i\in I} M_i$.

Como foi feito no produto direto, na soma direta externa, pode-se também definir as *inclusões naturais* $i_k : M_k \longrightarrow \sum_{i\in I} M_i$, onde $i_k(m_k) = (x_i)_{i\in I}$, com $x_k = m_k$ e $x_i = 0$ se $i \neq k$ e as *projeções naturais* $\pi_k : \sum_{i\in I} M_i \longrightarrow M_k$, com $\pi_k(m_i)_{i\in I} = m_k$.

Seja $(m_i)_{i\in I} \in \sum_{i\in I} M_i$, então temos

$$\begin{aligned}
(m_i)_{i\in I} &= (m_1, m_2, \ldots, m_n, 0, 0, \ldots) \\
&= (m_1, 0, \ldots, 0, 0, \ldots) + (0, m_2, \ldots, 0, 0, \ldots) + \cdots + (0, 0, \ldots, m_n, 0, 0, \ldots) \\
&= i_1(m_1) + i_2(m_2) + \cdots + i_n(m_n) \\
&= \sum_{k=1}^{n} i_k(m_k) \\
&= \sum_{k=1}^{n} i_k(\pi_k(m_i)_{i\in I}) \\
&= \sum_{k=1}^{n} (i_k \circ \pi_k)(m_i)_{i\in I}
\end{aligned}$$

Assim como foi feito no produto direto, temos a seguinte proposição.

Proposição 4.4. *Sejam π_k as projeções sobre as componentes e i_k as inclusões naturais. Então temos:*

(i) $\pi_k \circ i_k = Id_{M_k}$, $\forall\ k \in I$;

(ii) $\pi_k \circ i_h = 0$ *se* $h \neq k$.

Demonstração:

(i) Seja $m_k \in M_k$, assim temos

$$\begin{aligned}
(\pi_k \circ i_k)(m_k) &= \pi_k(i_k(m_k)) && \text{- definição de composta}\\
&= \pi_k(0, 0, \ldots, m_k, 0, \ldots) && \text{- definição de } i\\
&= m_k && \text{- definição de } \pi_k\\
&= Id_{M_k} && \text{- definição de } Id_{M_k}
\end{aligned}$$

(ii) Sejam $m_h \in M_h$ com $h \neq k$, temos

$$\begin{aligned}
(\pi_k \circ i_h)(m_h) &= \pi_k(i_h(m_h)) && \text{- definição de composta}\\
&= \pi_k(0, 0, \ldots, m_h, 0, \ldots) && \text{- definição de } i\\
&= 0 && \text{- definição de } \pi_k
\end{aligned}$$

□

Proposição 4.5. *Sejam $\{M_i\}_{i\in I}$ uma família de A-módulos, $M = \sum_{i\in I} M_i$ a soma direta externa e $\{i_k : M_k \longrightarrow M\}_{k\in I}$ as inclusões naturais. Dado um A-módulo N e uma família de A-homomorfismos $\{h_k : M_k \longrightarrow N\}_{k\in I}$, então existe um único A-homomorfismo $f : M \longrightarrow N$ tal que o diagrama*

$$\begin{array}{ccc}
M & \xrightarrow{f} & N \\
{\scriptstyle i_k}\uparrow & \nearrow_{h_k} & \\
M_k & &
\end{array}$$

é comutativo, $\forall\ k \in I$.

Demonstração:

- *Existência.*

  Consideremos $f : M \longrightarrow N$ definida por $f((m_i)_{i\in I}) = \sum_{k\in I} h_k(m_k), \forall\ (m_i)_{i\in I} \in M$.

Vamos mostrar que f é um A-homomorfismo.

Sejam $(m_i)_{i\in I}, (m'_i)_{i\in I} \in M$ e $a \in A$, então

(i) $f((m_i)_{i\in I} + (m'_i)_{i\in I}) = f((m_i)_{i\in I}) + f((m'_i)_{i\in I})$.

$$\begin{aligned}
f((m_i)_{i\in I} + (m'_i)_{i\in I}) &= f((m_i + m'_i)_{i\in I}) && \text{- definição de soma de } M\\
&= \sum_{k\in I} h_k(m_k + m'_k) && \text{- definição de } f\\
&= \sum_{k\in I} [h_k(m_k) + h_k(m'_k)] && \text{- pois } h_k \text{ é } A\text{-homomorfismo}\\
&= \sum_{k\in I} h_k(m_k) + \sum_{k\in I} h_k(m'_k) && \text{- propriedade de somatório}\\
&= f((m_i)_{i\in I}) + f((m'_i)_{i\in I}) && \text{- definição de } f
\end{aligned}$$

(ii) $f(a(m_i)_{i\in I}) = af((m_i)_{i\in I})$.

$$\begin{aligned}
f(a(m_i)_{i\in I}) &= f((am_i)_{i\in I}) && \text{- definição de multiplicação por escalar de } M\\
&= \sum_{k\in I} h_k(am_k) && \text{- definição de } f\\
&= \sum_{k\in I} ah_k(m_k) && \text{- pois } h_k \text{ é } A\text{-homomorfismo}\\
&= a\sum_{k\in I} h_k(m_k) && \text{- propriedade de somatório}\\
&= af((m_i)_{i\in I}) && \text{- definição de } f
\end{aligned}$$

Segue de (i) e (ii) que f é um A-homomorfismo.

$\star$ Vamos mostrar que $f \circ i_k = h_k, \forall\ k \in I$.

Dado $m_k \in M_k$, temos que

$$\begin{aligned}
(f \circ i_k)(m_k) &= f(i_k(m_k)) && \text{- definição de composta}\\
&= f(0, 0, \ldots, m_k, 0, \ldots) && \text{- definição de } i\\
&= \sum_{i\in I} h_i(m_i) && \text{- definição de } f\\
&= h_1(0) + h_2(0) + \cdots + h_k(m_k) + \cdots\\
&= 0 + 0 + \cdots + h_k(m_k) + 0 + \cdots && \text{- pois } h_i \text{ é } A\text{-homomorfismo}\\
&= h_k(m_k)
\end{aligned}$$

Portanto, $f \circ i_k = h_k$.

- *Unicidade*.

  Suponhamos que exista um A-homomorfismo $g : M \longrightarrow N$ tal que $g \circ i_k = h_k, \forall\ k \in I$.

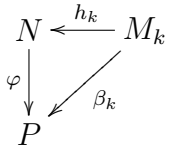
  Mostraremos que $f = g$.

  Com efeito, seja $(m_i)_{i\in I} \in M$, temos

$$\begin{aligned}
g((m_i)_{i\in I}) &= g\left(\sum_{k\in I} i_k(m_k)\right) && \text{- pois } (m_i)_{i\in I} = \sum_{k\in I} i_k(m_k)\\
&= \sum_{k\in I} g(i_k(m_k)) && \text{- pois } g \text{ é } A\text{-homomorfismo}\\
&= \sum_{k\in I} (g \circ i_k)(m_k) && \text{- definição de composta}\\
&= \sum_{k\in I} h_k(m_k) && \text{- por hipótose, pois } g \circ i_k = h_k\\
&= f(m_i)_{i\in I}
\end{aligned}$$

  Logo, $f = g$. □

Proposição 4.6. *Sejam $\{M_i\}_{i\in I}$ uma família de A-módulos, $M = \sum_{i\in I} M_i$ a soma direta externa e N um A-módulo qualquer. Então $N \simeq M$ se, e somente se, existe uma família de A-homomorfismos $\{h_k : M_k \longrightarrow N\}_{k\in I}$ que tem a seguinte propriedade: dado qualquer A-módulo P e uma família de A-homomorfismos $\{\beta_k : M_k \longrightarrow P\}_{k\in I}$, então existe um único A-homomorfismo $\varphi : N \longrightarrow P$ tal que o diagrama*



é comutativo, $\forall\ k \in I$.

Demonstração:

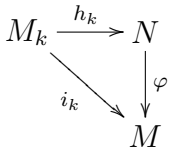
($\Rightarrow$) Se $N \simeq M$, então existe uma família de A-homomorfismos $\{q_k : N \longrightarrow M_k\}_{k\in I}$ que tem a propriedade dada na proposição.

Consideremos $N = M$ e $\{i_k : M_k \longrightarrow M\}_{k\in I}$ as inclusões, então o par $(M, \{i_k\})$ tem a propriedade universal, como mostrado na Proposição 4.5.

($\Leftarrow$) Se existe um par $(N, \{h_k\})$ que tem a propriedade universal, então $N \simeq M$.

Consideremos, $P = M$ e $\{i_k : M_k \longrightarrow M\}_{k\in I}$ as inclusões naturais, pela hipótese existe um

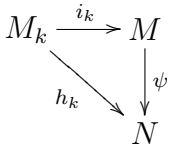
A-homomorfismo $\varphi : N \longrightarrow M$ tal que o diagrama



comuta, isto é,

$$\varphi \circ h_k = i_k, \ \forall \ k \in I.$$

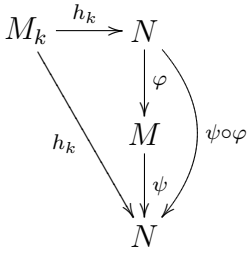
Pela Proposição 4.5 existe um A-homomorfismo $\psi : M \longrightarrow N$ tal que o diagrama



comuta, isto é,

$$\psi \circ i_k = h_k, \ \forall \ k \in I.$$

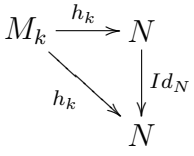
Juntando os diagramas, temos



Da comutatividade dos diagramas, temos que $\varphi \circ h_k = i_k$ e $\psi \circ i_k = h_k$, assim

$$\psi \circ i_k = h_k \Rightarrow \psi \circ (\varphi \circ h_k) = h_k \Rightarrow (\psi \circ \varphi) \circ h_k = h_k. \tag{4.5}$$

