**UNIVERSIDADE ESTADUAL DA PARAÍBA**
**CAMPUS VII**
**CENTRO CIÊNCIAS EXATAS E APLICADAS**
**DEPARTAMENTO DE MATEMÁTICA**
**CURSO DE MATEMÁTICA**

**Fabricio Almeida Silva Nogueira**

# TEORIA DE MÓDULOS: UM BREVE ESTUDO SOBRE MÓDULOS LIVRES

**Patos-PB**
**2024**

**Fabricio Almeida Silva Nogueira**

# TEORIA DE MÓDULOS: UM BREVE ESTUDO SOBRE MÓDULOS LIVRES

Trabalho de Conclusão de Curso, na modalidade Monografia, apresentado ao corpo docente do Curso de Licenciatura Plena em Matemática - CCEA - da Universidade Estadual da Paraíba como requisito parcial à obtenção do título de Licenciado em Matemática.

**Área de concentração**: Matemática

**Orientador**: Prof. Me. José Ginaldo de Souza Farias

**Patos-PB**
**2024**

N778t Nogueira, Fabricio Almeida Silva.

Teoria dos módulos [manuscrito] : um breve estudo sobre módulos livres / Fabricio Almeida Silva Nogueira. - 2024.

68 f. : il.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências Exatas e Sociais Aplicadas, 2024.

"Orientação : Prof. Me. José Ginaldo de Souza Farias, Coordenação do Curso de Matemática - CCEA".

1. Estruturas Algébricas. 2. Teoria dos Módulos. 3. Módulos Livres. I. Título

21. ed. CDD 512.8

Elaborada por Kaliane Eveny Martins de Oliveira - CRB - 15/986 BSC7

**Fabricio Almeida Silva Nogueira**

**TEORIA DE MÓDULOS: UM BREVE ESTUDO SOBRE MÓDULOS LIVRES**

Trabalho de Conclusão de Curso, na modalidade Monografia, apresentado ao corpo docente do Curso de Licenciatura Plena em Matemática - CCEA - da Universidade Estadual da Paraíba como requisito parcial à obtenção do título de Licenciado em Matemática.

**Área de concentração**: Álgebra

Aprovado em: 14/11/24

**BANCA EXAMINADORA**

José Ginaldo de Souza F.

Prof. Me. José Ginaldo de Souza Farias (Orientador)
Universidade Estadual da Paraíba (UEPB)

Romulo Tonyathy da Silva Mangueira

Prof. Dr. Romulo Tonyathy da Silva Mangueira
Universidade Estadual da Paraíba (UEPB)

Gildevan Oliveira Silva

Prof. Gildevan Oliveira Silva
Universidade Estadual da Paraíba (UEPB)

Dedico esse trabalho a minha esposa, a minha mãe e a meu pai.

## AGRADECIMENTOS

Primeiramente, agradeço ao meu Deus todo poderoso, pois, sem Ele nada disso teria acontecido e por Ele ter cuidado tão bem de mim durante essa jornada, por toda capacidade que tem dado para vencer todas as dificuldades.

Agradeço a minha mãe Benedita e ao meu pai Cosme, por todo amor, apoio emocional e financeiramente, conselhos, proteção, orações, por sempre me motivarem e nunca desistirem de acreditar em mim e no meu sonho, amo muito vocês! Muito obrigado por tudo que sempre fizeram por mim, vocês são os melhores pais do mundo!

Agradeço a minha querida esposa Ingrid, a mulher que faz eu ser um homem melhor, muito obrigado por todo apoio, por sempre está comigo nos momentos bons e ruins da minha vida, por sempre está ali naqueles dias que só você sabe como eu estava me sentido, por sempre acreditar em mim, sempre me motivar e sempre me acolher, eu te amo muito! Muito obrigado por tudo!

Agradeço ao meu irmão Gabriel e as minhas irmãs Fernanda e Joyce, por sempre me ajudarem quando precisei, amo vocês!

Agradeço aos meus amigos: Eduardo, Carina, Willian, Emmanuel, Maycon, Matheus, Jefferson, Camila, Valmir e aos outros que de alguma forma contribuíram na minha formação, sou grato a vocês por toda ajuda nessa caminhada.

Agradeço aos demais amigos que são fora do mundo acadêmico que me apoiaram e os demais familiares que me deram forças para continuar essa jornada, muito obrigado!

Agradeço aos professores: Carol, Arlandson, Paulo, Marcos, Rômulo, Maria lisboa, Raiza, Ismael, Geovany Fernandes, Geovane Júnior, Sérgio, Fabíola, Sally, Érico, maria aparecida e aos demais que de forma significativa contribuíram na minha formação, muito obrigado a todos!

Agradeço imensamente ao Professor José Ginaldo, por toda a orientação, paciência e dedicação ao longo da realização deste trabalho. Sua experiência, apoio constante, amizade e disponibilidade foram fundamentais para o desenvolvimento deste TCC. Sua orientação não apenas contribuiu para a construção deste trabalho, mas também para meu crescimento acadêmico e pessoal.

Gostaria de expressar minha gratião especialmente aos professores Romulo Tonyathy e Gildevan Oliveira, por aceitarem o pedido de participarem da banca de defesa do meu trabalho de conclusão de curso, muito obrigado!

Que Deus abençoe grandemente a todos vocês!

“Não te mandei eu? Seja forte e corajoso, não temas, nem te espantes, porque o Senhor teu Deus é contigo, por onde quer que andares” - Josué 1:9

**RESUMO**

No estudo dos espaços vetoriais, temos uma estrutura na qual definimos duas operações de adição e multiplicação por escalar , em que consideramos corpo $\mathbb{K}$, mas cabe um questionamento nessa afirmação, ”se no lugar desse corpo $\mathbb{K}$, trabalhasse em cima de um Anel A? o que obteremos de volta?”a resposta é simples, dado um conjunto munido com duas operações e um anel A, denominamos essa estrutura de módulo. Dessa forma, esse trabalho tem como objetivo trazer um breve estudo sobre módulos livres, que é um módulo específico, que possui uma base. Assim, ao longo desse trabalho iremos mostrar definições, exemplos, teoremas, proposições e corolários que irão ajudar no entendimento do tema central. Para concluir, iremos mostrar que algumas propriedades que são válidas em espaços vetoriais, mas em módulos livres não são.

**Palavras-chave:** Estruturas Algébricas. Teoria de Módulo. Módulo Livres.

## ABSTRACT

In the study of vector spaces, we have a structure in which we define two operations of addition and multiplication by scalar, in which we consider body $\mathbb{K}$, but a question arises in this statement, "if instead of this body $\mathbb{K}$, worked on an A Ring? What would we get back?"The answer is simple, given a set equipped with two operations and a ring A, we call this structure a module. Therefore, this work aims to provide a brief study on free modules, which is a specific module, which has a base. Thus, throughout this work we will show definitions, examples, theorems, propositions and colorαries that will help in understanding the central theme. To conclude, we will show that some properties that are valid in vector spaces, but in free modules are not.

**Keywords:** Algebraic Structures. Module Theory. Free Module.

SUMÁRIO

# 1 INTRODUÇÃO

A maior parte da história da matemática está nos papiros e tabuas de argila, nesses documentos a álgebra era considerada como a área da matemática que era responsável por resoluções de equações, como por exemplo, no Papiro Hind, nos quais foram encontrados problemas envolvendo equações simples no processo de distribuição de mercadorias. Dessa forma, a álgebra é uma das áreas mais antigas da matemática, a partir disso podemos citar a álgebra abstrata que é a área que se estuda estruturas algébricas, teve inícios com vários matemáticos no qual uniram conhecimentos para discutir os fundamentos da álgebra, dentre eles Charles Babbage(1792 – 1871), George Peacock (1791 – 1858) e John Herschel (1792 – 1878) . Entre esses matemáticos, podemos citar uma obra publicada por Peacock, que publicou sua obra chamada Treatise on Algebra, que ele apresentava o estudo da álgebra por meio de um conjunto de postulados (MILLES, 2004).

Diante disso o estudo de álgebra vem crescendo ao longo da história, como por exemplo, o estudo da álgebra linear, que tem como uma estrutura algébrica central os espaços vetoriais, que é basicamente uma estrutura munida com duas operações que podemos denominar de adição e multiplicação de escalares, no qual esses escalares pertencem ao um corpo. Mas, e se seguimos essa mesma linha de raciocínio e apenas trocarmos esse corpo por um anel, será que obtemos uma nova estrutura? A resposta é sim, e que chamaremos de teoria de módulos. É notório que ao fazermos essa mudança, passa a ser uma nova estrutura e que perderemos algumas propriedades, pois um anel é considerado mais “fraco” do que um corpo, pois tem uma propriedades a menos.

Dessa forma, o objetivo desse trabalho é trazer um breve estudo, dividido em 3 capítulos, sobre um módulo específico: módulo Livre. No capítulo 1 traremos um breve contexto histórico do estudo de álgebra e os direcionamentos dos processo deste trabalho, Já no 2 capítulo, iremos trabalhar toda a teoria de módulo, como as definições de módulos, submódulo, módulo quociente, homomorfismo de módulo, produto direto, soma direta e por fim sequências exatas, no qual esses tópicos serão essenciais para o entendimento do capítulo central.

No capítulo 3, trabalharemos o estudo dos módulos livres. Em espaços vetoriais, quando um determinado subconjunto de elementos é linearmente independente e que gera todo o conjunto, chamamos esse subconjunto de base. Com isso, o estudo de módulo livre é parecido, pois para um módulo ser uma módulo livre só precisa que possua uma base. Dessa forma, trabalharemos algumas definições importante, exemplos de módulos livres e mostrando que algumas propriedades que são validas nos estudo de espaços vetoriais, porém, em módulos livre não são e, por fim, algumas proposições e corolários interessantes.

No final desse estudo se encontra dois apêndices, um sobre grupos e aneis, e outro sobre espaços vetoriais, contendos as princiapis definições para tornar uma trabalho mais completo e ajudar no entendimento no tema central.

# 2 TEORIA DE MÓDULOS

Neste capítulo iremos trabalhar os seguintes tópicos: Módulos, submódulo, módulo quociente, homomorfismo de módulo, produtos, soma direta e sequências exatas. No qual iremos mostrar definições, exemplos, preposições, teoremas e alguns resultados importantes para compreensão do tema central desse trabalho.

### 2.0.1 Módulos

**Definição 2.0.1.1:** *Seja $A$ um anel e um $M$ um conjunto não vazio, munido com as seguintes operações:*

*Adição (+) :*

$$\begin{aligned} M \times M &\longrightarrow M \\ (a,b) &\longrightarrow a+b \end{aligned}$$

*Operação Externa* $(\cdot)$ *:*

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

*Dizemos que a terna* $(M,+,\cdot)$ *é um módulo sobre o anel $A$ ( ou $A$-Módulo à esquerda ou $A$-Módulo à direita ) se satisfas as seguintes propriedades*:

I - *(Associatividade da Adição)* $a+(b+c)=(a+b)+c$*; para todo* $a,b,c \in M$

II - *(Comutatividade da Adição)* $a+b=b+a$*; para todo* $a,b \in M$

III - *(elemento neutro da Adição) vai existir um* $0_M \in M$ *, tal que para todo* $a \in M$*,* $a+0_M=a$

IV - *(Simétrico da Adição) para todo* $a \in M$*, vai existir um* $-a \in M$ *tal que* $a+(-a)=0_M$

V - *(Associativa da operação externa)* $(\lambda\cdot\beta)\cdot a=\lambda\cdot(\beta\cdot a)$*; para todo* $\lambda,\beta \in A$ *e* $a \in M$

VI - *(Distributividade com relação aos elementos de M)* $\lambda\cdot(a+b)=\lambda\cdot a+\lambda\cdot b$*; para todo* $\lambda \in A$ *e* $a,b \in M$

VII - *(Distributividade com relação às escalares)* $(\lambda+\beta)\cdot a=\lambda\cdot a+\beta\cdot a$*; para todo* $\lambda,\beta \in A$ *e* $a \in M$

VIII - *(Elemento neutro da operação externa) vai existir* $1_A \in A$ *tal que* $a\cdot 1_A=a$*; para todo* $a \in M$

**Observação:** Note que sastifazer as 4 primeira propriedades é o mesmo dizer que é um grupo abeliano.

**Observação:** Uma forma simplificada de dizer que a terna $(M, +, \cdot)$ é um módulo sobre o anel A ( ou A-Módulo ) se M com a operação de adição é um grupo abeliano e sastisfaz as 4 ultimas propriedades. Porém, se o anel A não tiver unidade, nesse caso será omitido a condição VIII. Nesse estudo, usaremos sempre A-módulo à esquerda e anéis com unidade.

**Preposição 2.0.1.2:**Seja M um A-módulo, então vale as seguintes propriedades:

I - $0_A \cdot m = 0_M$ *, para todo* $m \in M$
II - $\alpha \cdot 0_M = 0_M$ *, para todo* $\alpha \in A$
III - $(-a) \cdot m = -(a \cdot m) = a \cdot (-m)$ *, para todo* $a \in A$ *e* $m \in M$
IV - $(a - b) \cdot m = a \cdot m - b \cdot m$ *, para todo* $a, b \in A$ *e* $m \in M$
V - $a \cdot (m - n) = a \cdot m - a \cdot n$ *, para todo* $a \in A$ *e* $m, n \in M$

**Demostrações:**

[I] De fato,

$$0_A \cdot m = (0_A + 0_A) \cdot m = 0_A \cdot m + 0_A \cdot m$$
$$\Rightarrow 0_A \cdot m + 0_A \cdot m = 0_A \cdot m$$

Como $0_A \cdot m \in M$, então $-(0_A \cdot m) \in M$. Daí,

$$0_A \cdot m + 0_A \cdot m - (0_A \cdot m) = 0_A \cdot m - (0_A \cdot m)$$
$$\Rightarrow 0_A \cdot m = 0_M$$

□

[II] De fato,

$$\alpha \cdot 0_M = \alpha \cdot (0_M + 0_M) = \alpha \cdot 0_M + \alpha \cdot 0_M$$
$$\Rightarrow \alpha \cdot 0_M + \alpha \cdot 0_M = \alpha \cdot 0_M$$

Como $\alpha \cdot 0_M \in M$, então $-(\alpha \cdot 0_M) \in M$. Daí,

$$\alpha \cdot 0_M + \alpha \cdot 0_M - (\alpha \cdot 0_M) = \alpha \cdot 0_M - (\alpha \cdot 0_M)$$
$$\Rightarrow \alpha \cdot 0_M = 0_M$$

□

[III] Dado $a \cdot m \in M$, o seu simétrico aditivo é $-(a \cdot m) \in M$. Daí, basta mostrar que $(-a) \cdot m$ e $a \cdot (-m)$ são também simétricos aditivo de $a \cdot m$. De fato,

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

De forma análoga, temos

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

Portanto,

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

$\square$

[IV] De fato,

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

$\square$

[V] De fato,

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

$\square$

**Exemplo 2.0.1.3:** Todo espaço vetorial sobre um corpo K é um K-módulo.

De fato, como todo corpo é um anel, então um espaço vetorial sobre um corpo K satisfaz todas as propriedades para ser um K-módulo.

