Sobre uma base para A-módulos

Ailton Ribeiro de Assis ra: 134713
Claudio Michael Qureshi ra:137920
Juliana Fernandes Larrosa ra: 089366
Julio Cesar Valencia Guevara ra: 099814
Leandro da Silva Tavares ra: 134710
Leandro Morgado ra:133569
Steve da Silva Vicentim ra:134717
Thais Borges Damacena ra: 099887
Universidade Estadual de Campinas - UNICAMP

7 de Maio de 2012

Resumo

Uma das maiores diferenças entre espaços vetoriais (A-módulos, com A corpo) e um A-módulo em geral, é que nem sempre é possível obter uma base para o segundo.

Na primeira seção, introduziremos o conceito de módulo livre (que são justamente os módulos que possuem base), apresentaremos algumas propriedades elementares que se obtêm da definição e exibiremos alguns exemplos. Na segunda seção, generalizaremos a definição de dimensão para A-módulos livres. Na terceira seção, discutiremos duas questões cuja resposta se verifica verdadeira para espaços vetoriais, mas não valem para A-módulos em geral: todo conjunto gerador contém uma base e todo conjunto l.i. pode ser estendido a uma base. Na quarta seção, finalizaremos o trabalho estudando A-módulos, para A um domínio de ideais principais, e neste contexto explicitamos condições suficientes para garantir a existência de uma base.

Para nós, A anel representa um anel comutativo com unidade $\neq \{0\}$ (salvo menção contrária).

1 Primeiras definições e exemplos

Definição 1.1. Seja M um A-módulo. Um conjunto $X \subseteq M$ é dito uma base para M se todo elemento de M pode ser escrito unicamente como uma combinação linear finita de elementos de X com coeficientes em A. Equivalentemente:

(i) Dado $m \in M$, existem $\lambda_1, ..., \lambda_n \in A$ e $x_1, ..., x_n \in X$ tais que $m = \lambda_1 x_1 + ...\lambda_n x_n$. Em outras palavras, X gera M;

(ii) Dados $\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_n \in A$ e $x_1, \ldots, x_n \in M$, se $\lambda_1 x_1 + ... + \lambda_n x_n = \mu_1 x_1 + ... + \mu_n x_n$, então $\lambda_i = \mu_i$ para $i = 1, 2, \ldots, n$. Em outras palavras, X é um conjunto linearmente independente (l.i.).

Observação 1.2. *Do mesmo jeito que para espaços vetoriais pode provar-se que a condição (ii) é equivalente a:*

(ii') Dados $\lambda_1, ..., \lambda_n \in A$ *e* $x_1, ..., x_n \in M$*, se* $\lambda_1 x_1 + ...\lambda_n x_n = 0$*, então* $\lambda_1 = ... = \lambda_n = 0$*.*

Definição 1.3. Um A-módulo M é dito A-módulo livre se ele possui uma base. Por convenção o grupo $\{0\}$ é um A-módulo livre para qualquer anel A, com base $B = \emptyset$.

Exemplo 1.4.

(1) $M = A \times ... \times A$, com a base canônica $B = \{(1, 0, ..., 0), (0, 1, 0, ..., 0), ..., (0, ..., 0, 1)\}$;

(2) $M = A[X]$ é um A-módulo livre com base $B = \{1, X, X^2, ...\}$;

(3) Os inteiros de Gauss $M = \mathbb{Z} + i\mathbb{Z}$ com a base $B = \{1, i\}$ é um $\mathbb{Z}$-módulo livre. De fato, claramente B gera M, e como B é linearmente independente sobre $\mathbb{R}$, será linearmente independente também sobre $\mathbb{Z}$.

Exemplo 1.5. Seja $\mathbb{K}$ um corpo (em particular um anel). Um exemplo típico de $\mathbb{K}$-módulo livre são os espaços vetoriais sobre o corpo $\mathbb{K}$.

De fato, se $\mathbb{V}$ é um $\mathbb{K}$-espaço vetorial em particular $\mathbb{V}$ é um $\mathbb{K}$-módulo. Mostremos que $\mathbb{V}$ possui uma base. Definamos

$$\Sigma = \{B \subset \mathbb{V} : B \text{ é linearmente independente}\}$$

e considere em Σ a ordem parcial dada pela inclusão de conjuntos. Segue que $\Sigma \neq \emptyset$ pois como $\mathbb{K}$ é um corpo, então para cada $v \in \mathbb{V}$ com $v \neq 0$ temos que $\{v\} \in \Sigma$. Seja $\Omega \subset \Sigma$ uma cadeia e tome $T = \cup_{B \in \Omega} B$. Mostremos que $T \in \Sigma$. De fato, dados $v_1, \ldots, v_k \in T$, então existem $B_1, \ldots, B_k \in \Omega$ tais que $v_j \in B_j$, a menos de reordenamento e pelo fato de Ω ser uma cadeia podemos supor que $B_1 \subset B_2 \subset \cdots \subset B_k$, logo $\{v_1, \ldots, v_k\} \subset B_k$ mas como $B_k \in \Sigma$ segue que quando tivermos

$$r_1 v_1 + \cdots + r_k v_k = 0,$$

com $r_i \in \mathbb{K}$, necessariamente deve-se ter que $r_1 = \ldots = r_k = 0$ assim $T \in \Sigma$. Pelo lema de Zorn temos que existe um elemento maximal $\mathcal{B} \in \Sigma$. Resta mostrar que $\mathcal{B}$ gera $\mathbb{V}$. Seja $w \in \mathbb{V}$ tal que $w \notin \mathcal{B}$ (pois caso contrario não há nada a mostrar), então $\mathcal{B} \cup \{w\} \notin \Sigma$ pela maximalidade de $\mathcal{B}$. Segue que $0 \in \mathbb{V}$ pode ser expressado como combinação linear não trivial de elementos em $\mathcal{B} \cup \{w\}$ a qual debe ser necessariamente da forma

$$rw + r_1 v_1 + \cdots + r_k v_k = 0,$$

onde $r, r_j \in \mathbb{K}$ e $v_j \in \mathcal{B}$. Segue que a única opção é que $r \neq 0$ (caso contrário, como $\{v_1, \ldots, v_k\}$ é l.i. teríamos que também $r_1 = r_2 = \ldots = r_k = 0$ e a combinação linear seria trivial) e multiplicando por r^{-1} temos que

$$w = -r^{-1} r_1 v_1 - \cdots - r^{-1} r_k v_k,$$

como se queria mostrar.

Antes de ver uma outra caracterização para módulos livres, vamos relembrar o conceito de soma direta de A-módulos.

Definição 1.6. Seja $\{M_\alpha\}_{\alpha\in\Gamma}$ uma família arbitrária de A-módulos. Definimos sua soma direta como o conjunto:

$$\bigoplus_{\alpha\in\Gamma} M_\alpha := \{\text{funções } m : \Gamma \to \cup_{\alpha\in\Gamma} M_\alpha; m(\alpha) \in M_\alpha,\ \forall\alpha \in \Gamma,\ \text{e } m(\alpha) = 0 \text{ para quase todo } \alpha \in \Gamma\},$$

e, se $m \in \bigoplus_{\alpha\in\Gamma} M_\alpha$ escreveremos $m(\alpha) = m_\alpha$.

Munido das operações:

- $(m_1 + m_2)(\alpha) = m_1(\alpha) + m_2(\alpha)\ \forall\alpha \in \Gamma=$;
- $(am)(\alpha) = am(\alpha)\ \forall\alpha \in \Gamma\ (a \in A)$.

damos a $\bigoplus_{\alpha\in\Gamma} M_\alpha$ uma estrutura de A-módulo.