Por outro lado, a Id_N torna o diagrama



comutativo, isto é,

$$Id_N \circ h_k = h_k, \ \forall \ k \in I. \tag{4.6}$$

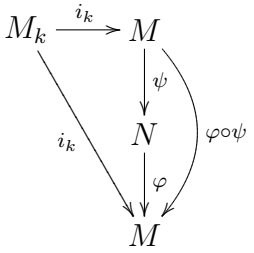
Igualando (4.5) e (4.6), obtemos

$$(\psi \circ \varphi) \circ h_k = Id_N \circ h_k.$$

Pela unicidade do A-homomorfismo, concluímos

$$\psi \circ \varphi = Id_N.$$

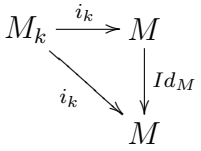
De modo análogo, tem-se



Da comutatividade dos diagramas, temos que $\varphi \circ h_k = i_k$ e $\psi \circ \ i_k = h_k$, assim

$$\varphi \circ h_k = i_k \Rightarrow \varphi \circ (\psi \circ \ i_k) = i_k \Rightarrow (\varphi \circ \psi) \circ i_k = i_k. \tag{4.7}$$

Como o par $(M, \{i_k\})$ tem a propriedade universal, segue que existe um único A-homomorfismo $Id_M : M \longrightarrow M$ tal que o diagrama



comuta, isto é,

$$Id_M \circ i_k = i_k, \ \forall \ k \in I. \tag{4.8}$$

Igualando (4.7) e (4.8), obtemos

$$(\varphi \circ \psi) \circ i_k = Id_M \circ i_k.$$

Pela unicidade do A-homomorfismo, concluímos

$$\varphi \circ \psi = Id_M.$$

Portanto, temos que o A-homomorfismo $\varphi : M \longrightarrow N$ é um A-isomorfismo, pois existe um A-homomorfismo $\psi : N \longrightarrow M$ tal que

$$\psi \circ \varphi = Id_N \quad \text{e} \quad \varphi \circ \psi = Id_M.$$

Logo, $N \simeq M$. □

Então, a menos de isomorfismo, somente a soma direta externa tem a propriedade universal.

4.3 Soma Direta Interna

Consideraremos neste seção, um conjunto finito de índices, ou seja, $I = \{1, 2, \ldots, n\}$.

Seja $\{M_i\}_{i\in I}$ uma família de submódulo de um A-módulo M, denotaremos por $M_1 + M_2 + \cdots + M_n$ o submódulo de M gerado pela $\bigcup_{i\in I} M_i$, isto é,

$$M_1 + M_2 + \cdots + M_n = \{m_1 + m_2 + \cdots + m_n \mid m_i \in M_i, \forall\, i \in I\}.$$

Definição 4.3. *Dizemos que uma família de submódulos $\{M_i\}_{i\in I}$ de um A-módulo M é independente se para todo índice i temos,*

$$M_i \cap (M_1 + M_2 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n) = \{0\}.$$

Proposição 4.7. *Uma família de submódulos $\{M_i\}_{i\in I}$ de um A-módulo M é independente, se e somente se,*

$$\sum_{i=1}^{n} m_i = 0,\ \textit{com}\ m_i \in M_i,\ \textit{tem-se}\ m_i = 0, \forall\, i \in I.$$

Demonstração:

($\Rightarrow$) Se a família $\{M_i\}_{i\in I}$ é independente e $\sum_{i=1}^{n} m_i = 0$ com $m_i \in M_i$, então $m_i = 0, \forall i \in I$.

De fato, como $\sum_{i=1}^{n} m_i = 0$, temos

$$m_1 + \cdots + m_{i-1} + m_i + m_{i+1} + \cdots + m_n = 0 \Rightarrow m_i = -(m_1 + \cdots + m_{i-1} + m_{i+1} + \cdots + m_n).$$

Então, $m_i \in M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n$, mas também temos $m_i \in M_i$, assim

$$m_i \in M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n).$$

Por hipótese, sabemos que a família $\{M_i\}_{i\in I}$ é independente, logo

$$M_i \cap (M_1 + M_2 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n) = \{0\}.$$

Segue então que $m_i = 0, \forall\, i \in I$.

($\Leftarrow$) Se $\sum_{i=1}^{n} m_i = 0$, implica que $m_i = 0, \forall\, i \in I$, então a família $\{M_i\}_{i\in I}$ é independente.

Seja $m_i \in M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n)$, mostraremos que $m_i = 0$.

De fato, se $m_i \in M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n)$, temos que $m_i \in M_i$ e $m_i \in (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n)$, assim temos

$$m_i = m_1 + \cdots + m_{i-1} + m_{i+1} + \cdots + m_n \Rightarrow m_1 + \cdots + m_{i-1} + (-m_i) + m_{i+1} + \cdots + m_n = 0 \Rightarrow \sum_{i=1}^{n} m_i = 0.$$

Por hipótese, segue que $m_i = 0, \forall\, i \in I$.

Portanto, $M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n) = \{0\}$, logo a família $\{M_i\}_{i \in I}$ é independente. □

Proposição 4.8. *Seja $\{M_i\}_{i \in I}$ uma família de submódulos de um A-módulo M. Esta família é independente se, e somente se,*

$$\sum_{i=1}^{n} m_i = \sum_{i=1}^{n} m_i' \text{ com } m_i, m_i' \in M_i, \forall\, i \in I, \text{ implicar que } m_i = m_i', \forall\, i \in I.$$

Demonstração:

($\Rightarrow$) Suponhamos que a família $\{M_i\}_{i \in I}$ seja independente e que $\sum_{i=1}^{n} m_i = \sum_{i=1}^{n} m'i, \forall\, i \in I$, então $m_i = m_i', \forall\, i \in I$.

De fato, por hipótese temos

$$\sum_{i=1}^{n} m_i = \sum_{i=1}^{n} m'i \Rightarrow \sum_{i=1}^{n} m_i - \sum_{i=1}^{n} m'i = 0 \Rightarrow \sum_{i=1}^{n} (m_i - m_i') = 0.$$

E também que $\{M_i\}_{i \in I}$ é independente, logo usando a Proposição 4.7, tem-se

$$m_i - m_i' = 0 \Rightarrow m_i = m_i', \forall i \in I.$$

($\Leftarrow$) Se $\sum_{i=1}^{n} m_i = \sum_{i=1}^{n} m'i$ com $m_i, m_i' \in M_i, \forall\, i \in I,$ implicar que $m_i = m_i', \forall\, i \in I$, então a família $\{M_i\}_{i \in I}$ é independente.

De fato, consideremos

$$m_1 + m_2 + \cdots + m_n = 0.$$

Podemos escrever, $0 \in M$, da seguinte forma

$$0 + 0 + \cdots + 0 = 0.$$

Da unicidade do elemento neutro, segue

$$m_1 + m_2 + \cdots + m_n = 0 + 0 + \cdots + 0 \Rightarrow \sum_{i=1}^{n} m_i = \sum_{i=1}^{n} 0.$$

Por hipótese, temos

$$m_i = 0, \forall\, i \in I.$$

Assim, usando a Proposição 4.7, concluímos que a família $\{M_i\}_{i\in I}$ é independente. □

Definição 4.4. *Dizemos que um A-módulo M é uma soma direta interna da família $\{M_i\}_{i\in I}$ de seus submódulos se*

(i) $M = M_1 + M_2 + \cdots + M_n$; *($M$ é gerado pelos M_i's)*

(ii) $\{M_i\}_{i\in I}$ *é uma família de submódulos independentes.*

Se M é a soma *direta interna* de $\{M_i\}_{i\in I}$, denotaremos M por

$$M = \oplus_{i\in I} M_i.$$

Como o conjunto de índices é finito escrevemos a soma direta interna por

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n.$$

Exemplo 4.1. Para qualquer A-módulo M, temos que $M = M \oplus \{0\}$. Então os submódulos M e $\{0\}$ são chamados de somandos diretos triviais de M.

Exemplo 4.2. Consideremos o $\mathbb{Z}$-módulo $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ e seus submódulos $H_1 = \{\overline{0}, \overline{2}, \overline{4}\}$ e $H_2 = \{\overline{0}, \overline{3}\}$.

Como,

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

Concluímos que $\forall\, \overline{m} \in \mathbb{Z}_6$, temos

$$\overline{m} = \overline{h_1} + \overline{h_2}, \text{ com } \overline{h_1} \in H_1 \text{ e } \overline{h_2} \in H_2.$$

Além disso, $H_1 \cap H_2 = \{\overline{0}\}$. Logo, $\mathbb{Z}_6 = H_1 \oplus H_2$.

Veremos agora a relação entre soma direta externa e a soma interna de M.

Proposição 4.9. *Seja M um A-módulo e $\{M_i\}_{i\in I}$ uma família de submódulos independentes de M. Então,*

$$\sum_{i\in I} M_i \simeq \oplus_{i\in I} M_i.$$

Demonstração:

Consideremos a seguinte função

$$f : \sum_{i\in I} M_i \longrightarrow \oplus_{i\in I} M_i$$

$$(m_1, m_2, \ldots, m_n) \longrightarrow f(m_1, m_2, \ldots, m_n) = m_1 + m_2 + \cdots + m_n.$$

Vamos mostrar que f é um A-homomorfismo.

Sejam $(m_i)_{i\in I}, (m'_i)_{i\in I} \in \sum_{i\in I} M_i$ e $a \in A$, então

(i) $f((m_i)_{i\in I} + (m'_i)_{i\in I}) = f((m_i)_{i\in I}) + f((m'_i)_{i\in I})$.

$$\begin{aligned} f((m_i)_{i\in I} + (m'_i)_{i\in I}) &= f((m_i + m'_i)_{i\in I}) && \text{- definição de soma de } \sum_{i\in I} M_i \\ &= (m_1 + m'_1) + \cdots + (m_n + m'_n) && \text{- definição de } f \\ &= (m_1 + \cdots + m_n) + (m'_1 + \cdots + m'_n) && \text{- associando e comutando} \\ &= f((m_i)_{i\in I}) + f((m'_i)_{i\in I}) && \text{- definição de } f \end{aligned}$$

(ii) $f(\alpha(m_i)_{i\in I}) = \alpha f((m_i)_{i\in I})$.

$$\begin{aligned} f(\alpha(m_i)_{i\in I}) &= f((\alpha m_i)_{i\in I}) && \text{- definição de multiplicação por escalar de } \sum_{i\in I} M_i \\ &= \alpha m_1 + \cdots + \alpha m_n && \text{- definição de } f \\ &= \alpha(m_1 + \cdots + m_n) && \text{- pois } \oplus_{i\in I} M_i \text{ é um } A\text{-módulo} \\ &= \alpha f((m_i)_{i\in I}) && \text{- definição de } f \end{aligned}$$

De (i) e (ii) segue que f é um A-homomorfismo.