**Exemplo 2.0.1.4:** Seja A um anel e $I_A$ um ideal desse anel, com as operações:

Adição(+):

$$\begin{aligned} I_A \times I_A &\longrightarrow I_A \\ (a,b) &\longrightarrow a+b \end{aligned}$$

Operação Externa($\cdot$):

$$\begin{aligned} A \times I_A &\longrightarrow I_A \\ (\lambda,a) &\longrightarrow \lambda \cdot a \end{aligned}$$

A terna $(I_A,+,\cdot)$é um A-módulo.

De fato, note que $I_A$ é um subanel de A, então $I_A$ é um grupo abeliano. Por outro lado temos que para quaisquer $\lambda,\beta \in A$ e a,b $\in I_A$, como $I_A \subset A$ e que A é um anel, então as condições:

I - $(\lambda \cdot \beta)\cdot a = \lambda \cdot (\beta \cdot a)$; para todo $\lambda,\beta \in A$ e $a \in M$
II - $\lambda \cdot (a+b) = \lambda \cdot a + \lambda \cdot b$; para todo $\lambda \in A$ e $a,b \in M$
III - $(\lambda + \beta)\cdot a = \lambda \cdot a + \beta \cdot a$; para todo $\lambda,\beta \in A$ e $a \in M$
IV - vai existir $1_A \in A$ tal que $a \cdot 1_A = a$; para todo $a \in M$

Vão ser satisfeitas, com isso concluimos que é um A-módulo.

**Observação:** Através desse exemplo, em particular, todo anel pode ser considerado como um módulo sobre si mesmo.

**Exemplo 2.0.1.5:** Seja (A,+) um grupo abeliano, pode ser um módulo sobre um anel $\mathbb{Z}^+$ com a seguinte operação:

Operação Externa($\cdot$):

$$\begin{aligned} \mathbb{Z}^+ \times A &\longrightarrow A \\ (n,a) &\longrightarrow n \cdot a = a^n \end{aligned}$$

A é um $\mathbb{Z}$-módulo.

**Exemplo 2.0.1.6:** Seja (G,+) um grupo abeliano e considere

$$End(G) = \{f : G \longrightarrow G\}$$

Como sendo o conjunto de todos os endomorfismo de grupo. Introduzindo a estrtuta de anéis em End(G), dada por

$$\begin{aligned}(+) : End(G) \times End(G) &\longrightarrow End(G)\\ (f,g) &\longrightarrow (f+g)(x) = f(x) + g(x)\end{aligned}$$

$$\begin{aligned}(\cdot) : End(G) \times End(G) &\longrightarrow End(G)\\ (f,g) &\longrightarrow (f \cdot g)(x) = f(g(x))\end{aligned}$$

Note que a terna $(End(G), +, \cdot)$ com essas estruturas bem definidas é um anel. Agora definimos a lei da composição externa dada por:

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

Dessa forma, temos que G é um End(G)-módulo.

De Fato, note que End(G) é um grupo abeliano, pelo fato que End(G) é um anel. Resta mostrar End(G) com a operação externa admiti estrutura de módulo.

Sejam $f, g \in End(G)$ e $a, b \in G$. Daí, temos que

[I]Associativa da operação externa

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

[II] Distributividade em relação às escalares

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

[III] Distributividade com relação aos elementos de End(G)

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

[IV] elemento neutro

Seja $I_d$ como sendo a função identidade de End(G), daí temos que para todo $a \in G$

$$
\begin{aligned}
I_d \odot a &= I_d(a) \\
&= a
\end{aligned}
$$

Portanto, concluimos que G é um End(G)-módulo.

**Exemplo 2.0.1.7:** Seja A um anel e X um conjunto qualquer. Indicaremos por $A^X$ como o conjunto de todas as funções de domínio X a valores de A. Definimos do seguinte modo as operações de módulo como:

Adição(+):

$$
\begin{aligned}
A^X \times A^X &\longrightarrow A^X \\
(f, g) &\longrightarrow (f+g)(x) = f(x) + g(x)
\end{aligned}
$$

Operação Externa($\cdot$):

$$
\begin{aligned}
A \times A^X &\longrightarrow A^X \\
(a, f) &\longrightarrow (af)(x) = a \cdot f(x)
\end{aligned}
$$

Temos que $(A^X, +)$ é um grupo abeliano e a terna $(A^X, +, \cdot)$ admite a estrutura de módulo, ou seja, é um A-módulo.

### 2.0.2 Submódulo

**Definição 2.0.2.1:** *Seja M um A-módulo e um subconjunto $N \subset M$. N diz-se um A-submódulo de M se satisfaz as seguintes condições:*

I - $0_M \in N$;

II - $u + k \in N$, *para todo* $u, k \in N$;

III - $a \cdot u \in N$, *para todo* $a \in A, u \in N$.

**Exemplo 2.0.2.2:** Seja M um A-módulo, temos que $\{0_M\}$ é um A-submódulo de M.

**Exemplo 2.0.2.3:** Seja M é um A-módulo, temos que M A-submódulo de M.

**Exemplo 2.0.2.4:** Seja V um espaço vetorial sobre um corpo K. Um subconjunto $S \subset V$ é um submódulo, se somente se, S é um subespaço vetorial.

De fato, como todo corpo é um anel, então as definições de submódulo e subespaço vetorial coincidem. Por outro lado, como V é um K-módulo e $S \subset V$ é um submódulo, onde os escalares pertencem ao corpo K, segue-se que as definições de submódulo e subespaço vetorial também vão se coincidir.

**Exemplo 2.0.2.5:** Seja $N_1$ e $N_2$ submódulos do A-módulo M. O conjunto $N_1 + N_2 = \{n_1 + n_2, \forall n_1 \in N_1$ e $n_2 \in N_2\}$ também é um submódulo, no qual é chamada de submódulo soma de $N_1$ e $N_2$.

[I] De fato, note que $N_1 + N_2 \neq \emptyset$, pois como $N_1$ e $N_2$ são submódulos, temos que pelo menos $0_M \in N_1$ e $0_M \in N_2$, daí temos que

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

[II] Seja $u, k \in N_1 + N_2$, onde $u = n_1 + n_2$ e $k = n_3 + n_4$, daí

$$\begin{aligned} u + k &= (n_1 + n_2) + (n_3 + n_4) \\ &= (n_1 + n_3) + (n_2 + n_4) \\ &= n_5 + n_6 \\ &= s \in N_1 + N_2 \end{aligned}$$

Onde $s = n_5 + n_6 \in N_1 + N_2$. Portanto, de fato, $u + k \in N_1 + N_2$.

[III] Seja $a \in A$ e $u \in N_1 + N_2$, onde $u = n_1 + n_2$, daí

$$a \cdot (n_1 + n_2) = a \cdot n_1 + a \cdot n_2 \in N_1 + N_2$$

De fato, como $N_1$ é um submódulo, temos que $a \cdot n_1 \in N_1$, do mesmo modo, temos que $a \cdot n_2 \in N_2$. Daí temos que $a \cdot n_1 + a \cdot n_2 \in N_1 + N_2$.

Portanto, como mostramos que os itens I, II e III da definição de submódulo são satisfeitos, concluimos que o $N_1 + N_2$ é um submódulo.

**Exemplo 2.0.2.6** Seja M um A-módulo e $\{N_i\}_{i\in I}$ uma família de submódulos de M. então $\bigcap\limits_{i\in I} N_i$ é um submódulo de M.

[I] note que

$$\bigcap_{i\in I} N_i \neq \emptyset$$

Ja que $N_i$ é submódulo, para cada $i \in I$, então $0_M \in N_i$, daí $0_M \in \bigcap\limits_{i\in I} N_i$.

[II] Sejam $u, k \in \bigcap\limits_{i\in I} N_i$, então $u + k \in \bigcap\limits_{i\in I} N_i$.

De fato, ja que $u, k \in \bigcap\limits_{i\in I} N_i$, então temos que $u, k \in N_i$ e como $N_i$ é submódulo, para todo $i \in I$, temos que $u + k \in N_i$, logo $u + k \in \bigcap\limits_{i\in I} N_i$.

[III] Seja $a \in A$ e $u \in \bigcap\limits_{i\in I} N_i$, daí $a \cdot u \in \bigcap\limits_{i\in I} N_i$.

De fato, como $u \in \bigcap\limits_{i\in I} N_i$, então temos que $u \in N_i$, como $N_i$ é submódulo, para todo $i \in I$, então $a \cdot u \in N_i$, logo $a \cdot u \in \bigcap\limits_{i\in I} N_i$.

Portanto, como mostramos que os itens I, II e III da definição de submódulo são satisfeitos, concluimos que $\bigcap\limits_{i\in I} N_i$ é um submódulo.

**Exemplo 2.0.2.7:** Seja S um subconjunnto de um A-módulo M. O conjunto

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

É um submódulo de M, no qual chamamos o submódulo gerado por S.

[I] note que $(S) \neq \emptyset$, pois como $S \subset (S)$ temos que $0_M = 0_{Si} \in (S)$.

[II] Sejam $u, k \in (S)$, onde $u = \sum\limits_{i=1}^{n} a_i s_i$ e $k = \sum\limits_{j=1}^{m} a_j s_j$, para todo $a_i, a_j \in A$ e $s_i, s_j \in S$. Daí temos que

$$
\begin{aligned}
u+k &= \sum_{i=1}^{n} a_i s_i + \sum_{j=1}^{m} a_j s_j \\
&= \sum_{p=1}^{r} b_p x_p \in (S).
\end{aligned}
$$

Onde $b_p = a_i a_j \in A$ e $x_p = s_i s_j \in S$, então de fato é válido, ja que $u+k$ é um soma finita de elementos de S, multiplicados por elementos do anel A.

[III] Seja $a \in A$ e $u \in (S)$, onde $u = \sum_{i=1}^{n} a_i s_i$ para todo $a_i \in A, s_i \in S$. daí temos

$$
\begin{aligned}
a \cdot u &= a \cdot \sum_{i=1}^{n} a_i s_i \\
&= \sum_{i=1}^{n} a(a_i s_i) \\
&= \sum_{i=1}^{n} (a a_i) s_i \\
&= \sum_{i=1}^{n} b_i s_i \in (S)
\end{aligned}
$$

Onde $b_i = a a_i$.

Portanto, como mostramos que os itens I, II e III da definição de submódulo são satisfeitos, concluimos que (S) é um submódulo.

### 2.0.3 **Módulo Quociente**

Seja M um A-módulo e N um submódulo de M. Considerando a estrutura de grupo aditivo abeliano de M, é possível contruir um grupo quociente

$$\frac{M}{N} = \{x+N; x \in M\}$$

definimos agora a operação $\oplus$: $\frac{M}{N} \times \frac{M}{N} \to \frac{M}{N}$ dada por $(x+N) \oplus (y+N) = (x+y)+N$.

Note que esta operação está bem definida, pois sejam $x+N, y+N, z+N, r+N \in \frac{M}{N}$ tais que $x+N = y+N$ e $z+N = r+n$. Dessa forma, $x-y, z-r \in N$ e segue que $(x-y)+(z-r) \in N$. Assim, $(x+y)-(z+r) \in N$, o que implica que $(x+z)+N = (y+r)+N$, ou seja, $(x+N) \oplus (z+N) = (y+N) \oplus (r+N)$.

**Afirmação 1:** $(\frac{M}{N}, \oplus)$ é um grupo abeliano.

De fato, sejam $x, y, z \in M$, tem-se

[I] Associatividade da soma

$$\begin{aligned}(x+N)\oplus[(y+N)\oplus(z+N)] &= (x+N)\oplus[(y+z)+N]\\ &= [x+(y+z)]+N\\ &= [(x+y)+z]+N\\ &= [(x+y)+N]\oplus(z+N)\\ &= [(x+N)\oplus(y+N)]\oplus(z+N)\end{aligned}$$

[II] Elemento neutro da adição

$$\begin{aligned}(0_M+N)\oplus(x+N) &= (0_M+x)+N\\ &= x+N; \forall x\in M.\end{aligned}$$

Dessa forma, $0_M + N$ é o elemento neutro.

[III] Inverso aditivo

$$\begin{aligned}(x+N)\oplus(-x+N) &= [x+(-x)]+N\\ &= 0_M+N\end{aligned}$$

ou seja, $-x + N$ é o inverso aditivo de $x + N$.

[IV] Comutatividade

$$\begin{aligned}(x+N)\oplus(y+N) &= (x+y)+N\\ &= (y+x)+N\\ &= (y+N)\oplus(x+N).\end{aligned}$$

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

$$\begin{aligned}A\times\frac{M}{N} &\longrightarrow \frac{M}{N}\\ (a, x+N) &\longrightarrow a(x+N) = ax+N\end{aligned}$$

Note que a lei de composição externa está bem definida, pois dados $x + N = y + N$, tem-se $x - y \in N$ e dado $a \in A$, segue que $a(x - y) = ax - ay \in N$ o que implica que $ax + N = ay + N$, ou seja, $a(x + N) = a(y + N)$.

**Afirmação 2:** O grupo aditivo $\frac{M}{N}$, com essa lei de composição externa, define uma estrutura de A-módulo.

De fato, sejam $x + N, y + N, z + N \in \frac{M}{N}$ e $\alpha, \beta \in A$ quaisquer, tem-se:

[I]Associatividade da composição externa

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

[II] Distrubutividade em relação aos elemento de $\frac{M}{N}$

$$\begin{aligned} \alpha[(x + N) \oplus (y + N)] &= \alpha[(x + y) + N] \\ &= \alpha(x + y) + N \\ &= (\alpha x + \alpha y) + N \\ &= (\alpha x + N) \oplus (\alpha y + N) \\ &= \alpha(x + N) \oplus \alpha(y + N) \end{aligned}$$

[III] Distribuição em relação aos elementos de A

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

[IV] Elemento neutro da composição externa

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

Portanto, como mostramos que todos os itens são satisfeitos, concluimos que $\frac{M}{N}$ é um A-módulo.

**Definição 2.0.3.1:** $\frac{M}{N}$ é um A-módulo chamado de módulo quociente de M pelo seu submódulo N.

### 2.0.4 Homomorfismo de Módulo

**Definição 2.0.4.1:** *Sejam M e N dois A-módulo. Uma função $f : M \longrightarrow N$ chama-se homomorfismo ou A-homomorfismo, se para todo $x, y \in M$ e $a \in A$ verifica-se:*

I - $f(x + y) = f(x) + f(y)$

II - $f(ax) = af(x)$

**Proposição 2.0.4.2:** (Propriedades Elementares) Se $f : M \longrightarrow N$ é um A-homomorfismo, então vale:

I - $f(0_M) = 0_N$

II - f(-m) = -f(m)

III - f(m - n) = f(m) - f(n)

**Demostrações:**

[I] De fato, pois

$$\begin{aligned} f(0_M) &= f(0_M + 0_M) \\ &= f(0_M) + f(0_M) \end{aligned}$$

Subtraindo em ambos lados por $f(0_M)$, temos

$$\begin{aligned} f(0_M) - f(0_M) &= f(0_M) + f(0_M) - f(0_M) \\ 0_N &= f(0_M) \end{aligned}$$

Poratnto, vale.