De fato (lembre-se que cada M_α é um A-módulo),

1. ($\bigoplus_{\alpha\in\Gamma} M_\alpha$,+) é um grupo abeliano. Pois se $m_1,\ m_2,\ m_3 \in \bigoplus_{\alpha\in\Gamma} M_\alpha$, então valem as seguintes propriedades:

   (a) + é uma operação binária definida sobre $\bigoplus_{\alpha\in\Gamma} M_\alpha$.
   Como $m_1(\alpha)$,$m_2(\alpha) \in M_\alpha$ para todo $\alpha \in \Gamma$ e $m_1(\alpha) = 0$, $m_2(\alpha) = 0$ para quase todo $\alpha \in \Gamma$ temos que $(m_1 + m_2)(\alpha) \in M_\alpha$ para todo $\alpha \in \Gamma$ e $(m_1 + m_2)(\alpha) = 0$ para quase todo $\alpha \in \Gamma$. Logo, $m_1 + m_2 \in \bigoplus_{\alpha\in\Gamma} M_\alpha$.

   (b) Associatividade.
   $((m_1 + m_2) + m_3)(\alpha) = (m_1 + m_2)(\alpha) + m_3(\alpha) = (m_1(\alpha) + m_2(\alpha)) + m_3(\alpha) = m_1(\alpha) + (m_2(\alpha) + m_3(\alpha)) = m_1(\alpha) + (m_1 + m_2)(\alpha) = (m_1 + (m_2 + m_3))(\alpha)$.

   (c) Existência do elemento neutro.
   Seja $m : \Gamma \to \cup_{\alpha\in\Gamma} M_\alpha$ tal que $m(\alpha) = 0$ para todo $\alpha \in \Gamma$. Assim, $m \in \bigoplus_{\alpha\in\Gamma} M_\alpha$.
   Além disso, $(m + m_1)(\alpha) = m(\alpha) + m_1(\alpha) = 0 + m_1(\alpha) = m_1(\alpha) = (m_1 + m)(\alpha)$.

   (d) Existência do elemento simétrico.
   Seja $m : \Gamma \to \cup_{\alpha\in\Gamma} M_\alpha$ tal que $m(\alpha) = -m_1(\alpha)$ para todo $\alpha \in \Gamma$. Assim, $m \in \bigoplus_{\alpha\in\Gamma} M_\alpha$.
   Além disso, $(m + m_1)(\alpha) = m(\alpha) + m_1(\alpha) = -m_1(\alpha) + m_1(\alpha) = 0 = (m_1 + m)(\alpha)$.

   (e) Comutatividade.
   $(m_1 + m_2)(\alpha) = m_1(\alpha) + m_2(\alpha) = m_2(\alpha) + m_1(\alpha) = (m_2 + m_1)(\alpha)$.

2. A operação . definida acima satisfaz as seguintes propriedades:

   (a) $a(m_1 + m_2) = am_1 + am_2$ para todo $a \in A$.
   $(a(m_1 + m_2))(\alpha) = a(m_1 + m_2)(\alpha) = a(m_1(\alpha) + m_2(\alpha)) = am_1(\alpha) + am_2(\alpha) = (am_1 + m_2)(\alpha)$.

   (b) $(a + b)m_1 = a(bm_1)$ para todos $a, b \in A$.
   $((a + b)m_1(\alpha) = (a + b)m_1(\alpha) = am_1(\alpha) + bm_1(\alpha) = (am_1 + bm_2)(\alpha)$.

(c) $(ab)m_1 = a(bm_1)$ para todo $a \in A$.
$((ab)m_1)(\alpha) = (ab)m_1(\alpha) = a(bm_1(\alpha)) = a(bm_1)(\alpha) = (a(bm_1))(\alpha)$.

(d) $1m_1 = m_1$
$(1m_1)(\alpha) = 1m_1(\alpha) = m_1(\alpha)$.

Agora vamos ver uma caracterização importante dos módulos livres[1].

Proposição 1.7. *Seja M um A-módulo. Então M é um A-módulo livre se e somente se M é isomorfo à soma direta de cópias de A.*

Demonstração. ($\Rightarrow$) Se M é um módulo livre, considere $X = \{x_\alpha\}_{\alpha\in\Gamma}$ uma base de M. Então, dado um elemento $m \in M$, podemos escrevê-lo de forma única como $m = \sum_{\alpha\in\Gamma} a_\alpha x_\alpha$, com $a_\alpha \in A$, $\forall\alpha \in \Gamma$, e $a_\alpha = 0$ para quase todo $\alpha \in \Gamma$. Dessa forma, defina:

$$\phi : M \to \bigoplus_{\alpha\in\Gamma} A, \quad m = \sum_{\alpha\in\Gamma} a_\alpha x_\alpha \mapsto s : s_\alpha = a_\alpha,\ \forall\alpha \in \Gamma.$$

Assim:

1. ϕ é um homomorfismo de A-módulos.

   De fato, sejam $m_1 = \sum_{\alpha\in\Gamma} a_\alpha x_\alpha$, $m_2 = \sum_{\alpha\in\Gamma} b_\alpha x_\alpha$, onde a_α, $b_\alpha \in A$ para todo $\alpha \in \Gamma$ e $a_\alpha = 0$, $b_\alpha = 0$ para quase todo $\alpha \in \Gamma$. Assim,

   - $\phi(m_1 + m_2) = \phi(\sum_{\alpha\in\Gamma}(a_\alpha + b_\alpha)x_\alpha) = s$, onde $s_\alpha = a_\alpha + b_\alpha,\ \forall\alpha \in \Gamma$.
     $\phi(m_1) + \phi(m_2) = s_1 + s_2$, onde $s_{1_\alpha} = a_\alpha$ e $s_{2_\alpha} = b_\alpha$. Logo, $s_\alpha = s_{1_\alpha} + s_{2_\alpha}$, e portanto $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$.
   - $\phi(am_1) = \phi(\sum_{\alpha\in\Gamma}(aa_\alpha)x_\alpha) = s$, onde $s_\alpha = aa_\alpha,\ \forall\alpha \in \Gamma$
     $a\phi(m_1) = as_1$, onde $s_{1_\alpha} = a_\alpha,\ \forall\alpha \in \Gamma$. Logo, $s_\alpha = as_{1_\alpha}$, e portanto $\phi(am_1) = a\phi(m_1)$.

2. ϕ é bijetora.

   - Se $\phi(m_1) = \phi(m_2)$, então, $s_1 = s_2$, onde $s_{1_\alpha} = a_\alpha$ e $s_{2_\alpha} = b_\alpha$ para todo $\alpha \in \Gamma$. Assim, $a_\alpha = b_\alpha$ para todo $\alpha \in \Gamma$. Concluímos assim que $m_1 = m_2$ e portanto que ϕ é injetora.
   - Seja $s \in \bigoplus_{\alpha\in\Gamma} A$. Então, $s_\alpha = c_\alpha$, onde $c_\alpha \in M_\alpha$ para todo $\alpha \in \Gamma$ e $c_\alpha = 0$ para quase todo $\alpha \in \Gamma$. Defina então, $m = \sum_{\alpha\in\Gamma} c_\alpha x_\alpha$. Dessa forma, $m \in M$ e $\phi(m) = s$. Portanto, ϕ é sobrejetora.

Logo, ϕ é um isomorfismo de A-módulos.