- f é um A-epimorfismo, pois

  Dado $m \in \oplus_{i\in I} M_i$, então $m = m_1 + m_2 + \cdots + m_n$, consideremos

  $(m_1, m_2, \ldots, m_n) \in \sum_{i\in I} M_i$, aplicando a f, temos

$$f(m_1, m_2, \ldots, m_n) = m_1 + m_2 + \cdots + m_n \Rightarrow f(m_1, m_2, \ldots, m_n) = m.$$

Determinemos $ker(f)$.

$$ker(f) = \left\{ (m_1, m_2, \ldots, m_n) \in \sum_{i \in I} M_i \mid f(m_1, m_2, \ldots, m_n) = 0 \right\}.$$

Agora,

$$f(m_1, m_2, \ldots, m_n) = 0 \Rightarrow m_1 + m_2 + \cdots + m_n = 0 \Rightarrow \sum_{i=1}^{n} m_i = 0.$$

Como a família $\{M_i\}_{i \in I}$ é independente, segue que

$$m_i = 0, \ \forall \ i \in I.$$

Assim, temos

$$ker(f) = \{(0, 0, \ldots, 0)\}.$$

Logo, f é um A-monomorfismo. □

Proposição 4.10. *Sejam $\{M_i\}_{i \in I}$ uma família de A-módulos, $\left\{ i_k : M_k \longrightarrow \sum_{i \in I} M_i \right\}_{k \in I}$ as inclusões naturais e $M'_k = i_k(M_k)$. Então, $M_k \simeq M'_k$, $\forall \ k \in I$ e $\sum_{i \in I} M_i = \oplus_{i \in I} M'_i$.*

Demonstração:

- Mostraremos que $M_k \simeq M'_k$, $\forall \ k \in I$.
  De fato, como as inclusões naturais $\{i_k : M_k \longrightarrow \sum_{i \in I} M_i\}_{k \in I}$ são A-monomorfismo, pelo teorema do homomorfismo para módulos, temos

  $$M_k / ker(i_k) \simeq Im(i_k).$$

  Como $ker(i_k) = \{0\}$ e a $Im(i_k) = M'_k$, tem-se

  $$M_k \simeq M_k / \{0\} \simeq M'_k.$$

  Portanto,

  $$M_k \simeq M'_k.$$

- Mostraremos que $\sum_{i \in I} M_i = \oplus_{i \in I} M'_i$.

  (i) $\sum_{i \in I} M_i = M'_1 + M'_2 + \cdots + M'_n$.

Seja $m \in \sum_{i\in I} M_i$, então $m = (m_1, m_2, \ldots, m_n)$, assim podemos escrever m da seguinte forma

$$\begin{aligned} m &= (m_1, 0, \ldots, 0) + (0, m_2, \ldots, 0) + \cdots + (0, 0, \ldots, m_n) \\ &= i_1(m_1) + i_2(m_2) + \cdots + i_k(m_k) \\ &= m'_1 + m'_2 + \cdots + m'_n \in i_1(M_1) + i_2(M_2) + \cdots + i_n(M_n) \end{aligned}$$

Portanto, $m \in M'_1 + M'_2 + \cdots + M'_n$.

(ii) A família $\{M'_i\}_{i\in I}$ é independente.

Seja $(x_1, \ldots, x_n) \in (M'_i \cap M'_1 + \cdots + M'_{i-1} + M'_{i+1} + \cdots + M'_n)$, então $(x_1, \ldots, x_n) \in M'_i$, logo $x_j = 0,\ \forall\ j \neq i$ e também $(x_1, \ldots, x_n) \in (M'_1 + \cdots + M'_{i-1} + M'_{i+1} + \cdots + M'_n)$, assim

$$\begin{aligned} (x_1, \ldots, x_n) &= (x_1, \ldots, 0) + \cdots + (0, \ldots, x_{i-1}, \ldots, 0) + (0, \ldots, x_{i+1}, \ldots, 0) + \cdots + (0, \ldots, x_n) \\ &= (x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \end{aligned}$$

Igualando $(x_1, \ldots, x_n)$, obtemos

$$(0, \ldots, 0, x_i, 0, \ldots, 0) = (x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n).$$

Portanto, pela igualdade de n-uplas, segue que

$$x_i = 0,\ \forall\ i \in I.$$

Logo, $M'_i \cap M'_1 + \cdots + M'_{i-1} + M'_{i+1} + \cdots + M'_n) = \{(0, \cdots, 0, \cdots, 0)\}$. Então a família $\{M'_i\}_{i\in I}$ é independente.

Assim segue de (i) e (ii) que $\sum_{i\in I} M_i = \oplus_{i\in I} M'_i$. □

Por causa da correspondência entre somas internas e externas, é frequente usarmos o símbolo $\oplus$ para ambas.

Definição 4.5. *Seja N um submódulo de um A-módulo M. Dizemos que um submódulo N_1 de M é um suplementar de N se $M = N \oplus N_1$.*

Definição 4.6. *Um submódulo, que admite um suplementar é chamado somando direto de M.*

Observação 4.2. Mostra-se que todo subespaço vetorial é um somando direto, no entanto, isto não é sempre verdade para módulos. Por exemplo, consideremos $\mathbb{Z}$ como $\mathbb{Z}$-módulo, ${}_{\mathbb{Z}}\,\mathbb{Z}$ não tem somandos diretos não triviais.

Pois, suponhamos que $m\mathbb{Z}$ seja um somando não trivial de ${}_{\mathbb{Z}}\,\mathbb{Z}$. Então existe, $n\mathbb{Z}$ tal que $\mathbb{Z} = m\mathbb{Z} \oplus n\mathbb{Z}$ com $m, n \notin \{0, \pm 1\}$. Mas $m \cdot n \in m\mathbb{Z} \cap n\mathbb{Z} = \{0\}$, por $m\mathbb{Z}, n\mathbb{Z}$ serem independente. Segue que $m \cdot n = 0$, isto é um absurdo, pois $m, n \neq 0$.

Observação 4.3. Se N é um somando direto de um A-módulo M, o seu suplementar não é, em geral, único.

De fato, consideremos o $\mathbb{R}$-módulo $\mathbb{R}^2$ e o submódulo $N = \{(x, 0) \mid x \in \mathbb{R}\}$. Qualquer submódulo da forma $P = \{(x, mx) \mid x \in \mathbb{R}, m \neq 0\}$ é um suplementar de N, pois podemos escrever todo par $(x, y) \in \mathbb{R}^2$ da seguinte forma:

$$(x, y) = \left(x - \frac{y}{m}, 0\right) + \left(\frac{y}{m}, y\right) \in N + P.$$

Logo, para cada $m \neq 0$, temos que existe um submódulo P que é um suplementar de N, então o suplementar de N não é único.

Proposição 4.11. *Seja M um A-módulo, N_1 e N_2 submódulos de M, tais que $M = N_1 \oplus N_2$. Então,*

$$M/N_1 \simeq N_2.$$

Demonstração:

Definamos $f : M \longrightarrow N_2$ da seguinte forma: dado $m \in M$, podemos escrever, de forma única, como $m = n_1 + n_2$ com $n_1 \in N_1$ e $n_2 \in N_2$. logo $f(m) = f(n_1 + n_2) = n_2$. Mostraremos que f é um A-homomorfismo.

Sejam $m = (n_1 + n_2), m' = (n_1' + n_2') \in M$ e $a \in A$. Então
(i) $f(m + m') = f(m) + f(m')$.

$$\begin{aligned}
f(m + m') &= f[(n_1 + n_2) + (n_1' + n_2')] && \text{- substituição dos valores de } m \text{ e } m' \\
&= f((n_1 + n_1') + (n_2 + n_2')) && \text{- pela associatividade e comutatividade em } M \\
&= n_2 + n_2' && \text{- definição de } f \\
&= f(n_1 + n_2) + f(n_1' + n_2') && \text{- definição de } f \\
&= f(m) + f(m')
\end{aligned}$$

(ii) $f(\alpha m) = \alpha f(m)$.

$$\begin{aligned} f(\alpha m) &= f(\alpha(n_1 + n_2)) && \text{- substituição de } m \\ &= f(\alpha n_1 + \alpha n_2) && \text{- pois } M \text{ é um } A\text{-módulo} \\ &= \alpha n_2 && \text{- definição de } f \\ &= \alpha f(n_1 + n_2) && \text{- definição de } f \\ &= \alpha f(m) \end{aligned}$$

Logo, f é um A-homomorfismo e usando o teorema do A-homomorfismo para módulos temos,

$$M/ker(f) \simeq Im(f).$$

Como,

$$\begin{aligned} ker(f) &= \{m \in M \mid f(m) = 0\} \\ &= \{n_1 + n_2 \in M \mid f(n_1 + n_2) = 0\} \\ &= \{n_1 + n_2 \in M \mid n_2 = 0\} \\ &= \{n_1 \in M \mid n_1 \in N_1\} \\ &= N_1 \end{aligned}$$

e

$$\begin{aligned} Im(f) &= \{f(m) \mid m \in M\} \\ &= \{f(n_1 + n_2) \mid n_1 \in N_1 \text{ e } n_2 \in N_2\} \\ &= \{n_2 \mid n_2 \in N_2\} \\ &= N_2 \end{aligned}$$

Logo, fazendo as devidas substituições, temos que

$$M/N_1 \simeq N_2.$$

□

Corolário 4.1. *Dois suplementares de um mesmo submódulo são isomorfos.*

Demonstração:

Sejam P e Q dois suplementares de um submódulo N de um A-módulo M, então

$$M = N \oplus P \text{ e } M = N \oplus Q.$$

Pela Proposição 4.11, temos que

$$P \simeq M/N \text{ e } M/N \simeq Q.$$

Por transitividade, segue

$$P \simeq Q.$$

□

4.4 Projeção

Nesta seção fazemos um estudo de projeções de módulos e a utilizaremos como uma ferramenta na decomposição do módulo em soma direta interna.