□

[II] De fato, note que

$$\begin{aligned} 0_M &= f(m + (-m)) \\ &= f(m) + f(-m) \end{aligned}$$

Subtraindo em ambos lados por $f(m)$, temos

$$\begin{aligned} 0_M - f(m) &= f(m) + f(-m) - f(m) \\ -f(m) &= f(-m) \end{aligned}$$

Poratnto, vale.

$\square$

[III] De fato, pois

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

Poratnto, vale.

$\square$

**Exemplo 2.0.4.3:** Seja N um submódulo de um A-módulo de M. A função inclusiva $Id : N \longrightarrow M$, dada por $Id = x$ é um A-homomorfismo.

**Exemplo 2.0.4.4:** Seja N um submódulo de um A-módulo M. A projeção canônica

$$\begin{aligned} \pi : M &\longrightarrow \frac{M}{N} \\ x &\longrightarrow \pi(x) = x + N \end{aligned}$$

É um A-homomorfismo.

[I] De fato, sejam $x, y \in M$ e $a \in A$, daí temos

$$\pi(x+y) = (x+y)+N$$
$$= (x+N)+(y+N)$$
$$= \pi(x)+\pi(y)$$

[II] Por outro lado

$$\pi(ax) = (ax)+N$$
$$= a(x+N)$$
$$= a\pi(x)$$

Dessa forma, concluimos que é um A-homomorfismo.

**Definição 2.0.4.5:** *Se $f : M \longrightarrow N$ é um A-homomorsfismo injetivo, chamaremos $f$ de A-monomorfismo.*

**Definição 2.0.4.6:** *Se $f : M \longrightarrow N$ é um A-homomorsfismo sobrejetivo, chamaremos $f$ de A-epimorfismo.*

**Definição 2.0.4.7:** *Se $f : M \longrightarrow N$ é um A-homomorsfismo bijetivo, chamaremos $f$ de A-isomorfismo.*

**Definição 2.0.4.8:** *Se $f : M \longrightarrow N$ é um A-isomorfismo, diremos que $M$ e $N$ são A-módulos isomorfos e que denotaremos por $M \simeq N$.*

**Definição 2.0.4.9:** *Se $f : M \longrightarrow M$ é um A-homomorsfismo, chamaremos $f$ de A-Endomorfismo, no qual denotaremos por $End_A(M) = f : M \longrightarrow M$ é um A-Endomorfismo.*

**Definição 2.0.4.10:** *Se $f : M \longrightarrow M$ é um A-isomorfismo, chamaremos $f$ de A-Automorfismo, no qual denotaremos por $Aut_A(M) = f : M \longrightarrow M$ é um A-Automorfismo.*

**Proposição 2.0.4.11:**

I - Sejam $f : M \longrightarrow M'$ e $g : M' \longrightarrow M''$ A-homomorfismos. Então $g \circ f : M \longrightarrow M''$ também é um A-homomorfismo.

II - Se $f : M \longrightarrow M'$, $g : M' \longrightarrow M''$, $h : M'' \longrightarrow M'''$ são A-homomorfismos, então

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

III - Se $f_1 : M \longrightarrow M'$, $f_2 : M \longrightarrow M'$, $g : M' \longrightarrow M''$ são A-homomorfismos, então

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

IV - Dado um A-homomorfismo $f : M \longrightarrow N$, então

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

V - Dados A-homomorfismos $f : M \longrightarrow M'$ e $g : M' \longrightarrow M$, tais que $g \circ f = Id_M$, então f é um monomorfismo e g um epimorfismo.

**Demostrações:**

[I] De fato,Seja x,y $\in$ M, então:

$$\begin{aligned}(g \circ f)(x + y) &= g[f(x + y)]\\ &= g[f(x) + f(y)]\\ &= g(f(x)) + g(f(y))\\ &= (g \circ f)(x) + (g \circ f)(y)\end{aligned}$$

Seja a $\in$ A e x $\in$ M, daí

$$\begin{aligned}(g \circ f)(ax) &= g[f(ax)]\\ &= g[af(x)]\\ &= a[g(f(x))]\\ &= a[(g \circ f)(x)]\\ &= a(g \circ f)(x)\end{aligned}$$

$\square$

[II] De fato, pois seja x $\in$ M, daí

$$\begin{aligned}[h \circ (g \circ f)](x) &= h \circ [g(f(x))]\\ &= (h \circ g)(f(x))\\ &= [(h \circ g) \circ f](x))\end{aligned}$$

$\square$

[III] De fato, seja x $\in$ M, daí

$$\begin{aligned}[g_1 \circ (f_1 + f_2)](x) &= g_1[(f_1 + f_2)(x)]\\ &= g_1[(f_1(x) + f_2(x)]\\ &= g_1(f_1(x)) + g_1(f_2(x))\\ &= (g_1 \circ f_1)(x) + (g_1 \circ f_2)(x)\end{aligned}$$

□

[IV] De fato, basta considerar que para todo x ∈ M, temos

$$\begin{aligned}(Id_N \circ f)(x) &= Id_N(f(x))\\ &= f(x)\end{aligned}$$

Por outro lado, temos

$$\begin{aligned}(f \circ Id_M)(x) &= f(Id_M(x))\\ &= f(x)\end{aligned}$$

□

[V] Vamos mostrar que f é um A-monomorfismo e g é um A-epimorfismo. De fato, seja x,y ∈ M de tal modo que $f(x) = f(y)$, dai aplicando g, temos

$$g(f(x)) = g(f(y)) \Rightarrow (g \circ f)(x) = (g \circ f)(y) \Rightarrow Id(x) = Id(y) \Rightarrow x = y$$

Portanto f é um A-monomorfismo, resta mostrar que g é um A-epimorfismo. De fato, seja x ∈ M, daí temos $Id(x) = x$, por hipótese temos que

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

Daí, denotando $f(x) = y \in$ M', temos $g(y) = y$, então concluimos que g é um epimorfismo.

□

**Definição 2.0.4.12:** *Dado um homomorfismo $f : M \longrightarrow N$, chamamos de imagem de f e o núcleo( ou Kernel) de f, respectivamente os conjuntos:*

$$Im(f) = \{n \in N, \exists x \in M, tal que f(x) = n\}$$
$$Ker(f) = \{m \in M, tal que f(m) = 0\}$$

**Teorema 2.0.4.13:** (Homomorfismo para Módulo) Seja M e N dois A-módulos, se $f : M \longrightarrow N$ um homomorfismo, então

$$\frac{M}{Ker(f)} \simeq Im(f)$$

**Demostração:**

Inicialmente, iremos contruir um isomorfismo entre esse módulos. Considere as seguintes aplicações no diagrama a seguir

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "h"'] & N \arrow[d, "s"] \\ \frac{M}{Ker(f)} \arrow[r, "g"'] & Im(f) \end{tikzcd}$$

Agora definimos a função g como sendo

$$g : \tfrac{M}{Ker(f)} \longrightarrow Im(f)$$
$$(x + N) \longrightarrow f(x)$$

Note que g está bem definida, pois

$$x + N = y + N \Rightarrow x - y \in Ker(f) \Rightarrow f(x - y) = 0 \Rightarrow f(x) = f(y)$$

Daí, iremos mostar que g é um homomorfismo, ou seja, considere x,y $\in \frac{M}{Ker(f)}$, então

$$\begin{aligned} g[(x + N) + (y + N)] &= g[(x + y) + N] \\ &= f(x + y) \\ &= f(x) + f(y) \\ &= g(x + N) + g(y + N) \end{aligned}$$

Agora considere a $\in$ A e x $\in \frac{M}{Ker(f)}$, daí temos

$$\begin{aligned} g[a(x+N)] &= g[(ax)+N] \\ &= f(ax) \\ &= af(x) \\ &= ag(x+N) \end{aligned}$$

Logo concluimos que g é um A-homomorfismo. Agora iremos mostrar que g é injetiva e sobrejetiva

Injetividade: Dado x,y $\in$ M, tal que f(x) = f(y), então

$$f(x) = f(y) \Rightarrow f(x) - f(y) = 0 \Rightarrow f(x-y) = 0 \Rightarrow x - y \in Ker(f) \rightarrow x = y$$

Sobrejetividade: De fato, pois

$$\begin{aligned} Im(g) &= \{g(x+N), x+N \in \frac{M}{Ker(f)}\} \\ &= \{f(x), x \in M\} \\ &= Im(f) \end{aligned}$$

Portanto, como g é um A-homomorfismo bijetor, então g é isomorfismo.

□

**Colorário 2.0.4.14:** Seja $f : M \longrightarrow N$ um A-epimorfismo, então

$$N \simeq \frac{M}{Ker(f)}$$

**Demostração:** De fato, pois pelo teorema do homomorfismo para módulo nos garante que $\frac{M}{Ker(f)} \simeq Im(f)$ e note que f é um A-epimorfismo, então $Im(f) = N$, assim, $\frac{M}{Ker(f)} \simeq N$.

□

**Teorema 2.0.4.15:(Primeiro Teorema do Isomorfismo)** Seja M um A-módulo e P, N dois submódulos tais que $P \subset N$. Então

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

**Demostração:** Vamos considera uma função f definida da seguinte forma:

$$\begin{aligned} f : M/P &\longrightarrow M/N \\ x + P &\longrightarrow f(x+P) = x + N, \forall x \in M. \end{aligned}$$

Note que a função está bem definida, pois dados $x_1, x_2 \in M$ temos

$$x_1 + P = x_2 + P \Longrightarrow x_1 - x_2 \in P \subset N \Longrightarrow x_1 - x_2 \in N \Longrightarrow x_1 + N = x_2 + N$$

Daí, observe que f é um A-homomorfismo, pois para todo $x_1$ e $x_2 \in M$ e $a \in A$, temos [I]

$$\begin{aligned} f[(x_1 + P) + (x_2 + P)] &= f[(x_1 + x_2) + P] \\ &= (x_1 + x_2) + N \\ &= (x_1 + N) + (x_2 + N) \\ &= f(x_1 + P) + f(x_2 + P) \end{aligned}$$

[II]

$$\begin{aligned} f(a(x_1 + P)) &= f(ax_1 + P) \\ &= ax_1 + N \\ &= a(x_1 + N) \\ &= af(x_1 + P) \end{aligned}$$

Daí, note que f também é epimorfismo, pois

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

Dessa forma, pelo colorário 2.0.4.14 temos

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

Agora

$$\begin{aligned} Ker(f) &= \{x + P \in M/P, f(x + P) = 0 + N\} \\ &= \{x + P \in M/P, x + N = 0 + N\} \\ &= \{x + P \in M/P, x \in N\} \\ &= N/P \end{aligned}$$

Portanto,

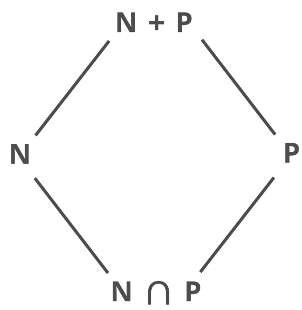
$$M/N \simeq \frac{M/P}{N/P}$$

□

**Teorema 2.0.4.16: ( Segundo Teorema do Isomorfismo)** Sejam N e P submódulos de um A-módulo M. Então temos

$$\frac{M/N}{N\cap P} \simeq \frac{N+P}{P}$$

Essa relação entre submódulos do enunciado pode ser vizualizada no seguinte diagrama:




**Demostração:** Vamos considera uma função f definida da seguinte forma:

$$f : N \longrightarrow \frac{N+P}{P}$$
$$x \longrightarrow f(x) = x + P, \forall x \in M.$$

Note que f é um A-homomorfismo, pois dados $x_1$ e $x_2 \in N$ e $a \in A$, temos
[I]

$$\begin{aligned} f(x_1 + x_2) &= (x_1 + x_2) + P \\ &= (x_1 + P) + (x_2 + P) \\ &= f(x_1) + f(x_2) \end{aligned}$$

[II]

$$\begin{aligned} f(a(x_1)) &= (ax_1) + P \\ &= a(x_1 + P) \\ &= af(x_1) \end{aligned}$$

E também f é um epimorfismo, pois

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

Portanto, pelo colorário 2.0.4.14, temos que

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

Daí, observe que dado um $x \in N, x \in Ker(f) \iff x + P = 0 + P \iff x - 0 = x \in P$. Dessa forma, se

$$x \in Ker(f) \iff f(x) = 0 \iff x + P = 0 + P \iff x - 0 = x \in P$$

portanto, $x \in Ker(f) \iff x \in P$. Agora, se

$$x \in Ker(f) \iff x \in N \text{ e } x \in P \iff x \in N \cap P$$

Dessa forma, substituindo $Ker(f)$, temos

$$\frac{M/N}{N \cap P} \simeq \frac{N+P}{P}$$

O resultado acima é denominado de isomorfismo de Noether.

□

### 2.0.5 **Produto direto**

Dados dois A-módulos M e N, podemos obter um novo A-módulo, basta considerar o conjunto de todos os pares ordenados da forma $(x, y)$ onde x $\in$ M e y $\in$ N, e considerar as seguinte operaçoes

$$(x, y) + (z, w) = (x + z, y + w) \text{ onde para todo x,z} \in \text{M e y,w} \in \text{N}$$
$$\lambda(x, y) = (\lambda x + \lambda y), \text{ para todo } \lambda \in \mathbb{R}$$

Nesse sentido, o propósito desse tópico é que quando consideramos uma família de A-módulos, infinitos, a construção anterior pode ser generalizada em dois sentidos. Assim, seja $\{M_i\}_{i \in I}$ uma família de A-módulos e $M = \prod_{i \in I} M_i$ o produto cartesiano dos menbros da família, onde I é o conjunto arbitrário de índices. Dessa forma, em M podemos definir a estrutura de módulos, ou seja

$$\text{Adição: } (m_i)_{i\in I} + (n_i)_{i\in I} = (m_i + n_i)_{i\in I}$$
$$\text{Multiplicação por escalar: } \lambda(m_i)_{i\in I} = (\lambda m_i)_{i\in I}$$

Onde $M = \{(m_1, m_2, ..., m_i)$ para todo $m_i \in M_i$ e para todo $i \in I$.

**Definição 2.0.5.1** *o A-módulo M construido a cima é chamado de produto direto da família* $\{M_i\}_{i\in I}$*. Ou seja, para cada* $i \in I$*, diremos 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 do tipo $I = \{1, 2, 3, ..., n\}$ denotaremos o produto direto do seguinte modo:

$$\prod_{i\in I} M_i = M_1 x M_2 x M_3 x ... x M_n$$

Onde cada Módulo $M_i$, com $i \in I$, pode ser canônicamente imerso no produto direto de M, so precisa considerar as aplicações $i_k : M_k \to M$ sendo que a cada $m_k \in M_k$ associado a família $(x_i)_{i\in I} \in M$, tal que para $i = k$ temos $x_i = m_k$ e para $i \neq k$ temos $x_i = 0$. As funções definidas a cima são monomorfismo e serão chamadas de inclusões naturais. De fato, pois,

$$\begin{aligned} Ker(f)(i_k) &= \{m_k \in M_k, i_k(m_k) = 0\} \\ &= \{m_k \in M_k, (0, 0, ..., m_k, ...) = (0, 0, ..., 0, ...)\} \\ &= \{0\} \end{aligned}$$

Logo $i_k$ é monomorfismo.