($\Leftarrow$) Se $M \simeq \bigoplus_{\alpha\in\Gamma} A$, seja $\phi : M \to \bigoplus_{\alpha\in\Gamma} A$ isomorfismo de A-módulos. Vamos considerar o conjunto $B = \{e_\alpha \in M : \alpha \in \Gamma\}$ dado por: $e_\alpha(i) = \begin{cases} 1 & \text{se } i = \alpha \\ 0 & \text{se } i \in \Gamma\backslash\{\alpha\} \end{cases}$ Note que B é uma base para $\bigoplus_{\alpha\in\Gamma} A$.

De fato,

[1] É interessante destacar que o livro de Atiyah-MacDonald utiliza esta caracterização como a definição de A-módulo livre. A Proposição 1.7 mostra que ambas as definições são equivalentes.

- Seja $s \in \bigoplus_{\alpha\in\Gamma} A$. Então $s : \Gamma \to \cup_{\alpha\in\Gamma} A$ é tal que $s(\alpha) = s_\alpha \in A$ para todo α e $s(\alpha) = 0$ para quase todo $\alpha \in \Gamma$.

  Assim, $s(i) = \sum_{\alpha\in\Gamma} s_\alpha e_\alpha(i)$, para $i \in \Gamma$. Ou seja, B gera $\bigoplus_{\alpha\in\Gamma} A$.

- Se $s_{\alpha_1}e_{\alpha_1} + s_{\alpha_2}e_{\alpha_2} + ... + s_{\alpha_n}e_{\alpha_n} = 0$, então,

  $(s_{\alpha_1}e_{\alpha_1} + s_{\alpha_2}e_{\alpha_2} + ... + s_{\alpha_n}e_{\alpha_n})(\alpha_i) = 0$, $i \in \{1, ..., n\}$. O que implica que $s_{\alpha_i} = 0$. Ou ainda, $s_{\alpha_1} = ... = s_{\alpha_n} = 0$. Portanto, B é um conjunto l.i.

Agora, sabemos que isomorfismos preservam bases [2]. Assim o conjunto $\{\phi^{-1}(e_\alpha) : \alpha \in \Gamma\}$ é uma base para M.

□

Corolário 1.8. *Seja M um A-módulo livre. Então $M = \{0\}$ ou $\#M \geq \#A$.*

Demonstração. Pela Proposição 1.7, se M é livre, então $M \simeq \bigoplus_{\alpha\in\Gamma} A$. Assim, se $M \neq \{0\}$, então $\#\Gamma \neq \emptyset$, seguindo que $\#M = \#\bigoplus_{\alpha\in\Gamma} A \geq \#A$. □

Exemplo 1.9. O $\mathbb{Z}$-módulo $\mathbb{Z}_n$ não é um $\mathbb{Z}$-módulo livre (pois $\#\mathbb{Z}_n < \#\mathbb{Z}$).

Observação 1.10. *Consideremos o A-módulo livre $S = \bigoplus_{\alpha\in\Gamma} A$. Então, para cada $\alpha \in \Gamma$ temos definido um epimorfismo $\pi_\alpha : S \to A$ dado por $\pi_\alpha(x) = x_\alpha$ (chamado projeção α-ésima).*
Observe que:

- *π_α é um homomorfismo de A-módulos.*

  De fato, sejam $s_1, s_2 \in S$. Assim, $s_1 : \Gamma \to \cup_{\alpha\in\Gamma} A$ e $s_2 : \Gamma \to \cup_{\alpha\in\Gamma} A$.

  - $\pi_\alpha(s_1 + s_2) = (x + y)_\alpha = x_\alpha + y_\alpha = \pi_\alpha(s_1) + \pi_\alpha(s_2)$
  - $\pi_\alpha(as) = (as)_\alpha = as_\alpha = a\pi_\alpha(s)$

- *π_α é sobrejetor.*

  De fato, seja $a \in A$ e considere $y = \sum_{\alpha\in\Gamma} ae_\alpha$, onde $e_\alpha(i) = \begin{cases} 1 & \text{se } i = \alpha \\ 0 & \text{se } i \in \Gamma\backslash\{\alpha\} \end{cases}$.

  Assim, $\pi_\alpha(y) = y_\alpha = a$.

Portanto, essas funções são epimorfismos de A-módulos. Pela proposição anterior, podemos estender esta ideia a A-módulos livres quaisquer. Se M é um módulo livre, escolhemos uma base (ordenada) $\{x_\alpha\}_{\alpha\in\Gamma}$ de M como A-módulo e podemos definir a projeção α-ésima via o isomorfismo ϕ da proposição anterior:

$$M \xrightarrow{\phi} \bigoplus_{\alpha\in\Gamma} A \xrightarrow{\pi_\alpha} A\,.$$

[2] De fato, seja $f : M \to N$ um isomorfismo e $X = \{x_\alpha; \alpha \in \Gamma\}$ uma base de N. Dado $m \in M$, existe único $n \in N$ tal que $m = f^{-1}(n)$. Como X é base de N, existem únicos $\lambda_1, ..., \lambda_n \in A$ e $x_1, ..., x_n \in X$ tais que $m = f^{-1}(\lambda_1 x_1 + ... + \lambda_n x_n) = \lambda_1 f^{-1}(x_1) + ...\lambda_n f^{-1}(x_n)$. Assim, $\{f^{-1}(x_\alpha); \alpha \in \Gamma\}$ é uma base para M.

O homomorfismo $\pi_\alpha \circ \phi$ será representado também como π_α (abuso de notação), sendo denominado projeção α-ésima (observe que depende da escolha da base ordenada). Nas demonstrações de propriedades de módulos livres finitamente gerados (como A-módulo), as projeções têm um papel muito importante, já que nos permitem fazer provas por indução (veja por exemplo a demonstração do Lema 4.2).

2 A dimensão de um A-módulo livre

Quando estamos no contexto referente a espaços vetoriais, temos que qualquer base de um espaço possui a mesma cardinalidade de suas demais bases. Este fato faz com que o conceito de dimensão de um espaço vetorial fique bem definido como a cardinalidade de uma base.

Neste capítulo, mostraremos que o conceito de dimensão pode ser estendido aos A-módulos livres, como cardinalidade de uma base.

Lema 2.1. *Seja M um A-módulo e I ideal de A. Então IM é um A-módulo e M/IM é um A/I-módulo.*

Demonstração. Temos inicialmente que:

$$IM := \left\{ \sum_j^n i_j m_j ; i_j \in I, m_j \in M \text{ e } n \in \mathbb{N} \right\}.$$

Claramente IM é fechado para a soma, e portanto é um subgrupo abeliano de M, pois M é abeliano. O fato de IM ser um A-módulo segue de I ser ideal e M ser A-módulo.

Definamos agora a seguinte operação:

$$\begin{aligned} \cdot : A/I \times M/IM &\to M/IM \\ (\lambda + I, m + IM) &\mapsto \lambda m + IM. \end{aligned}$$

Se $\lambda_1 + I = \lambda_2 + I$ e $m_1 + IM = m_2 + IM$, então $\lambda_1 - \lambda_2 \in I$ e $m_1 - m_2 \in IM$. Assim, observe que:

$$\begin{aligned} \lambda_1 m_1 - \lambda_2 m_2 &= \lambda_1(m_1 - m_2) + \lambda_1 m_2 - \lambda_2 m_2 \\ &= \lambda_1(m_1 - m_2) + (\lambda_1 - \lambda_2) m_2 \in IM. \end{aligned}$$

Portanto $\lambda_1 m_1 + IM = \lambda_2 m_2 + IM$, e $\cdot$ está bem definida. Como M é um A-módulo, segue que M/IM é um A/I-módulo.