Definição 4.7. *Seja M um A-módulo. Um A-homomorfismo $p : M \longrightarrow M$ chama-se uma projeção (ou projetor) de M se $p^2 = p$.*

Observação 4.4. Se $p : M \longrightarrow M$ é uma projeção, então
(i) $Im(p) = \{m \in M \mid p(m) = m\}$;
(ii) $ker(p) = Im(Id_M - p)$, onde Id_M é o operador identidade.

De fato, se

$$m \in Im(p) \Rightarrow m = p(m'), m' \in M \Rightarrow p(m) = p^2(m') \Rightarrow p(m) = p(m') \Rightarrow p(m) = m.$$

Então, $Im(p) = \{m \in M \mid p(m) = m\}$.

Agora, $ker(p) = Im(Id_M - p)$, pois se

$$m \in Im(Id_M - p) \Leftrightarrow m = (Id_M - p)(m'), m' \in M \Leftrightarrow m = m' - p(m') \Leftrightarrow$$

$$p(m) = p(m' - p(m')) \Leftrightarrow p(m) = p(m') - p^2(m') \Leftrightarrow p(m) = 0 \Leftrightarrow m \in ker(p).$$

Seja $M = \oplus_{i \in I} M_i$ uma decomposição de M em soma direta interna de seus submódulos $\{M_i\}_{i \in I}$. Podemos definir uma família de projetores $\{p_k : M \longrightarrow M\}_{k \in I}$ da seguinte forma: dado $m \in M$, escrevemos m de modo único da seguinte forma $m = \sum_{i \in I} m_i$, com $m_i \in M_i, \forall\, i \in I$ e assim definamos

$$p_k : M \longrightarrow M$$

$$m \longrightarrow p_k(m) = m_k.$$

Vamos mostrar que p_k definida desta forma é de fato um projetor.

Com efeito, seja $m \in M$, para cada $k \in I$, temos

$$\begin{aligned} p_k^2(m) &= p_k(p_k(m)) && \text{- definição de composta} \\ &= p_k(m_k) && \text{- definição de } p_k \\ &= m_k && \text{- definição de } p_k \\ &= p_k(m) && \text{- definição de } p_k \end{aligned}$$

Definição 4.8. *A família de projetores definida acima chama-se associada à decomposição em soma direta dada.*

Definição 4.9. *Seja $\{p_i\}_{i\in I}$ uma família de projetores de um A-módulo M. Dizemos que a família é ortogonal se, para todo par de índices $h, k \in I$, com $h \neq k$ tem-se que $p_h \circ p_k = 0$.*

Proposição 4.12. *Seja M um A-módulo, $M = \oplus_{i\in I} M_i$ uma decomposição de M em soma direta e $\{p_i\}_{i\in I}$ a família de projeções associada a esta decomposição, então esta família possui as seguintes propriedades:*
(i) *A família $\{p_i\}_{i\in I}$ é ortogonal;*
(ii) $\sum_{i\in I} p_i = Id_M$;
(iii) $Im(p_i) = M_i,\ \forall\ i \in I$.
Reciprocamente, se $\{p_i\}_{i\in I}$ é uma família de projetores verificando as condições (i) e (ii) então

$$M = \oplus_{i\in I} Im(p_i).$$

Demonstração:

(i) Sejam p_k e $p_j \in \{p_i\}_{i\in I}$ com $k \neq j$ e $m = \sum_{i=1}^{n} m_i \in M$, então

$$\begin{aligned} (p_k \circ p_j)(m) &= p_k(p_j(m)) && \text{- definição de composta} \\ &= p_k(m_j) && \text{- definição de } p_j \\ &= p_k(0 + \cdots + 0 + m_j + \cdots + 0) \\ &= 0 && \text{- definição de } p_k \end{aligned}$$

Logo, $\{p_i\}_{i\in I}$ é ortogonal.

(ii) Para todo $m \in M$, temos

$$\begin{aligned} Id_M(m) &= m && \text{- definição de } Id_M \\ &= \sum_{i=1}^{n} m_i && \text{- pois } M = \oplus_{i\in I} M_i \\ &= \sum_{i=1}^{n} p_i(m) && \text{- definição de } p_i \\ &= \left(\sum_{i=1}^{n} p_i\right)(m) && \text{- pois } p_i \text{ é um } A\text{-homomorfismo} \end{aligned}$$

Portanto, $Id_M = \sum_{i=1}^{n} p_i$.

(iii) Seja $m \in M$, então

$$\begin{aligned} Im(p_i) &= \{p_i(m) \mid m \in M\} \\ &= \{m_i \mid m_i \in M_i\} \\ &= M_i \end{aligned}$$

Portanto, $Im(p_i) = M_i$.

Reciprocamente, vamos mostrar que se $\{p_i\}_{i\in I}$ é uma família de projetores verificando (i) e (ii), então

$$M = \oplus_{i\in I} Im(p_i).$$

(a) Mostraremos que $M = Im(p_1) + Im(p_2) + \cdots + Im(p_n)$.

Com efeito, seja $m \in M$, pelo item (ii), temos que

$$\begin{aligned} m &= Id_M(m) = \left(\sum_{i=1}^{n} p_i\right)(m) \\ &= (p_1 + p_2 + \cdots + p_n)(m) \\ &= p_1(m) + p_2(m) + \cdots + p_n(m) && \text{- definição de soma de função} \end{aligned}$$

Como $p_i(m) \in Im(p_i),\ \forall i \in I$.

Então temos que $M = Im(p_1) + Im(p_2) + \cdots + Im(p_n)$.

(b) Mostraremos que a família $\{Im(p_i)\}_{i\in I}$ é independente.

Suponhamos $\sum_{i=1}^{n} p_i(m) = 0$, vamos mostrar que $p_i(m) = 0, \forall i \in I$.

De fato,

$$\sum_{i=1}^{n} p_i(m) = 0 \Rightarrow p_1(m) + p_2(m) + \cdots + p_n(m) = 0.$$

aplicando p_i na igualdade, temos

$$p_i(p_1(m) + p_2(m) + \cdots + p_n(m)) = p_i(0).$$

$$(p_i \circ p_1)(m) + (p_i \circ p_2)(m) + \cdots + (p_i \circ p_i)(m) + \cdots + (p_i \circ p_n)(m) = 0.$$

Como $\{p_i\}_{i\in I}$ são projeções e também ortogonal segue

$$p_i(m) = 0, \ \forall i \in I.$$

□

Corolário 4.2. *Se $p : M \longrightarrow M$ é uma projeção, então*

$$M = Im(p) \oplus Ker(p).$$

Demonstração:

Vamos mostrar que

(i) $M = Im(p) + ker(p)$.

Inicialmente observamos que $\forall\ m \in M$, tem-se

$$\begin{aligned} p(m - p(m)) &= p(m) - p^2(m) && \text{- pois } p \text{ é um } A\text{-homomorfismo} \\ &= p(m) - p(m) && \text{- pois } p \text{ é projeção} \\ &= 0 \end{aligned}$$

Logo, $m - p(m) \in ker(p)$.

Como $\forall\ m \in M$,

$$m = p(m) + (m - p(m)) \in Im(p) + ker(p).$$

Seque que $M = Im(p) + ker(p)$.

(ii) $Im(p) \cap ker(p) = \{0\}$.

Se $m \in Im(p) \cap ker(p)$, então para algum $m' \in M$ temos

$$p(m') = m \Rightarrow p^2(m') = p(m) \Rightarrow p(m') = 0 \Rightarrow m = 0.$$

Portanto, $Im(p) \cap ker(p) = \{0\}$.

Segue de (i) e (ii) que $M = Im(p) \oplus ker(p)$. □

Os resultados anteriores nos mostram que o problema de determinar somandos diretos de um módulo é equivalente a determinar projetores. Vamos usar este fato para determinar, dado um anel A, os somandos diretos do A-módulo ${}_AA$.

Definição 4.10. *Um elemento e de um anel A chama-se idempotente se $e^2 = e$.*

Exemplo 4.3. Para todo anel A, o elemento neutro 0 é um idempotente. Se A for um anel com elemento unidade, então $1^2 = 1$, logo 1 é um idempotente não nulo.

Exemplo 4.4. Seja A um domínio de integridade, se $e \in A$ é um idempotente de A, então

$$e^2 = e \Rightarrow e^2 - e = 0 \Rightarrow e(e-1) = 0$$

e como A é um anel de integridade segue que $e = 0$ ou $e = 1$. Assim os únicos idempotentes de um anel de integridade são 0 e 1.

Exemplo 4.5. Se e é um idempotente de um anel, a aplicação $Re : A \longrightarrow A$ definida por $Re(a) = ae$ é uma projeção de A.

De fato, seja $a \in A$, temos

$$\begin{aligned}
Re^2(a) &= Re(Re(a)) && \text{- definição de composta} \\
&= Re(ae) && \text{- definição de } Re \\
&= (ae)e && \text{- definição de } Re \\
&= a(ee) && \text{- associatividade de } A \\
&= ae && \text{- pois } e \text{ é um idempotente} \\
&= Re(a) && \text{- definição de } Re
\end{aligned}$$

Assim, Re é uma projeção.

Proposição 4.13. *Existe uma correspondência bijetora entre os projetores do A-módulo ${}_AA$ e os idempotentes do anel A.*

Demonstração:

Consideremos:

$X = \{p :_A A :\longrightarrow_A A \mid p^2 = p\}$ − o conjunto dos projetores do A-módulo A

$Y = \{0 \neq e \in A \mid e^2 = e\}$ − o conjunto dos idempotentes não nulos de A

Definamos as aplicações

(i) $f : X \longrightarrow Y$, definida por $f(p) = p(1)$. f está bem definida pois chamando $e = p(1)$ temos

$$e = p(1) = p^2(1) = p(p(1)) = p(e) = p(e1) = ep(1) = e^2.$$

Logo, $p(1) \in Y$.

(ii) $g : Y \longrightarrow X$ definida por $g(e) = Re$, onde $Re(a) = ae$, $\forall\ a \in A$. g está bem definida conforme mostramos no Exemplo 4.5.