Tambem serão definidas as funções que chamaremos de projeções sobre as componentes, de seguinte modo $p_k : M \to M_k$, associando a cada elemento $(m_i)_{i\in I} \in$ M a k-ésima componente $m_k \in M_k$. De fato, pois note que

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

Logo $p_k$ é um epimorfismo.

**Proposição 2.0.5.2:** Sejam $p_k$ as projeções sobre as componentes e $i_k$ as inclusões naturais. então é válido

I - $p_k \circ i_k = Id_{M_k}$, para todo $k \in I$

II - $p_k \circ i_h = 0$, para todo $h, k \in I$ tal que $h \neq k$

**Demostração:**

[I] De fato, pois para todo $k \in I$ e $m_k \in M_k$, temos

$$\begin{aligned}(p_k \circ i_k) &= p_k(i_k(m_k))\\ &= p_k(0, 0, , ..., m_k, 0, ...)\\ &= m_k\\ &= Id_{M_k}\end{aligned}$$

$\square$

[II] Já por outro lado, dado $h, k \in I$, tal que $h \neq k$ e para todo $m_h \in M_k$, temos

$$\begin{aligned}(p_k \circ i_h)(m_h) &= p_k(i_k(m_h))\\ &= p_k(0, 0, , ..., m_h, 0, ...)\\ &= m_k\\ &= 0\end{aligned}$$

$\square$

**Proposição 2.0.5.3:** Sejam $\{M_i\}$ uma família de A-módulos e $M = \prod_{i \in I} M_i$ o produto direto desta família, daí considere $\{p_k : M \to M_k\}_{k \in I}$ as projeções sobre as componentes. Dado um A-módulo N e uma família de A-homomorfismo $\{q_k : N \to M_k\}$, existe um único A-homomorfismo $f : N \to M$ tal que $q_k = p_k \circ f$ para todo $k \in I$, ou seja, o diagrama comuta.

$$\begin{tikzcd} N \arrow[r, "f"] \arrow[d, "q_k"'] & M \arrow[dl, "p_k"] \\ M_k & \end{tikzcd}$$

**Demostração:** De início vamos mostrar que a existência, ou seja, considere a aplicação

$f : N \to M$ definida do seguinte modo $f(n) = (q_i(n))_{i\in I}$, para todo $n \in N$, daí dado $n_1, n_2 \in N$ e $a \in A$, tem-se

[I]

$$\begin{aligned} f(n_1+n_2) &= (q_i(n_1+n_2))_{i\in I} \\ &= (q_i(n_1)+q_i(n_2))_{i\in I} \\ &= (q_i(n_1)) + (q_i(n_2))_{i\in I} \\ &= f(n_1)+f(n_2) \end{aligned}$$

[II]

$$\begin{aligned} f(an_1) &= (q_i(an_1))_{i\in I} \\ &= (aq_i(n_1))_{i\in I} \\ &= a(q_i(n_1))_{i\in I} \\ &= af(n_1) \end{aligned}$$

Logo f é um A-homomorfismo. Agora iremos que $p_k \circ f = q_k$, para todo $k \in I$. De fato, pois dado $n \in N$, temos

$$\begin{aligned} (p_k \circ f)(n) &= p_k(f(n)) \\ &= p_k(q_i(n))_{i\in I} \\ &= q_k \end{aligned}$$

Resta mostrar a unicidade, assim, suponha que exista um A-homomorfimo $g : N \to M$, que associa a todo $n \in N$ a um elemento $(g_i(n))_{i\in I}$ em M, tal que $p_k \circ f = q_k$, para todo $k \in I$, daí mostraremos que $f = g$.

De fato, pois aplicando $p_k$ em $g(n) = (g_i(n))_{i\in I}$, temos

$$g(n) = (g_i(n))_{i\in I} \Longrightarrow p_k(g(n)) = p_k(g_i(n))_{i\in I} \Longrightarrow (p_k \circ g)(n) = g_k(n) \Longrightarrow q_k(n) = g_k(n).$$

Portanto, como $q_k = g_k$, logo

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

Portanto, $f = g$.

$\square$

**Definição 2.0.5.4:** *Seja* $\{M_i\}_{i\in I}$ *uma família de A-módulos e* $M = \prod_{i\in I} M_i$. *Uma família* $(m_i)_{i\in I} \in M$ *diz-se uma família quase nula se* $m_i = 0_M$, *exceto para um número finito de índices.*

### 2.0.6 Soma Direta

**Definição 2.0.6.1:** *Seja* $\{M_i\}_{i\in I}$ *uma família de A-módulos. O conjunto das famílias quase nulas de* $M = \prod_{i\in I} M_i$, *com a estrutura de de A-módulos definidas pela restrição de operações de M, chama-se de soma direta externa da família e indicaremos pleo simbolo*

$$\sum_{i\in I} M_i$$

Se o conjunto de índices for finito $I = \{1, 2, 3, ..., n\}$, denotaremos por

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

**Observação:** Note que a partir da definição citada, podemos garantir que a soma direta externa de uma família de A-módulos é um submódulo do produto direto.

De fato, basta considerar a partir de uma quantidade finita de índices, ou seja, dado $0 \in M_i$, para todo $i \in I$, assim temos

[I] $0 \in \sum_{i\in I} M_i$ pois $m_i = 0$, exceto para um número finito de índices, em que este número é zero.

[II] Dados $(m_i)_{i\in I} \in \sum_{i\in I} M_i$ e $(s_i)_{i\in I} \in \sum_{i\in I} M_i$, daí temos

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

[III] Dado um $\lambda \in A$ e um $(m_i)_{i\in I} \in \sum_{i\in I} M_i$, sendo $\lambda$ uma escalar de família quase nula de M, temos

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

Portanto, concluimos que é submódulo.

**Observação:**E também temos que $\sum_{i\in I} M_i = \prod_{i\in I} M_i$, se o conjunto de índices for finito.

Como feito no produto direto, na soma direta é possível definir as inclusões naturais como sendo $i_k : M_k \to \sum_{i\in I} M_i$, onde $i_k(m_k) = (x_i)_{i\in I}$, com $x_k = m_k$ e $x_i = 0$ se $i \neq k$. Ja as projeções sobre as componentes, podemos definir como $p_k : \sum_{i\in I} M_i \to M_k$, onde $p_k(m_i)_{i\in I} = m_k$.

**Proposição 2.0.6.2:** Sejam $p_k$ as projeções sobre as componentes e $i_k$ as inclusões naturais, então é válido

I - $p_k \circ i_k = Id_{M_k}$, para todo $k \in I$

II - $p_k \circ i_h = 0$, para todo $h, k \in I$ tal que $h \neq k$

**Demostração:** Idêntica a demostração feita no produto direto.

$\square$

**Proposição 2.0.6.3:** Seja $\{M_i\}_{i\in I}$ uma família de A-módulos, dado $M = \sum_{i\in I} M_i$ e $i_k : M_k \to M$, como sendo a inclusões naturais. Um A-módulo N e uma família de A-homomorfismo $h_k : M_k \to N$, existe um único A-homomorfismo $f : M \to N$, tal que $h_k = f \circ i_k$, para todo $k \in I$, o diagrama a seguir é comutativo.

$$\begin{tikzcd} M \arrow[r, "f"] & N \\ M_k \arrow[u, "i_k"] \arrow[ur, "h_k"'] & \end{tikzcd}$$

**Demostração:** De ínicio, iremos definir $f : M \to N$, do seguinte modo

$$(m_i)_{i\in I} \to f((m_i)_{i\in I}) = \textstyle\sum_{k\in I} h_k(m_k), \text{ para todo } (m_i)_{i\in I} \in M$$

A partir daí, agora mostraremos que f é um A-homomorfismo. Sejam $(m_i)_{i\in I}$,$(p_i)_{i\in I} \in M$ e $\lambda \in A$, temos

[I]

$$\begin{aligned} f((m_i)_{i\in I} + (p_i)_{i\in I}) &= f((m_i + p_i)_{i\in I})) \\ &= \sum_{k\in I} h_k(m_k + p_k) \\ &= \sum_{k\in I} [h_k(m_k) + h_k(p_k)] \\ &= \sum_{k\in I} h_k(m_k) + \sum_{k\in I} h_k(p_k) \\ &= f((m_i)_{i\in I}) + f((p_i)_{i\in I}) \end{aligned}$$

[II]

$$
\begin{aligned}
f(\lambda(m_i)_{i\in I}) &= f((\lambda m_i)_{i\in I}) \\
&= \sum_{k\in I} h_k(\lambda m_k) \\
&= \sum_{k\in I} \lambda h_k(m_k) \\
&= \lambda \sum_{k\in I} h_k(m_k) \\
&= \lambda f((m_i)_{i\in I})
\end{aligned}
$$

Portanto, f é um A-homomorfismo. Agora iremos mostra que $h_k = f \circ i_k$, para todo $k \in I$. Ou seja, dado $m_k \in M_k$, temos

$$
\begin{aligned}
(f \circ i_k)(m_k) &= f(i_k(m_k)) \\
&= f(0,0,0,...,m_k,0,...) \\
&= \sum_{i\in I} h_i(m_i) \\
&= h_1(0) + h_2(0) + ... + h_k(m_k) + ... \\
&= 0 + 0 + ... + h_k(m_k) + ... \\
&= h_k(m_k)
\end{aligned}
$$

Então, resta mostrar a unicidade, dessa forma, suponha que exista um A-homomorfismo $g : M \to N$, tal que $h_k = g \circ i_k$, para todo $k \in I$. Com efeito, seja $(m_i)_{i\in i}$, temos

$$
\begin{aligned}
g((m_i)_{i\in i}) &= g(\sum_{k\in I} i_k(m_k) \\
&= \sum_{k\in I} g(i_k(m_k)) \\
&= \sum_{k\in I} (g \circ i_k)(m_k) \\
&= \sum_{k\in I} h_k(m_k) \\
&= f((m_i)_{i\in I})
\end{aligned}
$$

Logo, $f = g$

□

**Definição 2.0.6.4:** *Dizemos que uma família de submódulos $\{M_i\}_{i\in I}$ de um A-*

*módulo M é independente se para todo i, temos*

$$M_i \cap (M_1 + M_2 + ... + M_{i-1} + M_{i+1} + ... + M_n) = \{0\}$$

**Proposição 2.0.6.5:** Uma família de submódulos $\{M_i\}_{i\in I}$ de um A-módulo M é independente, se e somente se,

$$\sum_{i\in I} m_i = 0, \text{ com } m_i \in M, \text{ tem-se } m_i = 0, \forall i \in I$$

**Demostração:**

($\Longrightarrow$) De fato, como $\sum_{i\in I} m_i = 0$, temos

$$m_1 + ... + m_{i-1} + m_i + m_{i+1} + ... + m_n = 0 \Longrightarrow m_i = -(m_1 + ... + m_{i-1} + m_i + m_{i+1} + ... + m_n)$$

Então, $m_i \in M_1 + ... + M_{i-1} + M_i +_{i+1} +... + M_n$, mas também temos que $m_i \in M_i$, dessa forma

$$m_i \in M_i \cap (M_1 + M_2 + ... + M_{i-1} + M_{i+1} + ... + M_n) = \{0\}$$

Note que, por hipótese, temos que a família $\{M_i\}_{i\in I}$ é independente, logo

$$M_i \cap (M_1 + M_2 + ... + M_{i-1} + M_{i+1} + ... + M_n) = \{0\}$$

Dessa forma, temos que $m_i = 0, \forall i \in I$.

($\Longleftarrow$) Seja $m_i \in M_i \cap (M_1 + M_2 + ... + M_{i-1} + M_{i+1} + ... + M_n)$, mostraremos que $m_i = 0$.

De fato, se $m_i \in M_i \cap (M_1 + M_2 + ... + M_{i-1} + M_{i+1} + ... + M_n)$, temos que $m_i \in M_i$ e $m_i \in (M_1 + M_2 + ... + M_{i-1} + M_{i+1} + ... + M_n)$, dessa forma

$$m_i = m_1 + ... + m_{i-1} + m_i + m_{i+1} + ... + m_n \Longrightarrow m_1 + ... + m_{i-1} + (-m_i) + m_i + m_{i+1} + ... + m_n = 0 \Longrightarrow \sum_{i\in I} m_i = 0$$

Daí, por hipótese, temos que $m_i = 0, \forall i \in I$.

Portanto, $M_i \cap (M_1 + M_2 + ... + M_{i-1} + M_{i+1} + ... + M_n) = \{0\}$, logo a família $\{M_i\}_{i\in I}$ é independente.

$\square$

**Proposição 2.0.6.6:** Seja $\{M_i\}_{i\in I}$ uma família de submódulos de A-módulo M. As seguintes afirmações são equivalentes

I - Todo elemento $m \in M$ se escreve de um único modo na forma $M = \sum_{i\in I} M_i$, onde $m_i \in M$, para todo $i \in I$ e a família $(m_i)_{i\in I}$ é quase nula.

II - Dado $M = \sum_{i\in I} M_i$, se $\sum_{i\in I} M_i = 0$, com $m_i \in M_i$, tem-se que $m_i = 0$, para todo $i \in I$.

III - seja $M = \sum_{i\in I} M_i$, então $M_i \cap \sum_{i\neq j} M_j = 0$.

**Demostração:**

[I] $\Longrightarrow$ [II] Suponha que $M = \sum_{i\in I} M_i$, daí considere a função $h : \sum_{i\in I} M_i \to M$ definida por $h((m_i)_{i\in I}) = \sum_{i\in I} m_i$. Agora suponha um $m \in M$ qualquer, note que existe um único $m_i \in M_i$, talque $m = \sum_{i\in I} m_i$, assim

$$h((m_i)_{i\in I}) = \sum_{i\in I} m_i = m$$

Daí, se $(m_i)_{i\in I} \in Ker(h)$, dessa forma, temos

$$h((m_i)_{i\in I}) = \sum_{i\in I} m_i = 0_M$$

Consequentemente, $m_i = 0_M$, para todo $i \in I$.

[II] $\Longrightarrow$ [III] Seja $m \in M_i \cap \sum_{i\neq j} m_j$ qualquer, assim $m \in M_i$ e $m \in \sum_{i\neq j} m_j$. Daí, se $m \in \sum_{i\neq j} m_j$, existe $m \in M_j$, com $j \neq i$, talque $m = \sum_{i\neq j} m_j$. Dessa forma

$$m = \sum_{i\neq j} m_j \Longrightarrow \sum_{i\neq j} m_j + (-m) = 0_M$$

ou seja, $m_j = 0_M$ para todo $j \neq i$ e em particular $m = 0_M$.