□

Teorema 2.2. *Sejam M um A-módulo livre e X e Y duas bases de M. Então $|X| = |Y|$.*

Demonstração. Seja I um ideal maximal de A, cuja existência é garantida pelo Lema de Zorn, e seja X uma base de M.

Mostremos primeiramente que $\{x + IM\}_{x \in X}$ é uma base do A/I-módulo M/IM e $|X| = \left|\{x + IM\}_{x \in X}\right|$.

Seja $y + IM \in M/IM$, então, como $y \in M$ temos:

$$y = \lambda_1 x_1 + ... + \lambda_n x_n \quad \text{com } \lambda_1, \lambda_2, \ldots, \lambda_n \in A \text{ e } x_1, x_2, \ldots, x_n \in X$$

$$\Rightarrow y + IM = (\lambda_1 x_1 + ... + \lambda_n x_n) + IM = (\lambda_1 + I)(x_1 + IM) + ... + (\lambda_n + I)(x_n + IM).$$

Portanto $\{x + IM\}_{x \in X}$ gera M/IM como A/I-módulo.

Para verificar que $\{x + IM\}_{x \in X}$ é uma base, falta mostrar que tal conjunto é linearmente independente.

Seja $(r_1 + I)(x_{j_1} + IM) + ... + (r_n + I)(x_{j_n} + IM) = 0$ em M/IM (com $r_1, ..., r_n \in A$ e $x_{j_1}, ..., x_{j_n} \in X$). Então $r_1 x_{j_1} + ... + r_n x_{j_n} \in IM$. Assim, podemos escrever:

$$r_1 x_{j_1} + ... + r_n x_{j_n} = i_1 x_{k_1} + ... + i_m x_{k_m},$$

com $i_1, ..., i_m \in I$ e $x_{k_1}, ..., x_{k_m} \in X$.

Pela unicidade da escrita dos elementos de M a partir de X (pois X é base) temos que $r_1, ..., r_n \in I$, e portanto $r_1 + I = ... = r_n + I = 0$ em A/I. Donde concluímos que $\{x + IM\}_{x \in X}$ é base do A/I-módulo M/IM.

Considere agora a aplicação $x \mapsto x + IM$ de X em $\{x + IM\}_{x \in X}$. É fácil ver que tal aplicação é sobrejetora. Suponha que não seja injetora. Assim, existem $x_1, x_2 \in X$ distintos tais que $x_1 - x_2 \in IM$. E, dessa forma, podemos escrever:

$$x_1 - x_2 = i_1 x_{j_1} + ... + i_n x_{j_n},$$

com $i_1, ..., i_n \in I$. E, novamente pela unicidade da escrita, teremos que $\{-1, 1\} \subseteq I$, gerando uma contradição, pois tomamos I ideal maximal de A.

Portanto, $|X| = \left|\{x + IM\}_{x \in X}\right|$.

Por fim, sejam X e Y bases do A-módulo M, então $\{x + IM\}_{x \in X}$ e $\{y + IM\}_{y \in Y}$ são bases do A/I-módulo M/IM e $|X| = \left|\{x + IM\}_{x \in X}\right|$ e $|Y| = \left|\{y + IM\}_{y \in Y}\right|$.

Como A/I é um corpo, então M/IM é um espaço vetorial, onde se verifica $\left|\{x + IM\}_{x \in X}\right| = \left|\{y + IM\}_{y \in Y}\right|$. E temos, portanto, $|X| = |Y|$.

□

Definição 2.3. Sejam M um A-módulo livre e X uma base de M definimos a dimensão de M com respeito a A por:

$$\dim(M) = |X|.$$

O seguinte exemplo mostra que para anéis não comutativos, o conceito de dimensão para A-módulos livres nem sempre está bem definido (ou seja, não é válido nesse contexto o Teorema 2.2)

Exemplo 2.4. Seja A anel e denotemos por $A^{(\mathbb{N})} = \oplus_{i \in \mathbb{N}} A$ e considere o anel $B = \mathrm{End}_A(A^{(\mathbb{N})})$ que possui uma estrutura natural de B-módulo sendo o produto externo a composição de endomorfismos. B possui duas bases finitas com diferente cardinalidade.

De fato, temos que o endomorfismo identidade constitui uma base de B por outro lado se consideramos a base canônica $\{e_i : i \in \mathbb{N}\}$ em $A^{(\mathbb{N})}$ e definimos $u, v : A^{(\mathbb{N})} \to A^{(\mathbb{N})}$ por meio de

$$u(e_{2i+1}) = 0,\ u(e_{2i}) = e_i$$

$$v(e_{2i+1}) = e_i,\ v(e_{2i}) = 0$$

então o conjunto $\{u, v\}$ é também uma base de B como B-módulo, pois $a \circ u + b \circ v = 0$ implica

$$a(e_i) = a(u(e_{2i})) = a(u(e_{2i})) + b(v(e_{2i})) = (a \circ u + b \circ v)(e_{2i}) = 0 \quad \forall\ i \in \mathbb{N}$$

$$b(e_i) = b(v(e_{2i+1})) = a(u(e_{2i+1})) + b(v(e_{2i+1})) = (a \circ u + b \circ v)(e_{2i+1}) = 0 \quad \forall i \in \mathbb{N}$$

e portanto $a = b = 0$ logo $\{u, v\}$ é l.i.. Também é gerador pois se $x \in B$ definimos $a(e_i) = x(e_{2i})$ e $b(e_i) = x(e_{2i+1})$ para $i \in \mathbb{N}$, então temos que

$$x(e_{2i}) = a(e_i) = a(u(e_{2i})) = a(u(e_{2i})) + b(v(e_{2i})) = (a \circ u + b \circ v)(e_{2i}) = 0 \quad \forall i \geq 0$$

$$x(e_{2i+1}) = b(e_i) = b(v(e_{2i+1})) = a(u(e_{2i+1})) + b(v(e_{2i+1})) = (a \circ u + b \circ v)(e_{2i+1}) = 0 \quad \forall i \geq 0$$

e portanto $x = a \circ u + b \circ v$ (por coincidir na base $\{e_i : i \in \mathbb{N}\}$). Em particular $B \cong B \times B$.

3 Propriedades de espaços vetoriais que não se preservam para A-módulos livre

Sabemos que em um espaço vetorial, um vetor não nulo forma um conjunto linearmente independente. No entanto, o mesmo não é válido para A-módulos. Nesse sentido, considere o exemplo a seguir:

Exemplo 3.1. Considere o conjunto $\mathbb{Z} \times \mathbb{Z}_2$ como $\mathbb{Z}$-módulo. Temos que:

$$2 \cdot (0, 1) = (0, 0).$$

Nesse sentido, o conjunto $\{(0, 1)\}$ é formado por um elemento não nulo de $\mathbb{Z} \times \mathbb{Z}_2$, e não é linearmente independente.

Definição 3.2. Seja M um A-módulo. Dizemos que M é livre de torção quando para todo $m \in M$ não nulo tivermos que o conjunto $\{m\}$ é l.i.

Observação 3.3. *Seja M um A-módulo. M é livre de torção se, e somente se, dados $a \in A$ e $m \in M$ tais que $am = 0$, então $a = 0$ ou $m = 0$.*

Demonstração. ($\Rightarrow$) Sejam $a \in A, m \in M$ tais que $am = 0$. Se $m = 0$ não ha nada que provar, se $m \neq 0$ como M é livre de torção então o conjunto $\{m\}$ é l.i. logo $am = 0 \Rightarrow a = 0$.