Agora, para todo $e \in Y$ e $p \in X$, tem-se

$$\begin{aligned}
(f \circ g)(e) &= f(g(e)) && \text{- definição de composta}\\
&= f(Re) && \text{- definição de } g\\
&= Re(1) && \text{- definição de } f\\
&= 1e && \text{- definição de } Re\\
&= e\\
&= Id_Y(e)
\end{aligned}$$

e

$$\begin{aligned}
(g \circ f)(p) &= g(f(p)) && \text{- definição de composta}\\
&= g(p(1)) && \text{- definição de } f\\
&= R_{p(1)} && \text{- definição de } g\\
&= p
\end{aligned}$$

Pois, $\forall\ a \in A$, $R_{p(1)}(a) = ap(1) = p(a1) = p(a)$. Assim,

$$(g \circ f)(p) = p \Rightarrow (g \circ f)(p) = Id_X(p).$$

Logo, $f \circ g = Id_Y$ e $g \circ f = Id_X$. Então f é uma bijeção entre X e Y. □

Corolário 4.3. *Se $e \in A$ é um idempotente temos*

$$_AA = Ae \oplus A(1 - e).$$

Demonstração:

Como $Re : A \longrightarrow A$ é uma projeção pelo Corolário 4.2 temos

$$_AA = Im(Re) \oplus ker(Re).$$

Segue da Observação 4.4 que

$$_AA = Im(Re) \oplus Im(Id_M - Re).$$

Como

$$\begin{aligned} Im(Re) &= \{Re(a) \mid a \in A\} \\ &= \{ae \mid a \in A\} \\ &= Ae \end{aligned}$$

e

$$\begin{aligned} Im(Id_M - Re) &= \{(Id_M - Re)(a) \mid a \in A\} \\ &= \{a - Re(a) \mid a \in A\} \\ &= \{a - ae \mid a \in A\} \\ &= \{a(1-e) \mid a \in A\} \\ &= A(1-e) \end{aligned}$$

Portanto, fazendo as devidas substituições, temos

$$_AA = Ae \oplus A(1-e).$$

□

Corolário 4.4. *Se A é um domínio de integridade, os únicos somandos diretos de $_AA$ são $\{0\}$ e o próprio $_AA$.*

Demonstração:

Já observamos que os únicos idempotentes de um domínio de integridade são 0 e 1, assim pelo Corolário 4.2 temos

- Se $e = 0$, então

$$_AA = A \cdot 0 \oplus A \cdot (1-0) \Rightarrow_A A = A \cdot 0 \oplus A \cdot 1 \Rightarrow_A A = \{0\} \oplus A.$$

- Se $e = 1$, então

$$_AA = A \cdot 1 \oplus A \cdot (1-1) \Rightarrow_A A = A \cdot 1 \oplus A \cdot 0 \Rightarrow_A A = A \oplus \{0\}.$$

Assim, em qualquer caso os únicos somandos diretos de $_AA$ são $\{0\}$ e A. □

Corolário 4.5. *Seja A um anel. Então, todo somando direto de $_AA$ é um ideal principal de A.*

Demonstração:

Seja N_1 um somando direto de $_AA$, logo existe um submódulo N_2, tal que

$$A = N_1 \oplus N_2.$$

Seja $\{p_1, p_2\}$ a família de projetores associada a esta decomposição. Pela Proposição 4.13 $e = p(1)$ é um idempotente de A, logo pelo Corolário 4.3, temos

$$_AA = Ae \oplus A(1-e).$$

onde

$$\begin{aligned} Ae &= \{ae \mid a \in A\} \\ &= \{ap_1(1) \mid a \in A\} \\ &= \{p_1(a1) \mid a \in A\} \\ &= \{p_1(a) \mid a \in A\} \\ &= Im(p_1) \\ &= N_1 \end{aligned}$$

Logo, $N_1 = Ae$ é ideal principal de A. □

Capítulo 5

Módulos Livres

Neste capítulo trataremos de módulos livres, isto é, veremos quando um módulo é chamado de livre, mas antes disso, daremos uma noção de sequência cindida, depois faremos comparações entre algumas propriedades de espaço vetorial e de módulo, apresentando vários exemplos, em que o último se difere do primeiro.

5.1 Soma Direta e Sequência Exata

Estudaremos agora algumas relações entre somas diretas e sequência exatas.

Suponhamos que $M = M_1 \oplus M_2$. Então a sequência abaixo

$$0 \longrightarrow M_1 \xrightarrow{i_1} M_1 \oplus M_2 \xrightarrow{p_2} M_2 \longrightarrow 0$$

é exata.

De fato, temos que i_1 é um monomorfismo, logo a sequência é exata em M_1. E como p_2 é um epimorfismo, a sequência é exata em M_2. Resta mostrarmos que ela é exata em $M_1 \oplus M_2$. Como,

$$\begin{aligned} Im(i_1) &= \{i_1(m_1) \mid m_1 \in M_1\} \\ &= \{(m_1, 0) \mid m_1 \in M_1\} \\ &= \{m_1 + 0 \mid m_1 \in M_1\} \text{ - por causa do isomorfismo } \oplus_{i=1}^{n} M_i \simeq \sum_{i=1}^{n} M_i. \\ &= \{m_1 \mid m_1 \in M_1\} \\ &= M_1 \end{aligned}$$

e

$$\begin{aligned} ker(p_2) &= \{m_1 + m_2 \in M_1 \oplus M_2 \mid p_2(m_1 + m_2) = 0\} \\ &= \{m_1 + m_2 \in M_1 \oplus M_2 \mid m_2 = 0\} \\ &= \{m_1 \mid m_1 \in M_1\} \\ &= M_1 \end{aligned}$$

Portanto, $Im(i_1) = ker(p_2)$, logo a sequência é exata em $M_1 \oplus M_2$.

É natural nos perguntarmos, quando uma sequência

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

é tal que

$$F \simeq E \oplus G.$$

Para respondermos, vejamos a seguinte definição.

Definição 5.1. *Dizemos que uma sequência exata de A-módulos*

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

cinde se $E' = Im(f) = ker(g)$ é um somando direto de F.

Proposição 5.1. *Dada uma sequência exata de A-módulos*

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

as seguintes afirmações são equivalentes:
(i) *A sequência cinde;*
(ii) *Existe um A-homomorfismo $\psi : F \longrightarrow E$ tal que $\psi \circ f = Id_E$;*
(iii) *Existe um A-homomorfismo $\varphi : G \longrightarrow F$ tal que $g \circ \varphi = Id_G$;*
Nestas condições $F \simeq E \oplus G$.

Demonstração:

$(i) \Rightarrow (ii)$ Se a sequência cinde, então existe um A-homomorfismo $\psi : F \longrightarrow E$ tal que $\psi \circ f = Id_E$.

De fato, escrevendo $E' = Im(f)$ e como a sequência cinde, então existe um submódulo E'' de F tal que $F = E' \oplus E''$.

Assim, dado $m \in F$, escrevemos $m = m' + m''$ com $m' \in E'$ e $m'' \in E''$, como f é injetora, pois a sequência é exata, existe um único $y \in E$ tal que $f(y) = m'$, então

$$m = m' + m'' \Rightarrow m = f(y) + m''.$$

Assim definamos ψ da seguinte forma:

$$\psi : F \longrightarrow E$$

$$m \longrightarrow \psi(f(y) + m'') = y.$$

- Mostraremos que ψ é um A-homomorfismo.

  Sejam $m_1 = f(y_1) + m_1'', m_2 = f(y_2) + m_2'' \in F$ e $a \in A$. Então,

  (i) $\psi(m_1 + m_2) = \psi(m_1) + \psi(m_2)$.

$$\begin{aligned}
\psi(m_1 + m_2) &= \psi[(f(y_1) + m_1'') + (f(y_2) + m_2'')] \\
&= \psi[(f(y_1) + f(y_2)) + (m_1'' + m_2'')] && \text{- definição de soma de submódulo} \\
&= \psi[(f(y_1 + y_2)) + (m_1'' + m_2'')] && \text{- pois } f \text{ é um } A\text{-homomorfismo} \\
&= y_1 + y_2 && \text{- definição de } \psi \\
&= \psi(f(y_1) + m_1'') + \psi(f(y_2) + m_2'') && \text{- definição de } \psi \\
&= \psi(m_1) + \psi(m_2) && \text{- substituição de } m_1 \text{ e } m_2
\end{aligned}$$

  (ii) $\psi(am_1) = a\psi(m_1)$.

$$\begin{aligned}
\psi(am_1) &= \psi(a(f(y_1) + m_1'')) && \text{- substituição de } m_1 \\
&= \psi(af(y_1) + am_1'') && \text{- pois } F \text{ é um } A\text{-módulo} \\
&= \psi(f(ay_1) + am_1'') && \text{- pois } f \text{ é um } A\text{-homomorfismo} \\
&= ay_1 && \text{- definição de } \psi \\
&= a\psi(f(y_1) + m_1'') && \text{- definição de } \psi \\
&= a\psi(m_1) && \text{- substituição de } m_1
\end{aligned}$$

  Portanto, segue de (i) e (ii) que ψ é um A-homomorfismo.

- Vamos mostrar que $\psi \circ f = Id_E$.

  Seja $y \in E$, então $f(y) \in E'$, logo

$$\begin{aligned}(\psi \circ f)(y) &= \psi(f(y)) && \text{- definição de composta}\\ &= \psi(f(y)+0)\\ &= y && \text{- definição da } \psi\\ &= Id_E(y) && \text{- definição da } Id_E\end{aligned}$$

  Logo, $\psi \circ f = Id_E$.

$(ii) \Rightarrow (i)$ Existe um A-homomorfismo $\psi : F \longrightarrow E$ tal que $\psi \circ f = Id_E$, então a sequência $0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G \longrightarrow 0$ cinde.

Mostraremos que $F = Im(f) \oplus ker(\psi)$.

(a) $F = Im(f) + ker(\psi)$.

Seja $m \in F$, temos $\psi(m) \in E$, então $f(\psi(m)) \in Im(f)$.

Assim, $(m - f(\psi(m))) \in F$, aplicando a ψ neste elemento, obtemos

$$\begin{aligned}\psi(m - f(\psi(m))) &= \psi(m) - \psi(f(\psi(m))) && \text{- pois } \psi \text{ é um } A\text{-homomorfismo}\\ &= \psi(m) - (\psi \circ f)(\psi(m)) && \text{- definição de composta}\\ &= \psi(m) - Id_E(\psi(m)) && \text{- pois } \psi \circ f = Id_E\\ &= \psi(m) - \psi(m) && \text{- definição da } Id_E\\ &= 0\end{aligned}$$

Portanto, $(m - f(\psi(m))) \in ker(\psi)$.