[III] $\Longrightarrow$ [I] Dada a condição $M = \sum_{i\in I} M_i$, vem que todo elemento $m \in M$ pode ser escrito da seguinte forma $m = \sum_{i\in I} m_i$, onde $m_i \in M_i$ para todo $i \in I$ e a família $(m_i)_{i\in I}$ é quase nula. Daí resta verificar a unicidade, ou seja, considere $\sum_{i\in I} M_i = \sum_{i\in I} n_i$. Note que para todo $j \in I$, temos

$$m_i + \sum_{i\neq j} m_j = n_i + \sum_{i\neq j} m_j \Longrightarrow m_i - n_i = \sum_{i\neq j}(m_j - n_i)$$

Logo, $m_j - n_i \in M_i \cap \sum_{i\neq j} M_j$, assim $m_i = n_i$.

$\square$

**Definição 2.0.6.7:** *Um A-módulo M diz-se uma soma direta interna de uma família* $\{M_i\}_{i\in I}$ *de submódulo se verifica uma das condições equivalentes citadas na proposição anterior e indicaremos pelo símbolo*

$$M = \bigoplus_{i\in I} M_i$$

e se o conjunto $I = \{1, 2, 3, ..., n\}$ de índices for finito, notaremos por

$$M = M_1 \oplus M_2 \oplus ... \oplus M_n$$

Note que os conceitos de soma direta interna são bem familiarizados pelo espaços vetorias. Ou seja, um A-módulo M é uma soma direta interna de uma família $\{M_i\}_{i\in I}$ de submódulos se todo elemento de M se escreve, de uma única forma, como a soma de elementos dos submódulos de $M_i$.

**Exemplo 2.0.6.8:** Para qualquer A-módulo M, tem-se sempre que $M = M \oplus 0$. Os submódulos M e 0 dizem-se soma direta trivial.

**Exemplo 2.0.6.9:** Considere 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 $H_2 = \{\overline{0}, \overline{3}\}$, tais que $H_1 \cap H_2 = 0$. Note que

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

Ou seja, podemos escrever $\mathbb{Z}_6 = H_1 + H_2$, portanto $\mathbb{Z}_6 = H_1 \oplus H_2$.

**Proposição 2.0.6.10:** Seja M um A-módulo e um $\{M_i\}_{i\in I}$ uma família de submódulos tais que $M = \bigoplus_{i\in I} M_i$. Então

$$\bigoplus_{i\in I} M_i \simeq \sum_{i\in I} M_i$$

**Demostração:** Considere a função

$$\begin{aligned}
f : \sum_{i\in I} Mi &\longrightarrow \bigoplus_{i\in I} M_i \\
(m_i)_{i\in I} &\longrightarrow f((m_i)_{i\in I}) = m_1 + m_2 + ... + m_n
\end{aligned}$$

Note que f é um A-homomorfismo, pois dados $(m_i)_{i\in I}$ e $(s_i)_{i\in} \in \sum_{i\in I} M_i$ e $a \in A$, temos

[I]

$$
\begin{aligned}
f((m_i)_{i\in I} + (s_i)_{i\in I}) &= f((m_i + s_i)_{i\in I}) \\
&= (m_1 + s_1) + ... + (m_n + s_n) \\
&= (m_1 + m_2 + ... + m_n) + (s_1 + s_2 + ... + s_n) \\
&= f((m_i)_{i\in I}) + f((s_i)_{i\in I})
\end{aligned}
$$

[II]

$$
\begin{aligned}
f(a(m_i)_{i\in I}) &= f((am_i)_{i\in I}) \\
&= am_1 + am_2 + ... + am_n \\
&= a(m_1 + m_2 + ... + m_n) \\
&= af((m_i)_{i\in I})
\end{aligned}
$$

Mostraremos que f é epimorfismo e monomorfismo. Assim, dado um $m \in \bigoplus_{i\in I}$, então $m = m_1 + m_2 + ... + m_n$. Considere $(m_1, m_2, ..., m_n) \in \sum_{i\in I} M_i$, aplicando a f temos

$$f(m_1, m_2, ..., m_n) = m_1 + m_2 + ... + m_n \Longrightarrow f(m_1, m_2, ..., m_n) = m$$

Logo concluimos que é epimorfismo. seja Ker(f) da seguinte forma

$$Ker(f) = \{(m_1, m_2, ..., m_n) \in \textstyle\sum_{i\in I} M_i, f(m_1, m_2, ..., m_n) = 0$$

Isso implica que

$$f(m_1, m_2, ..., m_n) = 0 \Longrightarrow (m_1 + m_2 + ... + m_n) = 0 \Longrightarrow \textstyle\sum_{i\in I} m_i = 0$$

Como a família $\{M_i\}_{i\in I}$ é independente, segue que $m_i = 0, \forall i \in I$. Dessa forma

$$Ker(f) = \{0, 0, 0, ..., 0)\}$$

Logo, como f é ao mesmo tempo epimorfismo e monomorfismo, temos que f é um isomorfismo.

□

**Definição 2.0.6.11:** *Seja N um submódulo de um A-módulo. Dizemos que um submódulo $N_1 \in M$ é suplementar de N, se $M = N_1 \oplus N$. Assim, se um submódulo, que admiti um suplementar, chamaremos de somando direto de M.*

**Observação:** Em álgebra linear, demostra que todo subespaço vetorial é um somando direto. Porém, em módulo, isso nem sempre é verdade, por exemplo, considere $\mathbb{Z}$ como sendo um $\mathbb{Z}$-Módulo, dai note que $\mathbb{Z} \oplus \mathbb{Z}$ não tem somando direto trivial. De fato, pois supondo que $m\mathbb{Z}$ seja um somando direto não trivial de $\mathbb{Z} \oplus \mathbb{Z}$, dai existe um $n\mathbb{Z}$, tal que

$$\mathbb{Z} = m\mathbb{Z} \oplus n\mathbb{Z}, \text{ com } m, n \in \{0, \pm 1\}$$

Mas, $m.n \in m\mathbb{Z} \cap n\mathbb{Z} = \{0\}$, por $m\mathbb{Z}$ e $n\mathbb{Z}$ serem independente. Dai, segue que $m.n = 0$, absurdo, pois $m, n \neq$.

Ja por outro lado, temos que se N é um somando direto de um A-módulo M, o seu complemento não é, em geral, único. De fato, pois considere $\mathbb{R}^2$ como sendo um $\mathbb{R}$-Módulo, o submódulo $N = \{(a, 0), a \in \mathbb{R}\}$. Obeserve que qualquer submódulo da forma $S = \{(a, ma), a \in \mathbb{R}, m \neq 0\}$ é um suplementar de N, pois podemos escrever todo par $(a, b) \in \mathbb{R}^2$, sendo

$$(a, b) = (a - \tfrac{b}{m}, 0) + (\tfrac{b}{m}, b) \in N + S$$

Logo, para todo $m \neq 0$, temos que existe um submódulo P que é suplementar de N, ou seja, o suplementar não é único.

**Proposição 2.0.6.12:** Seja M um A-módulo e $N_1$ e $N_2$ submódulos, tais que $M = N_1 \oplus N_2$. Então, $\frac{M}{N_1} \simeq N_2$.

**Demostração:** Defina um função da seguinte forma $f : M \to N_2$. Dado $m \in M$, logo podemos escrever, de forma única, $m = n_1 + n_2$, com $n_1 \in N_1$ e $n_2 \in N_2$. Assim, $f(m) = f(n_1 - n_2) = n_2$. Mostraremos que f é um A-homomorfismo, ou seja, dados $m = (n_1 + n_2)$, $s = (s_1 + s_2) \in M$ e $a \in A$, então

[I]

$$\begin{aligned} f(m+s) &= f[(n_1+n_2)+(s_1+s_2)] \\ &= f[(n_1+s_1)+(n_2+s_2)] \\ &= n_2+s_2 \\ &= f(n_1+n_2)+f(s_1+s_2) \\ &= f(m)+f(s) \end{aligned}$$

[II]

$$
\begin{aligned}
f(am) &= f(a(n_1 + n_2)) \\
&= f(an_1 + an_2) \\
&= an_2 \\
&= af(n_1 + n_2) \\
&= af(m)
\end{aligned}
$$

Logo, f é um A-homomorfismo. Usando o teorema do A-homomorfismo para módulos, temos que

$$\frac{M}{Ker(f)} \simeq Im(f)$$

como,

$$
\begin{aligned}
Ker(f) &= \{m \in M, f(m) = 0\} \\
&= \{(n_1 + n_2) \in M, f(n_1 + n_2) = 0\} \\
&= \{(n_1 + n_2) \in M, n_2 = 0\} \\
&= \{n_1 \in M, n_1 \in N_1\} \\
&= N_1
\end{aligned}
$$

e

$$
\begin{aligned}
Im(f) &= \{f(m), m \in M\} \\
&= \{f(n_1 + n_2), n_1 \in N_1, n_2 \in N_2\} \\
&= \{n_2, n_2 \in N_2\} \\
&= N_2
\end{aligned}
$$

Logo, fazendos as substituições

$$\frac{M}{N_1} \simeq N_2$$

□

**Colorário 2.0.6.13:** Dois suplementos de um mesmo submódulos são isomorfos.

**Demostração:** Sejam S e P dois suplementos de um submódulo N de um A-módulo M, então temos que

$$M = N \oplus S \text{ e } M = N \oplus P$$

Pela preprosição anterior, temos

$$\frac{M}{N} \simeq S \text{ e } \frac{M}{N} \simeq P$$

Logo, por transitividade, temos $S \simeq P$.

### 2.0.7 Sequências Exatas

**Definição 2.0.7.1:** *Sejam F, G, H A-módulos e $f : F \to G$ e $g : G \to H$ A-homomorfismos. Dizemos que o diagrama a seguir*

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

é uma sequência exata de ordem 2 em G se $Im(f) \subset Ker(f)$. Em particular, se $Im(f) = Ker(f)$ o diagrama chama-se de sequência exata em G.

**Definição 2.0.7.2:** *Sejam $\{..., M_{i-1}, M_i, M_{i+1}, ...\}$ uma família infinita de A-módulos e $\{..., F_i : M_{i-1} \to M_i, ...\}$ um família de A-homomorfismo. Dizemos que o diagrama*

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

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

**Exemplo 2.0.7.3:** A sequência $0 \longrightarrow E \xrightarrow{f} F$ é exata, se e somente se, f é um A-monomorfismo.

De fato, note que como 0 é um A-homomorfismo nulo, daí temos que $Im(0) = Ker(0) = \{0\}$. Assim, f é um monomorfismo $\Longleftrightarrow Ker(f) = 0 = Im(g) \Longleftrightarrow$ a sequência é exata.

**Exemplo 2.0.7.4:** A sequência $E \xrightarrow{f} F \longrightarrow 0$ é exata, se somente se, f é um A-epimorfismo.

Note que 0 é um A-homomorfismo nulo, pois $0(x) = 0$, para todo x ∈ F. Assim, determinamos do seguinte modo

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

$$\begin{aligned} Ker(0) &= \{x \in F, 0(x)\} \\ &= F \end{aligned}$$

Daí, temos que $0 \circ f : E \to 0$, definida por $(0 \circ f)(x) = 0$ é um homomorfismo nulo. Dessa forma, f é um epimorfismo $\Longleftrightarrow Im(f) = f = Ker(f) \Longleftrightarrow$ a sequência é exata.

**Exemplo 2.0.7.5:** Diante das sequêcias ja apresentada, de imediato vem sequência $0 \longrightarrow E \xrightarrow{f} F \longrightarrow 0$, que é uma sequência exata se, e somente se, f é um isomorfismo.

De fato, pois ja mostramos que f é monomorfismo(injetiva) e epimorfismo(sobrejetiva), ou seja, f é isomorfismo(bijetora).

**Exemplo 2.0.7.6:** A sequência $0 \xrightarrow{0} M \xrightarrow{f} 0$ é uma sequência exata se, e somente se, $M = \{0\}$.

Note que 0 é um A-homomorfismo nulo, daí temos $Im(0) = Ker(0) = 0$. Logo temos que $f : M \to 0$, definida por $f(x) = 0$, para todo x $\in$ M. Assim, f é um A-homomorfismo nulo, logo a $Im(f) = 0$ e $Ker(f) = 0$, então

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

**Exemplo 2.0.7.7:** A sequência $0 \longrightarrow 2\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{w} \mathbb{Z}_2 \longrightarrow 0$, onde $i : 2\mathbb{Z} \to \mathbb{Z}$ é a inclusão e $w : \mathbb{Z} \to \mathbb{Z}_2$ a aplicação que cada inteiro associa a sua classe em $\mathbb{Z}_2$, é uma sequência exata.

Note que i é um monomorfismo, logo a sequência é exata em $2\mathbb{Z}$, também temos que w é um epimorfismo, logo a sequência é exata em $\mathbb{Z}_2$. Daí resta mostrar que é exata em $\mathbb{Z}$, de fato

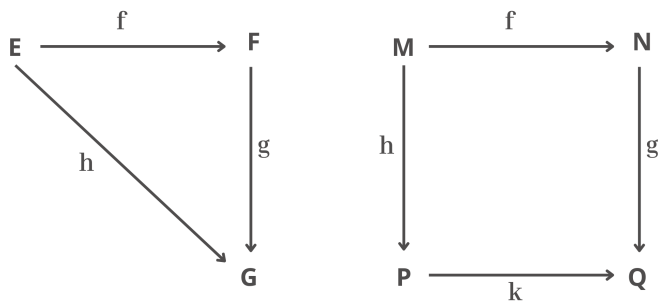
$$\begin{aligned} Im(i) &= \{i(x), x \in 2\mathbb{Z}\} \\ &= \{x, x \in 2\mathbb{Z}\} \\ &= 2\mathbb{Z} \end{aligned}$$

$$\begin{aligned} Ker(w) &= \{x \in \mathbb{Z}, w(x) = 0\} \\ &= \{x \in \mathbb{Z}, \overline{x} = 0\} \\ &= \{x \in \mathbb{Z}, x \in 2\mathbb{Z}\} \\ &= 2\mathbb{Z} \end{aligned}$$

Portanto, como $Im(i) = Ker(w)$, temos que a sequência é exata.

**Definição 2.0.7.8:** *Dizemos que uma família de A-módulos $\psi$ e uma família de A-homomorfismo $\phi$ forma um diagrama comutativo, se para todo par de módulo $M,N \in \psi$ e todo par de A-homomorfismo $f,g \in \phi$, tais que $f : M \to N$ e $g : M \to N$, então $f = g$.*

**Exemplo 2.0.7.9:** considere o diagrama a seguir




O primeiro diagrama será comutativo se $h = g \circ f$, de maneira análoga, o segundo diagrama será comutativo se $g \circ f = k \circ h$.

**Definição 2.0.7.10:** *Dizemos que uma sequência exata de A-módulo*

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

*cinde se $E' = Im(f) = Ker(f)$ é um somando direto de F.*

**Proposição 2.0.7.11:** Seja uma sequência exata de A-módulo

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

as seguintes afirmações a seguir são equivalentes

I - A sequência cinde

II - Existe um A-homomorfismo $\pi : F \to E$ tal que $\pi \circ f = Id_E$

III - Existe um A-homomorfismo $\beta : G \to F$ tal que $g \circ \beta = Id_G$

Nestas condições $F \simeq E \oplus G$.