($\Leftarrow$) Vamos supor verdadeira a propriedade $am = 0 \Rightarrow a = 0$ ou $m = 0$ para todo $a \in A, m \in M$, então $\forall m \in M, m \neq 0$ vai-se verificar que $am = 0 \Rightarrow a = 0$ logo o conjunto $\{m\}$ é l.i. e portanto M é livre de torção. □

3.1 Extensão de um conjunto l.i. a uma base

Um resultado clássico sobre espaços vetoriais é que todo conjunto linearmente independente pode ser estendido a uma base.

No entanto, vale ressaltar que esse resultado não é válido em geral para A-módulos. Vejamos o exemplo a seguir:

Exemplo 3.4. Consideremos os inteiros de Gauss $\mathbb{Z}+i\mathbb{Z}$ como $\mathbb{Z}$-módulo. Note inicialmente que o conjunto $2+2i$ é linearmente independente o qual é consequência direita de ser $\mathbb{C}$ um corpo (se $a, z \in \mathbb{C}$ com $a \neq 0$, $az = 0 \Rightarrow z = a^{-1}az = a^{-1} \cdot 0 = 0$).

Vimos anteriormente que em um A-módulo livre, toda base tem a mesma cardinalidade. Ademais, $\mathbb{Z}^2$ é um $\mathbb{Z}$-módulo livre com base $C = \{1, i\}$. Nesse sentido, toda base deve ter dois elementos.

Suponha que existe $a + bi \in \mathbb{Z} + i\mathbb{Z}$ tal que o conjunto $B = \{2 + 2i, a + bi\}$ forme uma base. Nesse sentido, temos que os elementos de C podem ser escritos em função dos elementos de B. Dessa forma, existem $m, n, p, q \in \mathbb{Z}$ tais que:

$$\begin{cases} m(2+2i) + n(a+bi) = 1 \\ p \cdot (2+2i) + q \cdot (a+bi) = i \end{cases}.$$

Matricialmente (igualando parte real é imaginária), a expressão acima é equivalente a:

$$\begin{pmatrix} m & n \\ p & q \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ a & b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Mas note que a segunda matriz tem determinante par. Como o produto dos determinantes é o determinante do produto, segue que a primeira matriz, formada por coeficientes inteiros, não tem determinante inteiro, o que é absurdo.

Segue que o conjunto $\{2 + 2i\}$ não pode ser estendido a uma base de $\mathbb{Z} + i\mathbb{Z}$.

3.2 Redução de um conjunto gerador a uma base

Outro resultado conhecido sobre espaços vetoriais é que todo conjunto que gera o espaço pode ser reduzido a uma base. No entanto, mais uma vez, esse resultado não é válido em geral para A-módulos. A esse respeito, considere o exemplo:

Exemplo 3.5. Consideremos novamente os inteiros de Gauss $\mathbb{Z} + i\mathbb{Z}$ como $\mathbb{Z}$-módulo. Temos inicialmente que o conjunto $X = \{2 + 2i, 3 + 3i, i\}$ é um gerador do espaço.

Para verificar esse fato, como $i \in X$, basta observar que o elemento 1 e i pode ser escrito como combinação linear de elementos de X. Nesse sentido:

$$1 = (3 + 3i) - (2 + 2i) - i.$$

No entanto, temos que X não pode ser reduzido a uma base. Vamos verificar todas as possibilidades:

- $X_1 = \{2+2i, 3+3i\}$ não é base, pois todos as combinações lineares desses elementos são da forma $z + zi$;
- $X_2 = \{2+2i, i\}$ não é base, pois as combinações lineares desses elementos são da forma $2z + i(2z + y)$, ou seja, a parte real é par;
- $X_3 = \{3+3i, i\}$ não é base, pois as combinações lineares desses elementos são da forma $3z + i(3z + y)$, ou seja, a parte real é múltiplo de 3.

Portanto, segue que o conjunto $\alpha = \{2+2i, 3+3i, i\}$, que é um gerador do espaço, não pode ser reduzido a uma base de $\mathbb{Z} + i\mathbb{Z}$.

3.3 Submódulos de um módulo livre

Nem sempre um submódulo de um módulo livre é livre. Considere o exemplo:

Exemplo 3.6. Consideremos o anel dos inteiros módulo 6, $\mathbb{Z}_6$. $\mathbb{Z}_6$ é um $\mathbb{Z}_6$-módulo livre com base $\{\overline{1}\}$ (observe, no entanto, que $\mathbb{Z}_6$ como $\mathbb{Z}_6$-módulo, não é livre de torção).

No entanto, $N = \{\overline{0}, \overline{2}, \overline{4}\}$ é um $\mathbb{Z}_6$-submódulo de $\mathbb{Z}_6$ que não é livre. De fato, todo subconjunto unitário de N é linearmente dependente ($\overline{3}.n = 0$ para todo $n \in N$).

3.4 Quociente de um módulo livre por um submódulo livre

O fato de termos um módulo livre M e um submódulo livre N, nem sempre implica que o quociente M/N é livre. De fato, considere o exemplo a seguir.

Exemplo 3.7. Considere $\mathbb{Z}$ como um $\mathbb{Z}$-módulo livre com base $\{1\}$. Seja $n > 0$, um inteiro e considere o $\mathbb{Z}$-submódulo livre (n) (de fato, {n} é uma base para (n)).

Observamos que $\mathbb{Z}/(n) = \mathbb{Z}_n$ não é livre como $\mathbb{Z}$-módulo. De fato, todo conjunto $\{\overline{k}\} \subset \mathbb{Z}/(n)$ formado por um elemento é l.i. pois $n.\overline{k} = \overline{nk} = \overline{0}$ para todo $\overline{k} \in \mathbb{Z}/(n)$.

4 Módulo sobre domínio de ideais principais.

Nesta seção, vamos ver primeiro, uma condição sobre o anel A de escalares para garantir que todo A-módulo seja livre e finalizar com um teorema sobre a obtenção de uma base para um submódulo a partir de uma base do módulo.

4.1 Condição suficiente para garantir existência de base.

Já sabemos que se A for corpo, então todo A-módulo tem uma base (por ser um espaço vetorial), mas podemos enfraquecer esta condição.

Vamos nos concentrar em um caso especial, onde A é um domínio de ideais principais (ou seja, todo ideal de A está gerado por um só elemento). Portanto, nesta seção A será um domínio de ideais principais.

Somente pedir que A seja um domínio de ideais principais não é suficiente como vimos no exemplo 1.9. A seguinte proposição nos dá uma condição necessária.

Proposição 4.1. *Se M é um A-módulo com torção então M não é livre como A-módulo.*

Demonstração. Vamos supor por absurdo que M é livre, e seja B uma base para M. Como M tem torção, então existe $a \in A$ e $m \in M$ tal que $am = 0$, mas $a \neq 0$ e $m \neq 0$. Como $m \in M$ e B é base para M, então existem $m_1, m_2, \ldots, m_n \in M$ tais que $m = \sum_{i=1}^{n} a_i m_i$ com $a_i \in A$ para todo $i = 1, \ldots, n$. Logo $\sum_{i=1}^{n} aa_i m_i = am = 0$ implica $aa_i = 0 \ \forall i = 1, \ldots, n$ (pois B é base, e em particular linearmente independente). Como $a \neq 0$ e A é um domínio então $aa_i = 0 \Rightarrow a_i = 0$ para $1 \leq i \leq n$ o qual implica que $m = \sum_{i=1}^{n} a_i m_i = 0$, gerando uma contradição. Por tanto M não pode ser livre como A-módulo, como queríamos demonstrar. □

Agora é natural fazermos a pergunta se todo A-módulo sem torção vai ser livre (lembrar que A é domínio de ideais principais). Vamos provar que a resposta é afirmativa no caso em que o A-módulo for finitamente gerado.