Logo, podemos escrever

$$m = f(\psi(m)) + (m - f(\psi(m))) \in Im(f) + ker(\psi).$$

Portanto,

$$F = Im(f) + ker(\psi).$$

(b) A família $\{Im(f), ker(\psi)\}$ é independente.

Seja $y \in Im(f) \cap ker(\psi)$, então $y \in Im(f) \cap ker(\psi)$, logo existe $x \in E$ tal que $f(x) = y$ e também

$$\psi(y) = 0 \Rightarrow \psi(f(x)) = 0 \Rightarrow (\psi \circ f)(x) = 0 \Rightarrow Id_E(x) = 0 \Rightarrow x = 0.$$

Logo,

$$y = f(x) \Rightarrow y = f(0) \Rightarrow y = 0.$$

Portanto, a família $\{Im(f), ker(\psi)\}$ é independente.

Assim, segue de (a) e (b) que $F = Im(f) \oplus Ker(\psi)$.

$(i) \Rightarrow (iii)$ Se a sequência cinde, então existe um A-homomorfismo $\varphi : G \longrightarrow F$ tal que $g \circ \varphi = Id_G$.

De fato, escrevendo $E' = ker(g)$ e como a sequência cinde, então existe um submódulo E'' de F tal que $F = E' \oplus E''$.

Assim, dado $y \in G$, como g é sobrejetora, pois a sequência é exata, então existe $x \in F$ tal que $g(x) = y$. Também, tem-se que x se escreve de modo único como $x = x' + x''$, com $x' \in E'$ e $x'' \in E''$. Daí,

$$\begin{aligned}
y &= g(x) \\
&= g(x' + x'') && \text{- pois } x = x' + x'' \\
&= g(x') + g(x'') && \text{- pois } g \text{ é um } A\text{-homomorfismo} \\
&= 0 + g(x'') && \text{- pois } x' \in E' = ker(g) \\
&= g(x'')
\end{aligned}$$

Então, definamos φ da seguinte forma:

$$\varphi : G \longrightarrow F$$

$$y \longrightarrow \varphi(g(x'')) = x''.$$

Vamos mostrar que φ é um A-homomorfismo.

Sejam $y_1, y_2 \in G$, então existem $x_1'', x_2'' \in F$ tal que $y_1 = g(x_1'')$ e $y_2 = g(x_2'')$ e $a \in A$. Então,
(a) $\varphi(y_1 + y_2) = \varphi(y_1) + \varphi(y_2)$.

$$\begin{aligned}
\varphi(y_1 + y_2) &= \varphi(g(x_1'') + g(x_2'')) && \text{- substituindo } y_1 = g(x_1'') \text{ e } y_2 = g(x_2'') \\
&= \varphi(g(x_1'' + x_2'')) && \text{- pois } g \text{ é um } A\text{-homomorfismo} \\
&= x_1'' + x_2'' && \text{- definição da } \varphi \\
&= \varphi(g(x_1'')) + \varphi(g(x_2'')) && \text{- definição da } \varphi \\
&= \varphi(y_1) + \varphi(y_2) && \text{- substituindo } y_1 = g(x_1'') \text{ e } y_2 = g(x_2'')
\end{aligned}$$

(b) $\varphi(ay_1) = a\varphi(y_1)$.

$$\begin{aligned}
\varphi(ay_1) &= \varphi(ag(x_1'')) && \text{- substituição de } y_1 = g(x_1'') \\
&= \varphi(g(ax_1'')) && \text{- pois } g \text{ é um } A\text{-homomorfismo} \\
&= ax_1'' && \text{- definição de } \varphi \\
&= a\varphi(g(x_1'')) && \text{- definição de } \varphi \\
&= a\varphi(y_1) && \text{- pois } y_1 = g(x_1'')
\end{aligned}$$

Portanto, segue de (a) e (b) que φ é um A-homomorfismo.

Mostraremos que $g \circ \varphi = Id_G$.
Seja $y \in G$, então existe $x'' \in F$ tal que $g(x'') = y$. Assim

$$\begin{aligned}
(g \circ \varphi)(y) &= g(\varphi(y)) && \text{- definição de composta} \\
&= g(\varphi(g(x''))) && \text{- substituição de } y = g(x'') \\
&= g(x'') && \text{- definição de } \varphi \\
&= y && \text{- definição de } g \\
&= Id_G(y) && \text{- definição de } Id_G
\end{aligned}$$

Logo, $g \circ \varphi = Id_G$.

$(iii) \Rightarrow (i)$ Se existe um A-homomorfismo $\varphi : G \to F$ tal que $g \circ \varphi = Id_G$, então a sequência é cinde. Vamos mostrar que $F = ker(g) \oplus Im(\varphi)$. Para isto, mostraremos que:

(a) $F = ker(g) + Im(\varphi)$.

De fato, seja $m \in F$, então $g(m) \in G$, logo $\varphi(g(m)) \in Im(\varphi)$. Assim, $(m - \varphi(g(m))) \in F$. Aplicando a g neste elemento, obtemos

$$\begin{aligned}
g(m - \varphi(g(m))) &= g(m) - g(\varphi(g(m))) && \text{- pois } g \text{ é um } A\text{-homomorfismo} \\
&= g(m) - (g \circ \varphi)(g(m)) && \text{- definição de composta} \\
&= g(m) - Id_G(g(m)) && \text{- pois } g \circ \varphi = Id_G \\
&= g(m) - g(m) && \text{- definição de } Id_G \\
&= 0
\end{aligned}$$

Portanto, $(m - \varphi(g(m))) \in ker(g)$.

Logo, podemos escrever

$$m = \varphi(g(m)) + (m - \varphi(g(m))) \in Im(\varphi) + ker(g).$$

Portanto, $F = ker(g) + Im(\varphi)$.

(ii) A família $\{Im(\varphi), ker(g)\}$ é independente.

Seja $y \in Im(\varphi) \cap ker(g)$, então $y \in Im(\varphi)$ e $y \in ker(g)$. Assim,

$y \in Im(\varphi) \Rightarrow \exists\, m \in G$ tal que $\varphi(m) = y$ e como $y \in ker(g)$, temos

$$g(y) = 0 \Rightarrow g(\varphi(m)) = 0 \Rightarrow (g \circ \varphi)(m) = 0 \Rightarrow Id_G(m) = 0 \Rightarrow m = 0.$$

Logo,

$$y = \varphi(m) \Rightarrow y = \varphi(0) \Rightarrow y = 0.$$

Portanto, a família $\{Im(\varphi), ker(g)\}$ é independente.

Segue de (a) e (b) que $F = ker(g) \oplus Im(\varphi)$.

Agora, como $\psi \circ f = Id_E$ e $g \circ \varphi = Id_G$, temos que f e φ são injetoras e aplicando o teorema do homomorfismo para módulos temos

$$E \simeq E/ker(f) \simeq Im(f) \text{ e } G \simeq G/ker(\varphi) \simeq Im(\varphi).$$

Portanto,

$$E \simeq Im(f) = ker(g) \text{ e } G \simeq Im(\varphi).$$

Logo,

$$F \simeq E \oplus G, \text{ pois } F = ker(g) \oplus Im(\varphi).$$

□

5.2 Módulos Livres

Sejam A um anel e I um conjunto de índices. Denotaremos por $A^{(I)}$ a soma direta externa $\sum_{i\in I} A_i$, onde $A_i = A, \forall\ i \in I$. Assim, $A^{(I)}$ é o conjunto das famílias quase nulas $(\lambda_i)_{i\in I}$, com $\lambda_i \in A, \forall\ i \in I$.

Definição 5.2. *Seja $\{m_i\}_{i\in I}$ uma família de elementos de um A-módulo M. Dizemos que um elemento $m \in M$ é uma combinação linear dos elementos desta família se existe $(\lambda_i)_{i\in I}$ tal que*

$$m = \sum_{i\in I} \lambda_i m_i.$$

Observamos que esta soma faz sentindo e é finita, pois as famílias $(\lambda_i)_{i\in I}$ são quase nulas.

Definição 5.3. *Dizemos que um subconjunto $S = \{m_i\}_{i\in I}$ de um A-módulo M é um gerador de M se todo elemento de M for uma combinação linear de elementos de S.*

Definição 5.4. *Uma família $\{m_i\}_{i\in I}$ de elementos de um A-módulo M é linearmente independente ou livre se para toda $(\lambda_i)_{i\in I} \in A^{(I)}$, tem-se*

$$\sum_{i\in I} \lambda_i m_i = 0 \Rightarrow \lambda_i = 0,\ \forall\ i \in I.$$

Uma família que não é linearmente independente chama-se linearmente dependente.

Definição 5.5. *Uma família $\{m_i\}_{i\in I}$ de elementos de um A-módulo M é uma base de M se é uma família linearmente independente e gera M.*

Definição 5.6. *Dizemos que um A-módulo M é livre se existe uma base para M.*

Exemplo 5.1. Todo espaço vetorial sobre um corpo K é um K-módulo livre.

De fato, mostra-se que todo espaço vetorial sobre um corpo K possui uma base, logo é um K-módulo livre.

Exemplo 5.2. Se A é um anel comutativo com elemento unidade, então o A-módulo ${}_AA$ é livre e o conjunto $\{1\}$ é uma base. Mas geralmente, $\{u\}$ é base de A, se e somente se, u é um elemento inversível de A.

De fato, sendo $\{u\}$ uma base, então para todo $x \in A$ existe $\lambda \in A$ tal que

$$x = \lambda u.$$

Então, tomando $x = 1$, temos que existe $\lambda_1 \in A$ tal que

$$1 = \lambda_1 u.$$

Logo, u é inversível.

Reciprocamente, se u é um elemento inversível de A, então existe $\lambda \in A$ tal que

$$\lambda u = 1. \tag{5.1}$$

Daí, para todo $x \in A$, temos

$$x = x1. \tag{5.2}$$

Substituindo (5.1) em (5.2), temos

$$x = x(\lambda u) \Rightarrow x = (x\lambda)u.$$

Portanto, $\{u\}$ gera A. E se $a \in A$ é tal que $au = 0$, multiplicando à direita $u' \in A$ temos,

$$(au)u' = 0u' \Rightarrow (au)u' = 0 \Rightarrow a(uu') = 0.$$

Como u é inversível, segue que

$$a1 = 0 \Rightarrow a = 0.$$

Logo, $\{u\}$ é linearmente independente e portanto base de A.