**Demostração:**

[I] $\Longrightarrow$ [II] De fato, pois escrevendo $E' = Im(f)$ e como a sequência cinde, então existe um submódulo $E''$ de F tal que $F = E' \oplus E''$. Assim, dado um $m \in F$, podemos escrever $m = m' + m''$, como sendo $m' \in E'$ e $m'' \in E''$, note que f é injetora pelo fato da sequência ser exata, daí existe um único $x \in E$ tal que $f(x) = m'$, então

$$m = m' + m'' \Longrightarrow m = f(x) + m''$$

Dai, podemos definir $\pi$ da seguinte forma:

$$\begin{aligned} \pi : F &\longrightarrow E \\ m &\longrightarrow \pi(f(x) + m'') = x \end{aligned}$$

Agora mostraremos que $\pi$ é um A-homomorfismo.

De fato, seja $m_1 = f(x_1) + m_1''$ e $m_2 = f(x_2) + m_2'' \in F$ e $a \in A$. Então temos que

[I]

$$\begin{aligned} \pi(m_1 + m_2) &= \pi[(f(x_1) + m_1'') + (f(x_2) + m_2'')] \\ &= \pi[(f(x_1) + f(x_2)) + (m_1 + m_2'')] \\ &= \pi[(f(x_1 + x_2)) + (m_1 + m_2'')] \\ &= x_1 + x_2 \\ &= \pi(f(x_1) + m_1'') + \pi(f(x_2) + m_2'') \\ &= \pi(m_1) + \pi(m_2) \end{aligned}$$

[II]

$$\begin{aligned} \pi(am_1) &= \pi(a(f(x_1) + m_1'')) \\ &= \pi(af(x_1) + am_1'') \\ &= \pi(f(ax_1) + am_1'') \\ &= ax_1 \\ &= a\pi(f(x_1) + m_1'') \\ &= \pi(m_1) \end{aligned}$$

Logo, podemos concluir que por I e II, $\pi$ é um A-homomorfismo. Agora iremos mostrar que $\pi \circ f = Id_E$.

Seja $x \in E$, então$f(x) \in E'$, logo

$$\begin{aligned}(\pi \circ f)(x) &= \pi(f(x))\\ &= \pi(f(x)+0)\\ &= x\\ &= Id_E\end{aligned}$$

Logo, $\pi \circ f = Id_E$

[II] $\Longrightarrow$ [I] Mostraremos que $F \simeq Im(f) \oplus Ker(\pi)$.

(i) $F = Im(f) + Ker(\pi)$.

Sejam $m \in F$, temos que $\pi(m) \in E$, então $f(\pi(m)) \in Im(f)$. Assim, $(m - f(\pi(m))) \in F$, aplicando a $\pi$ neste elemento temos

$$\begin{aligned}\pi(m - f(\pi(m))) &= \pi(m) - \pi(f(\pi(m)))\\ &= \pi(m) - (\pi \circ f)(\pi(m))\\ &= \pi(m) - Id_E(\pi(m))\\ &= \pi(m) - \pi(m)\\ &= 0\end{aligned}$$

Portanto, $(m - f(\pi(m))) \in Ker(\pi)$. Logo podemos escrever

$$m = f(\pi(m)) + (m - f(\pi(m))) \in Im(f) + Ker(\pi)$$

Portanto, $F = Im(f) + Ker(\pi)$.

(ii) A família $\{Im(f), Ker(pi)\}$ é independente.

Seja $x \in Im(f) \cap Ker(\pi)$, então existe um $y \in E$ tal que $f(y) = x$ e também

$$\pi(x) = o \Longrightarrow \pi(f(y)) = 0 \Longrightarrow (\pi \circ f)(y) = 0 \Longrightarrow Id_E(y) = 0 \Longrightarrow y = 0.$$

logo

$$x = f(y) \Longrightarrow x = f(0) \Longrightarrow x = 0.$$

Portanto, concluimos que é independente. Dessa forma, por (i) e (ii), temos que $F = Im(f) \oplus Ker(\pi)$, assim é cinde.

[I] $\Longrightarrow$ [III] De fato, pois escrevendo $E' = Ker(g)$ e como a sequência é cinde, existe um submódulo $E''$ de F tal que $F = E' \oplus E''$. Dessa forma, seja um $y \in G$, como g é sobrejetora, pois ja que a sequência é exata, existe uma $x \in F$ tal que $g(x) = y$. Também note que se x se escreve de uma única maneira como $x = x' + x''$, com $x' \in E'$ e $x'' \in E''$. Dai,

$$\begin{aligned} y &= g(x) \\ &= g(x' + x'') \\ &= g(x') + g(x'') \\ &= 0 + g(x'') \\ &= g(x'') \end{aligned}$$

Então daí, podemos definir $\beta$ como

$$\begin{aligned} \beta : G &\longrightarrow F \\ y &\longrightarrow \beta(g(x'')) = x'' \end{aligned}$$

Vamos mostrar que $\beta$ é um A-homomorfismo.

De fato, Sejam $y_1$,$y_2 \in G$, existem $x_1''$ e $x_2'' \in F$ tal que $y_1 = g(x_1'')$ e $y_2 = g(x_2'')$ e $a \in A$. Dai, temos que

[I]

$$\begin{aligned} \beta(y_1 + y_2) &= \beta(g(x_1'') + g(x_2'')) \\ &= \beta(g(x_1'' + x_2'')) \\ &= x_1'' + x_2'' \\ &= \beta(g(x_1'')) + \beta(g(x_2'')) \\ &= \beta(y_1) + \beta(y_2) \end{aligned}$$

[II]

$$\begin{aligned}
\beta(ay_1 &= \beta(ag(x_1''))\\
&= \beta(g(ax_1''))\\
&= ax_1''\\
&= a\beta(g(x_1''))\\
&= a\beta(y_1)
\end{aligned}$$

Logo, por (i) e (ii), temos que $\beta$ é um A-homomorfismo. Agora mostraremos que $g \circ \beta = Id_G$.

De fato, Seja $y \in G$, existe um $x'' \in F$ tal que $g(x'') = y$. assim,

$$\begin{aligned}
(g \circ \beta)(y) &= g(\beta(y))\\
&= g(\beta(g(x'')))\\
&= g(x'')\\
&= y\\
&= Id_G(y)
\end{aligned}$$

Logo, podemos concluir que $g \circ \beta = Id_G$.

[III] $\Longrightarrow$ [I] Inicialmente, vamos mostrar que $F = Ker(g) \oplus Im(\beta)$, ou seja, mostraremos:
(i) $F = Ker(g) + Im(\beta)$.

De fato, seja $x \in F$, então $g(x) \in G$, logo $\beta(g(x)) \in Im(\beta)$. Assim, $(x - \beta(g(x)) \in F$, dai aplicando g, temos que

$$\begin{aligned}
g(x - \beta(g(x))) &= g(x) - g(\beta(g(x)))\\
&= g(x) - (g \circ \beta)(g(x)))\\
&= g(x) - Id_G(g(x)))\\
&= g(x) - g(x)\\
&= 0
\end{aligned}$$

Dessa forma,$(x - \beta(g(x))) \in Ker(g)$ . Logo, podemos escrever

$$m = \beta(g(x)) + (x - \beta(g(x))) \in Im(\beta) + Ker(g)$$

Portanto, concluimos que $F = Ker(g) + Im(\beta)$.

(ii) A família $\{Im(\beta), Ker(g)\}$ é independente.

Seja $y \in Im(\beta) \cap Ker(g)$, então $y \in Im(\beta)$ e $y \in Ker(g)$. Assim,$y \in Im(\beta)$ implica que existe um $x \in G$ tal que $\beta(x) = y$ e como $y \in Ker(g)$, temos

$$g(y) = 0 \Longrightarrow g(\beta(x)) = 0 \Longrightarrow (g \circ \beta)(x) = 0 \Longrightarrow Id_G(x) = 0 \Longrightarrow x = 0$$

Logo,

$$y = \beta(x) \Longrightarrow y = \beta(0) \Longrightarrow y = 0$$

Portanto, a família $\{Im(\beta), Ker(g)\}$ é independente. Assim, por (i) e (ii) temos que $F = Ker(g) \oplus Im(\beta)$.

Diante disso tudo, temos que $\pi \circ f = Id_E$ e $g \circ \beta = Id_G$, temos que f e $\beta$ são injetoras, assim, aplicando o teorema do homomorfismo para módulos, temos

$$E \simeq \frac{E}{Ker(f)} \simeq Im(f) \text{ e } G \simeq \frac{G}{Ker(\beta)} \simeq Im(\beta)$$

Portanto,

$$E \simeq Im(f) = Ker(g) \text{ e } G \simeq Im(\beta)$$

Logo,

$$F \simeq E \oplus G \text{ pois } F = Ker(g) \oplus Im(\beta)$$

□

# 3 MÓDULOS LIVRES

Um módulo livre sobre um anel A é um tipo especial de módulo que possui uma base, ou seja, um conjunto de elementos linearmente independente e que gera todo módulo por meio de uma conbinação linear com coeficientes em A. Assim, cada elemento do módulo pode ser representado de um forma única como uma conbinação dos elementos da base. Dessa forma, inicialmente para o estudo desse capítulo, introduziremos alguns definições importantes no estudos de módulos livres, exemplos, algumas propriedades que são válidas em espaços vetorias, mas não são em módulo livre, proprosições e colorários.

### 3.0.1 Módulos Livres

Dado um anel A, denotaremos por $A^{(I)} = \sum_{i \in I} A_i$ como sendo a soma direta de A, onde $A_i = A, \forall i \in I$. Dessa forma, $A^{(I)}$ é o conjunto das famílias quases nulas $(\lambda_i)_{i \in I}$ com $\lambda_i \in A, \forall i \in I$.

**Definição 3.0.1.1:** *Seja $\{m_i\}_{i \in I}$ uma família de elementos de um A-módulo. Dizemos que um elemento $m \in M$ é uma conbinação lienar dos elementos desta família se existir $(\lambda_i)_{i \in I}$ tal que*

$$m = \sum_{i \in I} \lambda_i m_i$$

Note que, a soma acima faz sentido, pois além de ser uma soma finita, temos que as famílias $\{m_i\}_{i \in I}$ são quase nulas.

**Definição 3.0.1.2:** *Diremos que uma família $\{m_i\}_{i \in I}$ de elementos de um A-módulo M diz-se linearmente independente(LI) ou livre se para todo $(\lambda_i)_{i \in I} \in A^{(I)}$ tem-se*

$$\sum_{i \in I} \lambda_i m_i = 0 \Longrightarrow \lambda_i = 0, \forall i \in I$$

*E se uma família não é linearmente independente, diremos que essa família é linearmente dependente (LD).*

**Definição 3.0.1.3:** *Diremos que um subconjunto $R = \{m_i\}_{i \in I}$ de elementos de um A-módulo M, é um gerador de M, se todo elemento de M for uma conbinação linear de elementos de R.*

**Definição 3.0.1.4:** *Uma família $\{m_i\}_{i \in I}$ de elementos de um A-módulo M. Diz-se que é uma base se é linearmente independente e gera M.*

**Definição 3.0.1.5:** *Um A-módulo M di-se livre se existe uma base para M.*

**Exemplo 3.0.1.6:** Todo espaço vetorial sobre um corpo K, é um K-módulo livre.

De fato, pois todo espaço vetorial sobre um copro K possui uma base, logo se possui uma base é um K-módulo livre.

**Exemplo 3.0.1.7:** Seja A um anel comutativo com unidade, então o A-módulo ${}_AA$( A-módulo à esquerda) é livre e o conjunto $\{1\}$ é uma base desse A-módulo. Mas, geralmente, $\{w\}$ é base de A, se e somente se, $w$ é um elemento inversível de de A.

Note que, qualquer conjunto da forma ${}_AA$ com mais de um elemento não pode ser uma base, pois não é LI. De fato, consideramos uma família $X \subset {}_AA$ com mais de um elemento. Dados $a, b \in X$, a conbinação linear $ba + (-a)b = 0$ e $(-a), b \in A$, ambos não são nulos, logo são LD. Ou seja, a base do A-módulo ${}_AA$ so pode ser da forma $\{w\}$, com $w \in A$ e se $w$ for um elemento inversível de A.

De fato, pois $\{w\}$ sendo uma base de A, então $x \in A$, existe um $\lambda \in A$, tal que

$$x = \lambda w$$

Dai, tomando $x = 1$, temos que existe um $\lambda_1 \in A$ tal que

$$1 = \lambda_1 w$$

Logo, $w$ é inversível. Reciprocamente, se $w$ é um elemento invertivel de A, então existe um $\lambda \in A$, tal que

$$\lambda w = 1$$

Dai, para todo $x \in A$, temos que $x = x.1$. Logo substituindo $\lambda w = 1$ e $x = x.1$, temos

$$x = x.1 \Longrightarrow x = x.(\lambda.w) \Longrightarrow x = y.w, \text{ onde } y = (x.\lambda) \in A$$

Dessa forma, temos que $\{w\}$ gera A. Também temos que se $a \in A$, tal que $aw = 0$, multiplicando pela direta por $w' \in A$, temos

$$(aw)w' = 0w' \Longrightarrow a(ww') = 0 \Longrightarrow a = 0$$

Portanto, $\{w\}$ é LI, logo é base de A.

**Observação:** Como consequência desse exemplo, temos que as unicas base do A-módulo ${}_{\mathbb{Z}}\mathbb{Z}$ são $\{1\}$ e $\{-1\}$, pois esses elementos são os únicos elementos invertiveis em $\mathbb{Z}$.

**Exemplo 3.0.1.8:** Um ideal à esquerda I de um anel A é um A-módulo livre , se e somente se, I é principal e gerador $\alpha$ de I tal que $Anl(\alpha) = 0$.

De fato, pois se I é um A-módulo livre, ele possui um base. Mas, se essa base tiver mais de um elemento, digamos $m_1, m_2$ com $m_1 \neq m_2$, temos

$$m_1(m_2) + m_2(-m_1) = 0$$

como $m_2, (-m_1) \in I$ não todos nulos, o que é absurdo, pois $m_1$ e $m_2$ pertencem a base de I, logo são independentes. Portanto, uma base para I é da forma $\{\alpha\}$, então I $= (\alpha)$, ou seja, segue que I é principal. Além disso, temos que $Anl(\alpha) = 0$, pois pelo contrário, existiria um $0 \neq m \in A$ tal que $m\alpha = 0$, isto é um absurdo, pois $\{\alpha\}$ não seria uma base.

De forma reciproca, se I é principal e um gerador $\alpha$ de I, tal que $Anl(\alpha) = 0$, então $\{\alpha\}$ é uma base de I.

De fato, pois se $\alpha$ é um gerador de I, então I $= (\alpha)$. Logo, temos que $\alpha$ gera I. Agora como $Anl(\alpha) = 0$, segue-se que

$$\alpha m = 0 \Longrightarrow m = 0$$

Logo, $\alpha$ é LI. Portanto, $\{\alpha\}$ é uma base de I.