Primeiramente, vamos provar o seguinte lema:

Lema 4.2. *Se M é um A-módulo livre finitamente gerado e N é um submódulo de M, então N também é livre e $dim(N) \leq dim(M)$.*

Demonstração. Vamos fazer a prova por indução em $n = dim(M)$. Para $n = 0$ o resultado é trivial. Vamos supor que a afirmação é verdadeira se o módulo tiver dimensão $n - 1 \geq 0$ e provaremos que a afirmação é verdadeira quando a dimensão é n.

Sejam então M um A-módulo livre com $dim(M) = n$, $B = \{m_1, m_2, \ldots, m_n\}$ uma A-base para M e N um submódulo de M. Consideremos o morfismo projeção na primeira variável $\pi_1 : M \to A$ definido por $\pi_1(\sum_{i=1}^{n} a_i m_i) = a_1$.

Observe que, como $\pi_1 : M \to A$ é um homomorfismo de A-módulo (Observação 1.10) e N é um A-submódulo de M, então $\pi_1(N)$ será um A-submódulo de A, ou seja, um ideal de A. Como A é um domínio de ideais principais, então existe um $d \in A$ tal que $\pi_1(N) = \langle d \rangle$.

Se $d = 0$, então $\pi_1(n) = 0$ para todo $n \in N$. Logo N vai ser um A-submódulo do A-módulo gerado pelo conjunto $\{m_2, m_3, \ldots, m_n\}$, que é livre de dimensão $n-1$. Portanto, N vai ser livre de dimensão menor ou igual a $n-1$ (em particular $dim(N) \leq dim(M) = n$) pela hipótese de indução.

Se $d \neq 0$, então podemos tomar $n_0 \in N$ tal que $\pi_1(n_0) = d$. Vamos considerar os A-submódulos $M' = \langle m_2, m_3, \ldots, m_n \rangle$ e $N' = N \cap M'$ de M. Como N' é um A-submódulo de M' que é livre

com $dim(M') = n-1$, então pela hipótese indutiva o mesmo N' vai ter que ser livre de dimensão menor ou igual que $n-1$. Seja $\{e_2, e_3, \ldots, e_m\}$ uma base de N', onde $m \leq n$.

Vamos provar que o conjunto $\mathcal{B} = \{n_0, e_2, e_3, \ldots, e_m\}$ será uma base para N (em particular M vai ser livre de dimensão $m \leq n$). Como $N' \subset N$ e $n_0 \in N$ é claro que $\mathcal{B} \subset N$. Vamos provar agora que é gerador:

De fato, se $n \in N$ então $\pi_1(n) = sd$ para algum $s \in A$ (pois $\pi_1(n) \in \pi_1(N) = \langle d \rangle$), logo $\pi_1(n - sn_0) = \pi_1(n) - s\pi_1(n_0) = sd - sd = 0$. Portanto, temos que $n - sn_0 \in M'$ (pois, como é fácil ver, $\ker(\pi_1) = M'$). Observemos que também $n - sn_0 \in N$ (pois $n \in N$ e $n_0 \in N$). Logo, $n - sn_0 \in M' \cap N = N' = \langle e_2, \ldots, e_m \rangle$, implicando claramente que $n \in \langle n_0, e_2, \ldots, e_m \rangle$. Segue que $\mathcal{B}$ gera N.

Agora, vamos provar que $\mathcal{B} = \{n_0, e_2, e_3, \ldots, e_m\}$ é linearmente independente:

Sejam $\alpha_1, \alpha_2, \ldots, \alpha_m \in A$ tal que

$$\alpha_1 n_0 + \sum_{i=2}^{m} \alpha_i e_i = 0 \tag{1}$$

Como $\pi_1(n_0) = d \Rightarrow dm_1 - n_0 \in M' = \langle m_2, \ldots, m_n \rangle$ então $\alpha_1 dm_1 = \alpha_1 dm_1 - (\alpha_1 n_0 + \sum_{i=2}^{m} \alpha_i e_i) = \alpha_1(dm_1 - n_0) - \alpha_2 e_2 - \ldots - \alpha_m e_m \in M'$ pois $dm_1 - n_0, e_2, e_3, \ldots, e_m \in M'$ (lembrar que $N' \subset M'$). Mas $\alpha_1 dm_1 \in M' \Rightarrow \pi_1(\alpha_1 dm_1) = \alpha_1 d = 0$, como A é domínio de integridade e $d \neq 0$ temos que $\alpha_1 = 0$. Voltando a equação (1) temos que $\sum_{i=2}^{m} \alpha_i e_i = 0$, implicando que $\alpha_2 = \ldots = \alpha_m = 0$, pois $\{e_2, \ldots, e_m\}$ são linearmente independentes. Logo, também o conjunto $\mathcal{B}$ vai ser linearmente independente.

Como $\mathcal{B} \subset N$ é gerador e linearmente independente, então é uma base e, portanto, o A-submódulo N vai ser livre com $\dim(N) = m \leq n$.

□

Finalmente vamos provar que a condição de ser M um A-módulo livre de torção finitamente gerado (com A domínio de ideais principais) é suficiente para garantir a existência de uma base.

Teorema 4.3. *Se M é um A-módulo livre de torção e finitamente gerado (com A domínio de ideias principais) então M é livre.*

Demonstração. Seja $S = \{y_1, y_2, \ldots, y_m\}$ um conjunto gerador de M como A-módulo (tal conjunto existe, pois M é finitamente gerado como A-módulo) e seja $S' = \{v_1, \ldots, v_n\}$ um subconjunto de S maximal com a propriedade de ser linearmente independente. Observe que como A é livre de torção, então $\{y_1\} \subset S$ vai ser linearmente independente. Portanto, a família de subconjuntos de S que são linearmente independentes será não vazia e finita, tendo um elemento maximal. Vamos

denominar por N o A-submódulo de M gerado pelo conjunto S', ou seja $N = \langle v_1, \ldots, v_n \rangle$.

Afirmação: Para cada i, $1 \leq i \leq m$, existe um $d_i \in A$ diferente de zero tal que $d_i y_i \in N$.

De fato, se $y_i = v_j \in N$ para algum $j \in \{1, \ldots, n\}$, basta tomar $d_i = 1$. Se $y_i \notin S'$, temos que pela maximalidade o conjunto $\{y_i\} \cup S'$ vai ser linearmente dependente. Portanto, existem escalares $d_i, c_1, \ldots, c_n$ não todos nulos tais que

$$d_i y_i + c_1 v_1 + \ldots + c_n v_n = 0.$$

Observemos que $d_i \neq 0$, pois se $d_i = 0$, como $\{v_1, \ldots, v_n\}$ é linearmente independente, então $c_1 = \ldots = c_n = 0$, contradizendo o fato de não serem todos nulos. Além disso, $d_i y_i = -c_1 v_1 - \ldots - c_n v_n \in N$, o que prova a afirmação.