Como consequência, do Exemplo 5.2, temos que as únicas bases do $\mathbb{Z}$-módulo ${}_{\mathbb{Z}}\mathbb{Z}$ são $\{-1\}$ e $\{1\}$, pois estes são os únicos elementos inversíveis de $\mathbb{Z}$.

Observação 5.1. Qualquer subconjunto do A-módulo ${}_AA$ com mais de um elemento é linearmente dependente.

Com efeito, consideremos uma família $X \subseteq_A A$ com mais de um elemento. Tomemos $0 \neq a, b \in X$, com $a \neq b$, assim temos a seguinte combinação linear

$$a \cdot b + (-a) \cdot b = 0.$$

com $(-a), b \in A$ não nulos, logo esta família é linearmente dependente. Então, resulta que as bases do A-módulo ${}_AA$ só podem ser conjuntos unitários, ou seja, da forma $\{u\}$, com $u \in A$.

Exemplo 5.3. Um ideal à esquerda I de um anel A é um A-módulo livre, se e somente se, I é principal e um gerador a de I é tal que $Anl(a) = 0$.

De fato, se I é um A-módulo livre, então existe uma base para I. Se esta base tiver mais de um elemento digamos x_1, x_2 com $x_1 \neq x_2$, temos que

$$x_1(x_2) + x_2(-x_1) = 0.$$

com $x_2, (-x_1) \in I$ não todos nulos, o que é um absurdo, pois x_1 e x_2 pertencem a uma base de I, logo são independentes.

Portanto, uma base para I é da forma $\{a\}$, então $I = (a)$, segue então que I é principal.

Além disso, $Anl(a) = 0$, pois caso contrário, se não fosse existiria um $0 \neq x \in A$ tal que $xa = 0$, e isto é um absurdo, pois $\{a\}$ não seria base.

Reciprocamente, se I é principal e um gerador a de I é tal que $Anl(a) = 0$, então $\{a\}$ é uma base de I.

Com efeito, seja a um gerador de I, então $I = (a)$, logo temos que a gera I, agora como o $Anl(a) = 0$, segue que

$$xa = 0 \Rightarrow x = 0.$$

Logo, a é linearmente independente.

Portanto, $\{a\}$ é uma base de I.

Exemplo 5.4. No $\mathbb{Z}$-módulo $\mathbb{Z} \oplus \mathbb{Z}$, o conjunto $\{e_1, e_2\}$, onde $e_1 = (1, 0)$ e $e_2 = (0, 1)$, é uma base.

Mais geralmente, dado um anel A, consideremos a soma direta $A^{(I)}$. Indicaremos por e_k o elemento $e_k = (x_i)_{i \in I}$ onde $x_k = 1$ e $x_i = 0$, se $i \neq k$. Então a família $\{e_k\}_{k \in I}$ é uma base de $A^{(I)}$, chamada base canônica.

5.3 Módulo $\times$ Espaço Vetorial

A seguir, damos alguns exemplos para mostrar que nem sempre os módulos se comportam como um espaço vetorial e que certas propriedades que intuitivamente podem parecer verdadeiras são, em geral, falsas.

Espaço Vetorial	Módulo
• Todo subconjunto linearmente independente pode ser ampliado a uma base.	• Em geral, isto não é verdade, por exemplo, o $\mathbb{Z}$-módulo ${}_{\mathbb{Z}}\mathbb{Z}$ é livre e temos que o conjunto $\{2\}$ é linearmente independente. No entanto não é base, pois só é base os elementos inversíveis, e nem pode ser ampliado a uma base, pois pela Observação 5.1, todo conjunto com dois ou mais elementos é linearmente dependente.
• Todo conjunto gerador contém uma base.	• Em geral, não é verdade, pois $\{2,3\}$ gera ${}_{\mathbb{Z}}\mathbb{Z}$, porém não contém uma base, pois nenhum elemento de $\{2,3\}$ é uma unidade de $\mathbb{Z}$.
• Um conjunto é linearmente dependente se, e somente se, um dos elementos é combinação linear dos demais.	• Em geral, não é verdade, por exemplo, considerando novamente a família $\{2,3\} \subset {}_{\mathbb{Z}}\mathbb{Z}$, temos que $\{2,3\}$ é linearmente dependente. Porém, não existe nenhum $\alpha \in \mathbb{Z}$ tal que $2 = \alpha \cdot 3$ ou $3 = \alpha \cdot 2$, logo nenhum dos dois é combinação linear do outro.
• Todo espaço vetorial tem base.	• Nem todo submódulo de um módulo livre é livre, pois o $\mathbb{Z}_6$ considerado como módulo sobre si mesmo é livre com base $\{\overline{1}\}$, mas por exemplo, o submódulo $H = \{\overline{0}, \overline{2}, \overline{4}\}$ de $\mathbb{Z}_6$ não é livre, pois não possui nenhuma base, já que todo subconjunto unitário de H é linearmente dependente.
• Seja $W \subsetneq V$ um subespaço de um espaço vetorial V de dimensão finita. Então a cardinalidade de uma base de W é menor que a cardinalidade de uma base de V.	• Seja M um A-módulo livre e $S \subsetneq M$ um submódulo, também livre. Nem sempre é verdade que a cardinalidade de uma base de S é menor que a cardinalidade de uma base de M. pois consideremos o $\mathbb{Z}$-módulo $\mathbb{Z} \oplus \mathbb{Z}$ e o submódulo S gerado pelos elementos $(1,1)$ e $(-1,1)$. Temos que $S \subset \mathbb{Z} \oplus \mathbb{Z}$, pois por exemplo, $e_1 = (1,0), e_2 = (0,1) \notin S$. Agora $\{e_1, e_2\}$ é base de $\mathbb{Z} \oplus \mathbb{Z}$ com cardinalidade 2 e $\{(1,1), (-1,1)\}$ é base de S com a mesma cardinalidade de $\mathbb{Z} \oplus \mathbb{Z}$.

Proposição 5.2. *Sejam M e N A-módulos. Suponhamos M livre com $X = \{x_i\}_{i\in I}$ uma base de M e $f : X \longrightarrow N$ uma função. Então, f pode ser estendida de modo único a um A-homomorfismo $\overline{f} : M \longrightarrow N$ tal que $\overline{f}(x_i) = f(x_i), \forall\, x_i \in X$.*

Demonstração:

Seja

$$f : X \longrightarrow N$$

$$x_i \longrightarrow f(x_i).$$

Como X é base de M, então todo $m \in M$ se escreve de modo único como

$$m = \sum_{i\in I} \lambda_i x_i, \quad \text{com } (\lambda_i)_{i\in I} \in A^{(I)}.$$

Definamos $\overline{f}$ da seguinte forma

$$\overline{f} : M \longrightarrow N$$

$$m \longrightarrow \overline{f}\left(\sum_{i\in I} \lambda_i x_i\right) = \sum_{i\in I} \lambda_i f(x_i).$$

- Mostraremos que $\overline{f}$ é um A-homomorfismo.
  Sejam $m_1, m_2 \in M$, então $m_1 = \sum_{i\in I} \lambda_i x_i$ e $m_2 = \sum_{i\in I} \beta_i x_i$ e $a \in A$.
  Então,

(i) $\overline{f}(m_1 + m_2) = \overline{f}(m_1) + \overline{f}(m_2)$.

$$\begin{aligned}
\overline{f}(m_1 + m_2) &= \overline{f}\left(\sum_{i\in I} \lambda_i x_i + \sum_{i\in I} \beta_i x_i\right) && \text{- substituição de } m_1 \text{ e } m_2 \\
&= \overline{f}\left(\sum_{i\in I} (\lambda_i + \beta_i) x_i\right) && \text{- def. de soma de somatório e } M \text{ é um } A\text{-módulo} \\
&= \sum_{i\in I} (\lambda_i + \beta_i) f(x_i) && \text{- definição de } \overline{f} \\
&= \sum_{i\in I} \lambda_i f(x_i) + \sum_{i\in I} \beta_i f(x_i) && \text{- def. de soma de somatório e } N \text{ é um } A\text{-módulo} \\
&= \overline{f}\left(\sum_{i\in I} \lambda_i x_i\right) + \overline{f}\left(\sum_{i\in I} \beta_i x_i\right) && \text{- definição de } \overline{f} \\
&= \overline{f}(m_1) + \overline{f}(m_2)
\end{aligned}$$

(ii) $\overline{f}(am_1) = a\overline{f}(m_1)$.

$$\begin{aligned}
\overline{f}(am_1) &= \overline{f}\left(a\sum_{i\in I}\lambda_i x_i\right) && \text{- substituição de } m_1\\
&= \overline{f}\left(\sum_{i\in I}(a\lambda_i)x_i\right) && \text{- propriedade de somatório}\\
&= \sum_{i\in I}(a\lambda_i)f(x_i) && \text{- definição de } \overline{f}\\
&= a\left(\sum_{i\in I}\lambda_i f(x_i)\right) && \text{- propriedade de somatório}\\
&= a\overline{f}\left(\sum_{i\in I}\lambda_i x_i\right) && \text{- definição de } \overline{f}\\
&= a\overline{f}(m_1)
\end{aligned}$$

Portanto, segue de (i) e (ii) que $\overline{f}$ é um A-homomorfismo.

- Mostraremos que $\overline{f}(x_i) = f(x_i), \forall\, x_i \in X$.

  De fato, dado $x_i \in X$, temos que $x_i = 1 \cdot x_i$, então aplicando $\overline{f}$ temos

$$\begin{aligned}
\overline{f}(x_i) &= \overline{f}(1 \cdot x_i)\\
&= 1 \cdot f(x_i) && \text{- definição de } \overline{f}\\
&= f(x_i)
\end{aligned}$$

- Mostraremos agora a unicidade de $\overline{f}$.