**Exemplo 3.0.1.9:** 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.

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 de base canônica.

O estudo de teoria de módulos é parecido com o de álgebra linear, a diferença está que em álgebra linear o estudo é feito em cima de um corpo K, ja teoria de Módulos é realizado em cima de um anel, mas se analisarmos um corpo K não de deixa de ser um anel. Entretanto, algumas propriedades que são válida em espaçoes vetoriais, não são válida nos estudos de módulo, veremos nos exemplos a seguir.

**Exemplo 3.0.1.10:** Em espaço vetorial, todo subconjunto linearmente independente pode ser ampliado a uma base. Porém, em geral não é verdade que todo subconjunto linearmente independente, de um módulo livre, pode ser ampliado a uma base.

De fato, por exemplo, o $\mathbb{Z}$-módulo ${}_{\mathbb{Z}}\mathbb{Z}$ é livre e o conjunto $\{2\}$ é LI. Entretanto, não é uma base, e nem pode ser ampliado para um base, pois todo subconjunto com dois ou mais elementos em ${}_{\mathbb{Z}}\mathbb{Z}$ é LD.

**Exemplo 3.0.1.11:** Em espaço vetorial, todo conjunto gerador contém uma base. Porém, em módulos, em geral é falso.

De fato, pois se pegamos o conjunto $\{2,3\}$ vemos que ele gera ${}_{\mathbb{Z}}\mathbb{Z}$. Entretanto, não contém uma base, pois nehum elemento de $\{2,3\}$ é unidade de $\mathbb{Z}$

**Exemplo 3.0.1.12:** Em espaço vetorial, um conjunto é linearmente dependente se um dos elementos é combinação linear dos demais. Já em módulos, se uma família de elementos $\{x_i\}_{i\in I}$ de A-módulo, um deles é conbinação linear dos outros, a família não é livre.

De fato, por exemplo, se pois se consideramos o subconjunto $\{2,3\}$ do A-módulo ${}_{\mathbb{Z}}\mathbb{Z}$, temos que ele é LD. Entretanto, não é possiível fazer uma conbinação linear de um elemento com os outros, ou seja, não existe nenhum $x \in \mathbb{Z}$, tal que $2 = x.3$ ou $3 = x.2$.

**Exemplo 3.0.1.13:** Em espaço vetorial, temos que todo espaço vetorial tem uma base, porém em módulo, nem sempre um submódulo de um módulo livre é livre.

De fato, por exemplo, o $\mathbb{Z}_6$, se considerar o módulo sobre ele mesmo é livre de base $\{\overline{1}\}$. Mas, o submódulo $H = \{\overline{0},\overline{2},\overline{4}\}$, não é livre, pois não possui uma base, ja que todo subconjunto unitario de H é LD.

**Exemplo 3.0.1.14:** Em espaço vetorial, seja $S \subsetneq V$ um subespaço do espaço vetorial $V$ de dimensão finita. Então a cardinalidade de uma base de $S$ é menor que a cardinalidade de uma base de $V$. Já em módulos, dado um A-módulo livre $M$ e $R \subsetneq M$ um submódulo , também livre. Nem sempre é verdade que a cardinalidade de uma base de $R$ é menor que a cardinalidade de uma base de $M$.

De fato, Basta considerar o $\mathbb{Z}$-módulo $\mathbb{Z}\oplus\mathbb{Z}$ e o seu submódulo $R$ gerado pelos elementos $d_1 = (1,1)$ e $d_2 = (-1,1)$. Daí, temos que $R \subset \mathbb{Z}\oplus\mathbb{Z}$, pois $e_1 = (1,0)$, $e_2 = (0,1) \notin R$. Agora note que, $\{e_1, e_2\}$ é uma base de $\mathbb{Z}\oplus\mathbb{Z}$ de cardinalidade 2 e $\{d_1, d_2\}$ é uma base de $R$ com cardinalidade 2, logos as cardinalidades são iguais.

**Proposição 3.0.1.15:** Sejam M e N A-módulos. Suponhamos que M é livre e seja $X = \{x_i\}_{i\in I}$ um base de M. Dada uma função $f : X \longrightarrow N$ sempre é possível estender f a um único f a um A-homomorfismo $\overline{f} : M \longrightarrow N$ tal que $\overline{f}(x_i) = f(x_i), \forall x_i \in X$

**Demostração:** De fato, considere f definida do seguinte modo

$$f : X \longrightarrow N$$
$$x_i \longrightarrow f(x_i)$$

Como X é uma base de M, então todo $m \in M$ se escreve de uma única forma, como

$$m = \sum_{i\in I} \lambda_i x_i, \ \forall (\lambda_i)_{i\in I} \in A^{(I)}$$

Agora definimos $\overline{f}$ do seguinte modo

$$\overline{f} : M \longrightarrow N$$
$$m \longrightarrow \overline{f}(\sum_{i\in I} \lambda_i x_i) = \sum_{i\in I} \lambda_i f(x_i)$$

Mostraremos que $\overline{f}$ é um A-homomorfismo.

De fato, pois dados $m_1, m_2 \in M$, onde $m_1 = \sum_{i\in I} \lambda_i x_i$ e $m_2 = \sum_{i\in I} \beta_i x_i$ e $a \in A$, temos que

[I]

$$\begin{aligned}
\overline{f}(m_1 + m_2) &= \overline{f}(\sum_{i\in I} \lambda_i x_i + \sum_{i\in I} \beta_i x_i) \\
&= \overline{f}(\sum_{i\in I}(\lambda_i + \beta_i) x_i) \\
&= \sum_{i\in I}(\lambda_i + \beta_i) f(x_i) \\
&= \sum_{i\in I} \lambda_i f(x_i) + \sum_{i\in I} \beta_i f(x_i) \\
&= \overline{f}(\sum_{i\in I} \lambda_i x_i) + \overline{f}(\sum_{i\in I} \beta_i x_i) \\
&= \overline{f}(m_1) + \overline{f}(m_2)
\end{aligned}$$

[II]

$$\begin{aligned}\overline{f}(a(m_1)) &= \overline{f}(a\sum_{i\in I}\lambda_i x_i)\\ &= \overline{f}(\sum_{i\in I}(a\lambda_i)x_i)\\ &= \sum_{i\in I}(a\lambda_i)f(x_i)\\ &= \sum_{i\in I}\lambda_i f(x_i)\\ &= a\overline{f}(\sum_{i\in I}\lambda_i x_i)\\ &= a\overline{f}(m_1)\end{aligned}$$

Logo, $\overline{f}$ é um A-homomorfismo. Agora mostraremos que $\overline{f}(x_i) = f(x_i), \forall x_i \in X$.

De fato, pois $x_i \in X$, temos que $x_i = 1.x_i$, então

$$\begin{aligned}f(x_i) &= \overline{f}(1.x_i)\\ &= 1.f(x_i)\\ &= f(x_i)\end{aligned}$$

Resta mostrar a unicidade. Seja $g : M \longrightarrow N$ tal que $g(x_i) = f(x_i), \forall x_i \in X$ e $m = \sum_{i\in I}\lambda_i x_i$. Aplicando g em M, temos

$$\begin{aligned}g(m) &= g(\sum_{i\in I}\lambda_i x_i)\\ &= \sum_{i\in I}\lambda_i g(x_i)\\ &= \sum_{i\in I}\lambda_i f(x_i)\\ &= \overline{f}(\sum_{i\in I}\lambda_i x_i)\\ &= \overline{f}(m)\end{aligned}$$

Portanto, $\overline{f} = g$.

$\square$

**Corolário 3.0.1.16:** Se M é um A-módulo com base $X = \{x_i\}_{i\in I}$, então M é isomorfo a $A^{(I)}$.

**Demostração:** Seja $y = \{e_k\}_{k\in I}$ uma base canônica de $A^{(I)}$ e considere a aplicação

$$\begin{aligned} f : X &\longrightarrow A^{(I)} \\ x_i &\longrightarrow f(x_i) = f(e_i) \end{aligned}$$

Iremos mostrar que a extensão $\overline{f} : M \longrightarrow A^{(I)}$ definida pela preposição 3.0.1.15 é um isomorfismo.

(i) $\overline{f}$ é sobrejetora

Seja $m = \sum_{i \in I} \lambda_i x_i \in M$ e $a \in A^{(I)}$, como y é base de $A^{(I)}$, então a se escreve de forma única

$$\begin{aligned} a &= \sum_{i \in I} \lambda_i e_i \\ &= \sum_{i \in I} \lambda_i f(x_i) \\ &= \overline{f}(\sum_{i \in I} \lambda_i x_i) \\ &= \overline{f}(m) \end{aligned}$$

Portanto, como $a \in A^{(I)}$, existe um $m = \sum_{i \in I} \lambda_i x_i \in M$ tal que $\overline{f}(m) = a$, logo é sobrejetora.

(ii) $\overline{f}$ é injetiva.

Seja $m = \sum_{i \in I} \lambda_i x_i$ tal que $\overline{f}(m) = 0$, mostraremos que $m = 0$. De fato,

$$\begin{aligned} 0 &= \overline{f}(m) \\ &= \overline{f}(\sum_{i \in I} \lambda_i e_i) \\ &= \sum_{i \in I} \lambda_i f(x_i) \\ &= \sum_{i \in I} \lambda_i e_i \\ &= \lambda_i, \forall i \in I \end{aligned}$$

Como y é base, logo $\{e_k\}_{k \in I}$ é LI. Portanto, $m = 0$, assim $\overline{f}$ é injetora. Dessa forma

$$M \simeq A^{(I)}$$

□

**Proposição 3.0.1.17:** Se $f : M \longrightarrow N$ é um isomorfismo de A-módulos e M é livre, então N também é.

**Demostração:** De fato, como M é livre, logo tem uma base, assim seja $X = \{x_i\}_{i\in I}$ a base de M. Vamos mostrar que $y = \{f(x_i)_{i\in I}\}$ é base de N.

(i) y gera N.

Seja $n \in N$, como f é sobrejetora, temos que $n \in Im(f)$. Assim, existe um $m = \sum_{i\in I} \lambda_i x_i$ tal que

$$\begin{aligned} n &= f(m) \\ &= f(\sum_{i\in I} \lambda_i x_i) \\ &= \sum_{i\in I} \lambda_i f(x_i) \end{aligned}$$

Logo, y gera N.

(ii) y é LI.

Seja $\lambda_i, \forall i \in A^{(I)}$ tal que

$$\textstyle\sum_{i\in I} \lambda_i f(x_i) = 0 \Longrightarrow f(\sum_{i\in I} \lambda_i x_i) = 0 \Longrightarrow \sum_{i\in I} \lambda_i x_i \in Ker(f)$$

Como Ker(f) $= \{0\}$, segue-se que

$$\textstyle\sum_{i\in I} \lambda_i x_i = 0$$

E como X é base, temos que $\lambda_i = 0, \forall i \in I$. Logo, y é LI.

Portanto, por (i) e (ii) temos que $y = \{f(x_i)_{i\in I}\}$ é base de N.

$\square$

**Proposição 3.0.1.18:** Todo A-módulo M é isomorfo a um quociente de um Amódulo livre.

**Demostração:** seja $X = \{x_i\}_{i\in I}$ um gerador de um A-módulo M e $B = \{e_k\}_{k\in I}$ uma base canônica do A-módulo $A^{(I)}$. Considere a seguinte função

$$\begin{aligned} f : B &\longrightarrow M \\ e_i &\longrightarrow f(e_i) = x_i \end{aligned}$$

Como X é um gerador, então a extensão $\overline{f} : A^{(I)} \longrightarrow M$ é um epimorfismo, pois

$$m = \sum_{i \in I} \lambda_i x_i \Longrightarrow m = \sum_{i \in I} \lambda_i f(e_i) \Longrightarrow m = \sum_{i \in I} f(\lambda_i e_i)$$

Logo, pelo teorema do homomorfismo para módulo, temos que

$$\frac{A^{(I)}}{Ker(f)} \simeq M$$

□

**Proposição 3.0.1.19:** Sejam M, N e L A-módulos, onde L é um A-módulo livre. As funções $f : M \longrightarrow N$ é epimorfismo e $g : L \longrightarrow N$ é um A-homomorfismo. Então existe um A-homomorfismo $h : L \longrightarrow M$ tal que o seguinte diagrama comuta

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

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

**Demostração:** Inicialmente, provaremos a existência de h. Assim, seja $X = \{x_i\}_{i \in I}$ uma base de L, queremos um A-homomorfismo, no qual $h : L \longrightarrow M$. Ja que, $\forall x_i \in X$, temos que $g(x_i) \in N$, como f é um epimorfismo, segue que $g(x_i0 \in Im(f)$. Então existe um $m_i \in M$ tal que $f(m_i) = g(x_i)$. Dai considere a seguinte função

$$\begin{aligned} d : X &\longrightarrow M \\ x_i &\longrightarrow d(x_i) = m_i \end{aligned}$$

Onde $f(m_i) = g(x_i)$, pela proposição 3.0.1.15, temos que se pode extende a um único A-homomorfismo $h : L \longrightarrow M$ tal que $h(x_i) = d(x_i), \forall x_i \in X$.

Agora, mostraremos que $f \circ h = g$. De fato, dado um $q = \sum_{i \in I} \lambda_i x_i \in L$, temos

$$
\begin{aligned}
(f \circ h)(q) &= f(h(q)) \\
&= f(h(\sum_{i \in I} \lambda_i x_i)) \\
&= f(\sum_{i \in I} \lambda_i h(x_i)) \\
&= \sum_{i \in I} \lambda_i f(d(x_i) \\
&= \sum_{i \in I} \lambda_i f(m_i) \\
&= \sum_{i \in I} \lambda_i g(m_i) \\
&= g(\sum_{i \in I} \lambda_i x_i) \\
&= g(q)
\end{aligned}
$$

Logo, $f \circ h = g$.

$\square$

**Corolário 3.0.1.20:** Dado uma sequência exata de A-módulo

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

Se L é livre, a sequência cinde.

**Demostração:** Considere o diagrama a seguir

$$
\begin{tikzcd}
 & & & \mathbf{L} \arrow[dl, dashed, "h"'] \arrow[d, "Id_L"] & \\
\mathbf{0} \arrow[r] & \mathbf{M} \arrow[r, "f"'] & \mathbf{N} \arrow[r, "g"'] & \mathbf{L} \arrow[r] & \mathbf{0}
\end{tikzcd}
$$

Pela proposição 3.0.1.19, existe um $h : L \longrightarrow M$ que é um A-homomorfismo, tal que $g \circ h = Id_L$ e pela proposição 2.0.7.11, a sequência cinde, logo

$$N \simeq M \oplus L$$

$\square$

**Proposição 3.0.1.21:** Seja L um A-módulo livre e $f : M \longrightarrow L$ um epimorfismo de A-módulos, então $M \simeq Ker(f) \oplus L$.