Se pegarmos $d = d_1 d_2 \ldots d_m$ (que serão diferentes de zero pois $d_i \neq 0 \ \forall i$ e A e domínio de integridade), então $dy_i \in N$. Com efeito, seja $k_i \in A$ tal que $d = d_i k_i$. Como $d_i y_i \in N$, então $dy_i = k_i(d_i y_i) \in N$. Vamos provar que a função:

$$f : M \to N, \quad m \mapsto dm$$

é um homomorfismo injetivo de A-módulos (e portanto $Im(f) \simeq M$).

- Bem definida: Se $m \in M$, então $m = \sum_{i=1}^{m} a_i y_i$ (com $a_i \in A$ para $1 \leq i \leq m$), aplicamos f de ambos lados e então $f(m) = dm = \sum_{i=1}^{m} da_i y_i = \sum_{i=1}^{m} a_i(dy_i) \in N$, pois $dy_i \in N$ para $1 \leq i \leq m$.
- Linearidade: $f(a_1 m_1 + a_2 m_2) = d(a_1 m_1 + a_2 m_2) = da_1 m_1 + da_2 m_2 = a_1(dm_1) + a_2(dm_2) = a_1 f(m_1) + a_2 f(m_2)$
- Injetividade: Se $f(m) = dm = 0$, como $d \neq 0$ e M é livre de torção, então $m = 0$. Portanto $\ker(f) = \{0\}$ e f é injetora.

Como f é homomorfismo de A-módulos, temos que $Im(f)$ é um A-submódulo de N. Ademais, como N é livre, pelo lema prévio temos que $Im(f)$ é livre, e como f é homomorfismo injetivo de A-módulo, segue que $M \simeq Im(f)$ e, portanto, o próprio M vai ser livre como A-módulo.

□

Exemplo 4.4. Se o A-módulo não for finitamente gerado temos, em geral, que o teorema anterior não é válido. Considere $\mathbb{Q}$ como $\mathbb{Z}-$módulo, então qualquer par de elementos $\frac{p}{q}, \frac{r}{s} \in \mathbb{Q}$ (com $p, q, r, s \in \mathbb{Z}$) são linearmente dependentes, pois se algum deles fosse 0 então é trivial, caso contrario $qr\frac{p}{q} + (-sp)\frac{r}{s} = 0$ com qr e sp inteiros não nulos. Portanto si $\mathbb{Q}$ fosse um $\mathbb{Z}$-módulo livre, qualquer base de $\mathbb{Q}$ deveria ter um só elemento (não nulo). Seja $\{\frac{p}{q}\}$ dita base com $\text{mcd}(p, q) = 1$ e $q > 0$, então existe um inteiro k tal que $k\frac{p}{q} = \frac{1}{2q}$ que implica $2pk = 1$ o qual é absurdo (pois 1 é impar). Assim $\mathbb{Q}$ não pode ser um $\mathbb{Z}-$módulo livre. Finalmente, observe que pelo fato de $\mathbb{Q}$ ser um domínio integral temos que $\mathbb{Q}$ como $\mathbb{Z}-$módulo é livre de torção.

4.2 Construção de uma base para um submódulo de um módulo livre sobre um domínio de ideais principais.

A partir de agora, vamos mostrar que, dado M um A-módulo livre finitamente gerado, e um submódulo N, é possível construir, sob certas condições, uma base para N a partir de uma base de M.

Lema 4.5. *Seja A um d.i.p.. Se M é um A-módulo livre finitamente gerado e $N \subset M$ um A-submódulo não-nulo, então existem $l \in M$ com $l \neq 0$ e uma aplicação $f : M \to A$, A-linear e $d \in A$ não-nulo, tais que:*

1. $f(N) = \langle d \rangle$ *e* $f(l) = 1$;
2. $M = \langle l \rangle \oplus ker(f)$;
3. $N = \langle dl \rangle \oplus (ker(f) \cap N)$.

Demonstração. Suponha que $dim(M) = n \geq 1$.

Consideremos a seguinte família de ideais de A:

$$J = \{I \subset A : I = f(N) \text{ onde } f \in Hom_A(M, A)\}.$$

Sendo M livre, então existe um conjunto $\{m_i\}_{i=1}^n \subset M$ que forma uma base para M, assim

$$M = \bigoplus_{i=1}^{n} \langle m_i \rangle.$$

Consideremos $p_i : M \to A$ as projeções em A, ou seja, $p_i(m) = p_i(\sum_{i=1}^{n} a_j m_j) = \delta_{ij} a_j = a_i$. Do fato de N ser um A-submódulo não-nulo, segue que existe $i_0 \in I_n$ tal que $p_{i_0}(N) \neq 0$. Portanto, a família J contém um ideal não-nulo.

A família J possui um elemento maximal. De fato, caso contrário existe uma cadeia

$$I_1 \subsetneq I_2 \subsetneq ... \subsetneq I_k \subsetneq ...$$

de elementos de J. Porém, tomemos $I = \cup_{k \in \mathbb{N}} I_k$. Como A é *d.i.p.*, então $I = (a)$, logo existe $k_0 \in \mathbb{N}$ tal que $a \in I_{k_0}$, o que implica que $I \subset I_{k_0}$ e portanto $I_k = I_{k_0}$ para todo $k \geq k_0$, já que $I_k \subset I$, chegando no absurdo desejado.

Assim, existe $I_0 = f_0(N) \in J$ com $f_0 \in Hom_A(M, A)$ que é elemento maximal de J. Observe que I_0 é um ideal de A e portanto, existe $d \in A$ tal que $I_0 =< d >$. Como $p_{i_0}(N) \neq \emptyset$, pela maximalidade de I_0 segue que $I_0 = f_0(N) \neq \{0\}$, logo $d \neq 0$.

Agora, mostraremos que existe $l \neq 0$ tal que $l \in M$ com $f_0(l) = 1$. Como $d \in f_0(N)$, existe $m \in N$ tal que $f_0(m) = d$.

Consideremos $g \in Hom_A(M, A)$ arbitrária. Vamos mostrar que d divide $g(m)$. Seja $(d, g(m))$ o ideal gerado por d e $g(m)$. Sendo A *d.i.p.* temos $\tilde{d} = (d, g(m))$, assim

$$\tilde{d} = bd + cg(m),\ b, d \in A.$$

Observe que de $\tilde{d} = bd + cg(m)$, temos que $\tilde{d} = (bf_0 + cg)(m)$. Chamaremos de $w = bf_0 + cg$, é claro que $w \in Hom_A(M, A)$. Como $\tilde{d}$ divide d, então $f_0(N) = \langle d \rangle \subset \langle \tilde{d} \rangle \subset w(N)$. Pela maximalidade de I_0, segue que $\langle d \rangle = \langle \tilde{d} \rangle$. Logo d divide $\tilde{d}$, consequentemente d divide $g(m)$.

Como $g \in Hom_A(M, A)$ é arbitrária, em particular, d divide $p_i(m)$, $\forall i \in I_n$. Logo, $p_i(m) = db_i$ com $b_i \in A$.

Dado $m \in M \subset L$, temos

$$m = (\sum_{i=1}^{n} a_j m_j) = \sum_{i=1}^{n} (p_j(m))m_j = \sum_{i=1}^{n} (db_j)m_j = d(\sum_{i=1}^{n} b_j m_j)$$

Defina $l = \sum_{i=1}^{n} b_j m_j$, logo $m = dl$. Por fim, $d = f_0(m) = f(dl) = d(f_0(l))$, implica que $f_0(l) = 1$. Deste modo, encerramos a demonstração do primeiro item do lema.