  Sejam $g : M \longrightarrow N$ um A-homomorfismo tal que $g(x_i) = f(x_i), \forall\, x_i \in X$ e $m = \sum_{i\in I}\lambda_i x_i \in M$, aplicando g em m, temos

$$\begin{aligned}
g(m) &= g\left(\sum_{i\in I}\lambda_i x_i\right)\\
&= \sum_{i\in I}\lambda_i g(x_i) && \text{- pois } g \text{ é um } A\text{-homomorfismo}\\
&= \sum_{i\in I}\lambda_i f(x_i) && \text{- pois } g(x_i) = f(x_i)\\
&= \overline{f}\left(\sum_{i\in I}\lambda_i x_i\right) && \text{- definição de } \overline{f}\\
&= \overline{f}(m)
\end{aligned}$$

  Portanto, $\overline{f}$ é única. □

Corolário 5.1. *Se M é um A-módulo com base $X = \{x_i\}_{i\in I}$, então $M \simeq A^{(I)}$.*

Demonstração:

Seja $y = \{e_k\}_{k\in I}$ a base canônica de $A^{(I)}$ e consideremos a função

$$f : X \longrightarrow A^{(I)}$$

$$x_i \longrightarrow f(x_i) = e_i.$$

Vamos mostrar que a extensão $\overline{f} : M \longrightarrow A^{(I)}$ definida na Proposição 5.2 é um isomorfismo.

(i) $\overline{f}$ é sobrejetora.

Sejam $m = \sum_{i\in I} \lambda_i x_i \in M$ e $a \in A^{(I)}$, como y é base de $A^{(I)}$, então a se escreve de forma única como

$$\begin{aligned} a &= \sum_{i\in I} \lambda_i e_i \\ &= \sum_{i\in I} \lambda_i f(x_i) && \text{- definição de } f \\ &= \overline{f}\left(\sum_{i\in I} \lambda_i x_i\right) && \text{- definição de } \overline{f} \\ &= \overline{f}(m) \end{aligned}$$

Portanto, dado $a \in A^{(I)}$, existe $m = \sum_{i\in I} \lambda_i x_i \in M$ tal que $\overline{f}(m) = a$.

Logo, $\overline{f}$ é sobrejetora.

(ii) $\overline{f}$ é injetora.

Seja $m = \sum_{i\in I} \lambda_i x_i \in M$ tal que $\overline{f}(m) = 0$, mostraremos que $m = 0$.

De fato,

$$\begin{aligned} 0 &= \overline{f}(m) \\ &= \overline{f}\left(\sum_{i\in I} \lambda_i x_i\right) && \text{- substituição de } m \\ &= \sum_{i\in I} \lambda_i f(x_i) && \text{- definição de } \overline{f} \\ &= \sum_{i\in I} \lambda_i e_i && \text{- definição de } f \\ &= \lambda_i,\ \forall\, i \in I && \text{- pois } y \text{ é base e } \{e_k\}_{k\in I} \text{ é L.I} \end{aligned}$$

Portanto, $m = 0$. Logo, $\overline{f}$ é injetora.

Assim,

$$M \simeq A^{(I)}.$$

□

Proposição 5.3. *Se $f : M \longrightarrow N$ é um isomorfismo de A-módulos e M é livre, então N também o é.*

Demonstração:

Seja $f : M \longrightarrow N$ um isomorfismo, como M é livre tem base, seja $X = \{x_i\}_{i \in I}$ uma base de M. Vamos mostrar que $y = \{f(x_i)\}_{i \in I}$ é uma base de N.

(i) y gera N.

Seja $n \in N$, como f é sobrejetora, temos que $n \in Im(f)$, assim existe $m = \sum_{i \in I} \lambda_i x_i \in M$ tal que

$$\begin{aligned} n &= f(m) \\ &= f\left(\sum_{i \in I} \lambda_i x_i\right) && \text{- substituição de } m \\ &= \sum_{i \in I} \lambda_i f(x_i) && \text{- pois } f \text{ é um } A\text{-homomorfismo} \end{aligned}$$

(ii) y é linearmente independente.

Seja $(\lambda_i)_{i \in I} \in A^{(I)}$ tal que

$$\sum_{i \in I} \lambda_i f(x_i) = 0 \Rightarrow f\left(\sum_{i \in I} \lambda_i x_i\right) = 0 \Rightarrow \sum_{i \in I} \lambda_i x_i \in ker(f)$$

Como o $ker(f) = \{0\}$, segue que

$$\sum_{i \in I} \lambda_i x_i = 0$$

Como X é base, temos que

$$\lambda_i = 0, \ \forall \ i \in I$$

Portanto, y é linearmente independente.

Então, segue de (i) e (ii) que $y = \{f(x_i)\}_{i \in I}$ é uma base de N. □

Proposição 5.4. *Todo A-módulo é isomorfo a um quociente de um A-módulo livre.*

Demonstração:

Sejam $X = \{x_i\}_{i\in I}$ um gerador de um A-módulo M e $Y = \{e_k\}_{k\in I}$ a base canônica do A-módulo $A^{(I)}$. Considere

$$f : Y \longrightarrow M$$

$$e_i \longrightarrow f(e_i) = x_i.$$

Como X é gerador, então a extensão $\overline{f} : A^{(I)} \longrightarrow M$ é um epimorfismo, pois

$$m = \sum_{i\in I} a_i x_i \Rightarrow m = \sum_{i\in I} a_i f(e_i) \Rightarrow m = \sum_{i\in I} f(a_i e_i).$$

Logo, pelo teorema do homomorfismo para módulos, temos que

$$A^{(I)}/ker(\overline{f}) \simeq M.$$

□

Proposição 5.5. *Sejam M, N e L A-módulos, $f : M \longrightarrow N$ um A-epimorfismo e $g : L \longrightarrow N$ um A-homomorfismo. Se L é livre, então existe um A-homomorfismo $h : L \longrightarrow M$ tal que o diagrama abaixo*

$$\begin{array}{ccccc} & & & & L \\ & & & \swarrow^{h} & \downarrow g \\ M & \xrightarrow{f} & N & \longrightarrow & 0 \end{array}$$

comuta, isto é, $f \circ h = g$.

Demonstração:

- Existência da h.

  Seja $X = \{x_i\}_{i\in I}$ uma base de L, queremos construir um A-homomorfismo

  $$h : L \longrightarrow M.$$

  Já que $\forall\, x_i \in X$, temos $g(x_i) \in N$, como f é um A-epimorfismo, segue que $g(x_i) \in Im(f)$, então existe $m_i \in M$ tal que $f(m_i) = g(x_i)$. Consideremos

  $$h_1 : X \longrightarrow M$$

  $$x_i \longrightarrow h_1(x_i) = m_i$$

  onde $f(m_i) = g(x_i)$.

Pela Proposição 5.2, temos que h_1 se estende a um único A-homomorfismo $h : L \longrightarrow M$ tal que $h(x_i) = h_1(x_i),\ \forall\ x_i \in X$.

- Mostraremos que $f \circ h = g$.

  De fato, dado $l = \sum_{i \in I} \lambda_i x_i \in L$, temos que

$$\begin{aligned}
(f \circ h)(l) &= f(h(l)) && \text{- definição de composta}\\
&= f\left(h\left(\sum_{i\in I} \lambda_i x_i\right)\right) && \text{- substituição de } l\\
&= f\left(\sum_{i\in I} \lambda_i h(x_i)\right) && \text{- pois } h \text{ é um } A\text{-homomorfismo}\\
&= f\left(\sum_{i\in I} \lambda_i h_1(x_i)\right) && \text{- pois } h(x_i) = h_1(x_i)\\
&= \sum_{i\in I} \lambda_i f(h_1(x_i)) && \text{- pois } f \text{ é um } A\text{-homomorfismo}\\
&= \sum_{i\in I} \lambda_i f(m_i) && \text{- pois } h_1(x_i) \in M\\
&= \sum_{i\in I} \lambda_i g(x_i) && \text{- pois } f(m_i) = g(x_i)\\
&= g\left(\sum_{i\in I} \lambda_i (x_i)\right) && \text{- pois } g \text{ é um } A\text{-homomorfismo}\\
&= g(l) && \text{- substituição de } l
\end{aligned}$$

  Portanto, $f \circ h = g$. □

Corolário 5.2. *Dada uma sequência exata de A-módulos*

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

Se L é livre, então a sequência cinde, isto é, $N \simeq M \oplus L$.

Demonstração:

Consideremos o diagrama

$$\begin{array}{ccccccccc}
 & & & & & & L & & \\
 & & & & & \swarrow^{h} & \downarrow{\scriptstyle Id_L} & & \\
0 & \longrightarrow & M & \xrightarrow{f} & N & \xrightarrow[g]{} & L & \longrightarrow & 0
\end{array}$$

Pela Proposição 5.5, existe um A-homomorfismo $h : L \longrightarrow N$ tal que $g \circ h = Id_L$ e pela Proposição 5.1 a sequência cinde, logo $N \simeq M \oplus L$. □

Corolário 5.3. *Se $f : M \longrightarrow L$ é um epimorfismo com L livre, então $M \simeq ker(f) \oplus L$.*

Demonstração:

Construímos a sequência abaixo que é exata,

$$0 \longrightarrow ker(f) \xrightarrow{i} M \xrightarrow{f} L \longrightarrow 0$$

Logo, pelo Corolário 5.2, temos $M \simeq ker(f) \oplus L$. □

Corolário 5.4. *Seja N um submódulo de um A-módulo livre M tal que o quociente M/N também é livre. Então, N é um somando direto de M e todos os seus suplementares são submódulos livres.*

Demonstração:

Consideremos a sequência abaixo, que é exata

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\pi} M/N \longrightarrow 0$$

Logo, pelo Corolário 5.2 ela é cinde e portanto $M \simeq N \oplus M/N$. Como os suplementares de um submódulo são todos isomorfos, segue que se N' é um suplementar de N, então $N' \simeq M/N$ e portanto é livre. □

Referências Bibliográficas

[1] BEZERRA, Nazaré. *Álgebra*. Notas de Aula.

[2] BEZERRA, Nazaré. *Álgebra Linear*. Notas de Aula.

[3] DOMINGUES, Hygino. e IEZZI, Gelson. *Álgebra Moderna*, São Paulo, Editora Atual, 2003.

[4] MILIES, Polcino. *Anéis e Módulos*, IME-USP, 1972.

[5] PEREIRA Fernanda. *Introdução à Teoria de Módulos*, Monografia de Iniciação Científica.