**Demostração:** Considere o diagrama a seguir

$$\begin{tikzcd}
& & & \mathbf{L} \arrow[dl, dashed, "h"'] \arrow[d, "Id_L"] & \\
\mathbf{0} \arrow[r] & \mathbf{Ker(f)} \arrow[r, "i"'] & \mathbf{M} \arrow[r, "f"'] & \mathbf{L} \arrow[r] & \mathbf{0}
\end{tikzcd}$$

Pelo colorário 3.0.1.20, temos que $M \simeq Ker(f) \oplus L$.

□

**Colorário 3.0.1.22:** Seja N um submódulo de um A-módulo livre M, tal que o quociente $\frac{M}{N}$ também é livre. Então N é um somando direto de M e os seus suplementos são submódulos livres.

**Demostração:** Considere a sequência a seguir

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{p} \frac{M}{N} \longrightarrow 0$$

Pelo colorário 3.0.1.20 e da proposição 2.0.7.11, temos que existe um N' tal que $M = N \oplus N'$. Como todo suplementar de N é isomorfo a $\frac{M}{N}$, portanto é livre.

□

### 3.0.2 Considerações Finais

Este trabalho buscou explorar a teoria dos módulos livres, com isso, fornecendo uma base sólida para diversos estudos em teoria de módulos. Dessa forma, o estudo de módulos livres pode ser um ponto de partida para aprofundar-se em outras classes de módulos mais específicos, como módulos projetivos e injetivos, pois esses módulos possuem propriedades únicas que ampliam o entendimento das interações entre anéis e módulos. Mas outro ponto a ser destacado, na construção desse trabalho, foi o baixo número de trabalhos acadêmicos nessa área com referências brasileiras, pois a maior parte de trabalhos sobre módulos se encontra em arquivo de lingua inglesa, essa foi o maior dificuldade na produção desse trabalho.

## REFERÊNCIAS

[1] ATIYAH, Michael. **Introduction to commutative álgebra**. CRC Press, 2018.

[2] FERNANDES, Rui Loja; RICOU, Manuel. **Introdução à álgebra**. IST Press, 2004.

[3] LANG, Serge. **Algebra: Graduate Texts in Mathematics**. 3. ed. Nova York: Springer, 2005.

[4] LOURÊDO, Aldo Trajano; OLIVEIRA, Alexandre Marinho. **Um primeiro curso de álgebra linear**. Campina Grande: ADUEPB, 2015.

[5] MILLES, César Polcino. **Anéis e Módulos** - 2. ed. - São Paulo: Editora Livraria da Física, 2018.

[6] MILIES, César Polcino. Breve História da Álgebra Abstrata. In: BIENAL DA SOCIEDADE BRASILEIRA DE MATEMÁTICA, 2., 2004, Salvador. **Anais eletrônicos**... Disponível em: http://www.bienasbm.ufba.br/M18.pdf. Acesso em 01 de nov de 2024.

[7] MUSILI, Chitikila. **Introduction to rings and modules**. 2. ed. Nova Deli: Narosa Publishing House, 2001.

[8] VIEIRA, Vandenberg Lopes. **Álgebra abstrata para licenciatura**. Campina Grande: ADUEPB, 2013.

## APÊNDICE A – Grupos e Anéis

**Definição 1:** *Um conjunto não vazio G munido de uma operação de "adição (+)"é um grupo se satisfaz as sequinte propriedades:*

1. *(Associatividade da Adição)* $a + (b + c) = (a + b) + c$; *para todo* $a, b, c \in G$
2. *(Comutatividade da Adição)* $a + b = b + a$; *para todo* $a, b \in G$
3. *(elemento neutro da Adição) vai existir um* $0 \in G$ *, tal que para todo* $a \in G$, $a + 0 = a$
4. *(Simétrico da Adição) para todo* $a \in G$*, vai existir um* $-a \in G$ *tal que* $a + (-a) = 0$

**Definição 2:** *Um grupo (G, +) é comutativo ou abeliano quando*

$$a + b = b + a; \text{ para todo } a, b \in G$$

ou seja, quando a operação em G for comutativa.

**Exemplo 1:** Os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ com as operações usuais da adição são exemplos de grupos abelianos.

**Definição 3:** *Seja A um conjunto não vazio, munido com as seguintes operações: Adição (+) :*

$$\begin{aligned} A \times A &\longrightarrow A \\ (a, b) &\longrightarrow a + b \end{aligned}$$

*Multiplicação* $(\cdot)$ *:*

$$\begin{aligned} A \times A &\longrightarrow A \\ (\lambda, b) &\longrightarrow a \cdot b \end{aligned}$$

*Dizemos que a terna* $(A, +, \cdot)$ *é um anel se satisfas as seguintes propriedades:*

1. *(Associatividade da Adição)* $a + (b + c) = (a + b) + c$; *para todo* $a, b, c \in A$
2. *(Comutatividade da Adição)* $a + b = b + a$; *para todo* $a, b \in A$
3. *(elemento neutro da Adição) vai existir um* $0_A \in A$ *, tal que para todo* $a \in A$, $a + 0_A = a$
4. *(Simétrico da Adição) para todo* $a \in A$*, vai existir um* $-a \in A$ *tal que* $a + (-a) = 0_A$

5. *(Associativa da multiplicação)* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$; *para todo* $a, b, c \in A$

6. *(Distributividade da multiplicação)* $a \cdot (b + c) = a \cdot b + a \cdot c$ *e* $(a + b) \cdot c = a \cdot c + b \cdot c$; *para todo* $a, b, c \in A$

**Definição 4:** *Dizemos que* $A$ *é um anel comutativo se, somente se:*

$$a \cdot b = b \cdot a; \text{ para todo } a, b \in A$$

**Definição 5:** *Um anel* $A$ *é dito com unidade quando existe* $1_A \in A$ *tal que :*

$$a \cdot 1_A = a; \text{ para todo } a, b \in A$$

**Exemplo 2:** As estruturas $(\mathbb{Z}, +, .), (\mathbb{Q}, +, .), (\mathbb{R}, +, .)$ e $(\mathbb{C}, +, .)$ com suas repectivas operações usuais da adição e multiplicação são exemplos de anéis comutativos com unidade. O número 1 é a unidade deste anéis.

**Definição 6:** *Seja* $A$ *um anel e* $B \subset A$ *não vazio, dizemos que* $B$ *é subanel de* $A$*, quando* $B$ *com as operações induzidas de* $A$*, ainda é um anel.*

**Exemplo 3:** Se $n \in \mathbb{Z}$, então $n\mathbb{Z}$ é um subanel de $\mathbb{Z}$, que por sua vez é um subanel de $\mathbb{Q}$ . Em geral, temos que a seguinte cadeia de subanel:

$$n\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

**Definição 7:** *Seja* $A$ *um anel. Um subconjunto não vazio* $I$ *de* $A$ *chama-se ideal de* $A$ *quando as seguintes propriedades.*

(I) $x - y \in I$, para todo $x, y \in I$
(II) $ax \in I$ e $xa \in I$, para todo $x \in I$ e $a \in A$

**Definição 7:** *Um subconjunto não vazio* $I$ *de um anel* $A$ *chama-se ideal à esquerda( à direita) de* $A$ *quando as seguintes propriedades.*

(I) $x - y \in I$, para todo $x, y \in I$
(II) $ax \in I$ e $(xa \in I)$, para todo $x \in I$ e $a \in A$

A expressão $xa \in I$ entre parênteses acima se refere a condição de ser ideal à direita.

**Exemplo 4:** Seja o anel $A = \mathbb{R}^{\mathbb{R}}$ (comutativo) de todas as funções $f : \mathbb{R} \longrightarrow \mathbb{R}$. Dado $a \in \mathbb{R}$ considere $I = \{f \in A,\ f(a) = 0\}$. É imediato verificar que $f - g \in I$, quaisquer que seja $f, g \in I$. Agora , se $g \in A$ e $f \in I$, então

$$(f \cdot g)(a) = f(a) \cdot g(a) = 0 \cdot g(a) = 0$$

Ou seja, $f \cdot g \in I$. Portanto, I é um ideal de A.

## APÊNDICE B – Espaços Vetoriais

**Definição 1:** *Um corpo é um conjunto* $\mathbb{K}$*, cujos os elementos são chamados escalares, com um par de operações:*

*Adição (+) :*

$$\begin{aligned} \mathbb{K} \times \mathbb{K} &\longrightarrow \mathbb{K} \\ (a, b) &\longrightarrow a + b \end{aligned}$$

*Multiplicação* $(\cdot)$ *:*

$$\begin{aligned} \mathbb{K} \times \mathbb{K} &\longrightarrow \mathbb{K} \\ (a, b) &\longrightarrow a \cdot b \end{aligned}$$

*Se satisfaz as seguintes propriedades:*

I - *(Associatividade da Adição)* $a + (b + c) = (a + b) + c$*; para todo* $a, b, c \in \mathbb{K}$

II - *(Comutatividade da Adição)* $a + b = b + a$*; para todo* $a, b \in \mathbb{K}$

III - *(elemento neutro da Adição) vai existir um* $0 \in \mathbb{K}$ *, tal que para todo* $a \in \mathbb{K}$, $a + 0 = a$

IV - *(Simétrico da Adição) para todo* $a \in \mathbb{K}$*, vai existir um* $-a \in \mathbb{K}$ *tal que* $a + (-a) = 0$

V - *(Associativa da multiplicação)* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*; para todo* $a, b, c \in \mathbb{K}$

VI - *(Distributividade com relação aos elementos de* $\mathbb{K}$*)* $x \cdot (a + b) = x \cdot a + x \cdot b$*; para todo* $x, a, b \in \mathbb{K}$

VII - *(comutatividade da multiplicação)* $a \cdot b = b \cdot a$*; para todo* $a, b \in \mathbb{K}$

VIII - *(Elemento neutro da multiplicação) vai existir* $1 \in \mathbb{K}$ *tal que* $a \cdot 1 = a$*; para todo* $a \in \mathbb{K}$

**Exemplo 1:** Os conjuntos $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ com as operações usuais de adição e multiplicação são corpos.

**Definição 2:** *Dizemos que um conjunto* $V \neq 0$*, munido de duas operações "adição"e "multiplicação por escalares":*

*Adição (+) :*

$$V \times V \longrightarrow V$$
$$(a, b) \longrightarrow a + b$$

*Multiplicação por escalares* $(\cdot)$ *:*

$$\mathbb{K} \times V \longrightarrow V$$
$$(\lambda, a) \longrightarrow \lambda \cdot a$$

*É um espaço vetorial sobre* $\mathbb{K} = \mathbb{R}$ *ou* $\mathbb{K} = \mathbb{C}$ *se satisfas as seguintes propriedades*:

I - *(Associatividade da Adição)* $a + (b + c) = (a + b) + c$*; para todo* $a, b, c \in V$

II - *(Comutatividade da Adição)* $a + b = b + a$*; para todo* $a, b \in V$

III - *(elemento neutro da Adição) vai existir um* $0 \in V$ *, tal que para todo* $a \in V$, $a + 0 = a$

IV - *(Simétrico da Adição) para todo* $a \in V$*, vai existir um* $-a \in V$ *tal que* $a + (-a) = 0$

V - *(Associativa da multiplicação por escalares)* $(\lambda \cdot \beta) \cdot a = \lambda \cdot (\beta \cdot a)$*; para todo* $\lambda, \beta \in \mathbb{K}$ *e* $a \in V$

VI - *(Distributividade com relação aos elementos de V)* $\lambda \cdot (a + b) = \lambda \cdot a + \lambda \cdot b$*; para todo* $\lambda \in \mathbb{K}$ *e* $a, b \in V$

VII - *(Distributividade com relação às escalares)* $(\lambda + \beta) \cdot a = \lambda \cdot a + \beta \cdot a$*; para todo* $\lambda, \beta \in \mathbb{K}$ *e* $a \in V$

VIII - *(Elemento neutro da operação externa) vai existir* $1 \in V$ *tal que* $a \cdot 1 = a$*; para todo* $a \in V$

**Definição 3:** *Seja V um espaço vetorial sobre um corpo* $\mathbb{R}$ *e W um subconjunto de V. Dizemos que W é um subespaço de V se satisfaz as seguinte condições:*

I - $0 \in W$

II - $\lambda \cdot a \in W$ para todo $\lambda \in \mathbb{R}$ e $a \in W$

III - $a + b \in W$, para todo $a, b \in W$.

**Exemplo 2:** Seja W = $\{(x, 0) : x \in \mathbb{R}$ um subconjunto de $\mathbb{R}^2$. Temos que W é um subespaço de $\mathbb{R}$.

De fato, pois temos que

I - $(0, 0) \in W$

II - Dados $\lambda \in \mathbb{R}$ e $a = (x, 0) \in W$. temos $\lambda a = (\lambda x, \lambda 0) = (\lambda x, 0) \in W$

III - Dados $a = (x, 0)$ e $b = (y, 0) \in W$. temos que $a + b = (x, 0) + (y, 0) = (x + y, 0) \in W$

**Definição 4:** *Seja $V$ um espaço vetorial real, $a_1, ..., a_n \in V$ e $\lambda_1, ..., \lambda_n \in \mathbb{R}$. Então o vetor*

$$v = a_1\lambda_1 + ... + a_n\lambda_n$$

*É um elemento de $V$ o qual chamamos de conbinação lienar.*

**Exemplo 2:** O vetor $v = (2, 5) \in \mathbb{R}^2$ é uma conbinação linear dos vetores de $v_1 = (1, 1)$ e $v_2 = (0, 1)$, pois $v = 2v_1 + 3v_2$.

**Definição 5:** *Seja $V$ um espaço vetorial e $A = \{a_1, ..., a_n\} \subset V$. Consideramos a equação:*

$$a_1\lambda_1 + ... + a_n\lambda_n = 0$$

*O conjunto $A$ diz linearmente independente (LI), se apenas admitir uma solução trivial, ou seja*

$$\lambda_1 = \lambda_2 = ... = 0$$

*E se existir um $\lambda_i \neq 0$, para algum $i = 1, ..., n$ o conjunto $A$ é liearmente dependente.*

**Exemplo 3:** Seja V = $\mathbb{R}^2$, os vetores $a_1 = (2, -1)$ e $a_2 = (1, 3)$, formam um conjunto LI.

De fato, pois considerando a conbinação linear $\lambda_1 a_1 + \lambda_2 a_2 = 0$, dai obtemos o sistema

$$\begin{cases} 2\lambda_1 & +\lambda_2 & = & 0 \\ -\lambda_1 & +3\lambda_2 & = & 0 \end{cases}$$

Daí, resolvendo os sistema vamos obter $\lambda_1 = \lambda_2 = 0$. Portanto o conjunto é LI.

**Definição 6:** *Um conjunto $B = \{a_1, ..., a_n\} \subset V$ é uma base para o espaço vetorial $V$ se:*

I - $B$ é LI
II - $B$ gera V

**Exemplo 4:** o conjunto

$$B = \{a_1, a_2\},\ a_1 = (2, -1) \text{ e } a_2 = (1, 3)$$

É um base para $\mathbb{R}^2$, pois $B$ é LI e gera $\mathbb{R}^2$.