Observemos agora que $l \in M$, logo $\langle l \rangle \subset M$. Ainda mais, de $f_0 \in Hom_A(M, A)$, é claro que $ker(f_0) \subset M$. Do item anterior, $f_0(l) = 1$, implica que $\langle l \rangle \cap ker(f_0) = \{0\}$, logo $\langle l \rangle \oplus ker(f_0) = \langle l \rangle + ker(f_0) \subset M$.

Dado $x \in M$, podemos escrever $x = x + (f_0(x))l - (f_0(x))l = (x - (f_0(x))l) + (f_0(x))l$. Pondo $y = x - (f_0(x))l$, segue que

$$f_0(y) = f_0(x - (f_0(x))l) = f_0(x) - (f_0(x)(f_0(l)) = 0.$$

Assim, $y \in ker(f_0)$ e $z = (f_0(x))l \in \langle l \rangle$, implicam que $M \subset \langle l \rangle \oplus ker(f_0)$. Assim, concluímos que

$$M = \langle l \rangle \oplus ker(f_0).$$

Para demonstrar o último item, basta observar que $m = dl \in N$ e que $ker(f_0) \cap N \subset N$. Como $\langle dl \rangle \subset \langle l \rangle$ e $(ker(f_0) \cap N) \subset ker(f_0)$, segue que $\langle dl \rangle \cap ker(f_0) \cap N = \{0\}$. Portanto, a soma de $\langle dl \rangle$ e $(ker(f_0) \cap N)$ é uma soma direta.

Dado $y \in N$, temos que $f_0(y) \in f_0(N) = \langle d \rangle$, logo existe $b \in A$ tal que $f_0(y) = b.d$. Podemos escrever $y = y + b.m - bm = (y - bm) + bm$ com $bm \in \langle dl \rangle$.

É claro que $y - bm \in N$ e $f_0(y - bm) = f_0(y - (bd)l) = f_0(y - (f_0(y))l) = f_0(y) - (f_0(y))f_0(l) = 0$, implica $y - bm \in ker(f_0)$. Assim, $y - bm \in ker(f_0) \cap N$.

Obtemos que $y = (y - b.m) + bm \in \langle dl \rangle \oplus (ker(f_0) \cap N)$ e então $N \subset \langle dl \rangle \oplus (ker(f_0) \cap N)$. Daí segue a igualdade

$$N = \langle dl \rangle \oplus (ker(f_0) \cap N).$$

Assim, tomando $f = f_0$ temos as propriedades requeridas.

□

Teorema 4.6. *Seja A um d.i.p, M um A-módulo livre finitamente gerado ($dim(M) = m$) e N um A-submódulo com $dim(N) = n \geq 1$. Então existem uma base $\{e_i\}_{i=1}^{m}$ de M, um subconjunto $\{e_{i_j}\}_{j=1}^{n} \subset \{e_i\}_{i=1}^{m}$ e elementos $\{d_j\}_{j=1}^{n} \subset A \setminus \{0\}$ tais que $d_j | d_{j+1}$ para $j = 1, \cdots, n-1$ tais que $\{d_j.e_{i_j}\}_{i=1}^{n}$ é uma base para N.*

Demonstração. Como M é livre e finitamente gerado, pelo Lema 4.5 $M = \langle l \rangle \oplus ker(f)$. Assim, pelo Teorema 4.3, $ker(f)$ é um submódulo livre. Portanto, existe uma base $\{\alpha_i\}_{i=1}^{m-1}$ para $ker(f)$. Assim, o conjunto $\{e_i\}_{i=1}^{m} \subset M$ tal que $e_1 = l$ e $e_{i+1} = \alpha_i$ é uma base para M.

Segue também pelo Teorema 4.3 que N é livre finitamente gerado com $dim(N) \leq dim(M)$.

A demonstração será feita usando indução na $dim(N) = n$.

Suponhamos primeiramente que $n = 1$. Pelo terceiro item do Lema 4.5, $N = \langle d.l\rangle \oplus (ker(f) \cap N)$ para $d \in A$ e $l \in M$ não-nulos.

Observemos que se L é um A-módulo finitamente gerado tal que $L = L' \oplus L''$ com L' e L'' A-submódulos de L, então $dim(L) = dim(L') + dim(L'')$.

Daí $dim(N) = dim(\langle d.l\rangle) + dim(ker(f) \cap N))$, o que implica $dim(ker(f) \cap N) = 0$. Portanto $N = \langle d.l\rangle$ com $l \in \{e_i\}_{i=1}^{n}$.

Suponhamos agora que o resultado seja válido para $n = k - 1$. Se $dim(N) = k$, o Lema 4.5 nos permite escrever $N = \langle d.l\rangle \oplus (ker(f) \cap N)$. Ainda, $(ker(f) \cap N) \subset N$ que é livre finitamente gerado, portanto $ker(f) \cap N$ é um A-submódulo livre finitamente gerado. Daí

$$dim(N) = dim(\langle d.l\rangle) + dim(ker(f) \cap N).$$

Donde segue que $dim(ker(f) \cap N) = k - 1$. Utilizando a hipótese de indução, existem $\{e'_{i_j}\}_{j=1}^{k-1}$ elementos da base de M e escalares $\{d'_j\}_{j=1}^{k-1} \subset A \setminus \{0\}$ com $d'_j | d'_{j+1}$ para $j = 1, \cdots, k-2$, tais que

$$ker(f) \cap N = \bigoplus_{j=1}^{k-1} \langle d'_j.e'_{i_j}\rangle.$$

Consideremos $\{d_j\}_{j=1}^{k} \subset A \setminus \{0\}$, com $d_1 = d$ e $d_{j+1} = d'_j$ e também $\{e_{i_j}\}_{j=1}^{k}$ subconjunto da base de M, onde $e_{i_1} = l$ e $e_{i_j} = e'_{i_j}$. Assim

$$N = \bigoplus_{j=1}^{k} \langle d_j.e_{i_j}\rangle.$$

Falta mostrar que $d_1 = d$ divide d_2. Pelo Lema 4.5, temos $f(N) = \langle d_1\rangle$ e como $d_2.e_{i_2} \in N$ e e_{i_2} é um elemento da base de M. Então $f(d_2.e_{i_2}) = d_2 \in \langle d_1\rangle$, logo $d_1 | d_2$, o que conclui a demonstração.

□

5 Conclusão.

O conceito de base para A-módulos pode ser obtido como uma generalização natural do mesmo conceito para espaços vetoriais, mas no caso em que A não é um corpo, nem sempre é possível obter uma base. No caso de existir uma base, é possível generalizar alguns resultados de Álgebra Linear, como a igualdade entre a cardinalidade das bases, como foi feito na seção 2 (a comutatividade do anel é essencial, como foi mostrado no Exemplo 2.4). No entanto, no nosso caso, as coisas ficam muito mais complicadas, já que mesmo as propriedades mais básicas dos espaços vetoriais podem falhar, como vimos na seção 3, mesmo que o anel de escalares seja um domínio de ideais principais. O caso em que o anel de escalares é um domínio de ideais principais é muito mais simples que o caso genérico; neste contexto é possível obter condições suficientes para garantir a existência da base, é valida a propriedade de que um submódulo de um módulo livre finitamente gerado é também livre finitamente gerado, e é possível obter uma base do submódulo a partir de uma base especial do módulo.

Referências

[1] Salvatore, Flavia A. - Olea, María M., *Anillos y Módulos semisimples - Módulos f.g. sobre un d.i.p.*, Trabajo Final - Estruturas Algebraicas - Facultad de Ciencias Exactas, Universidad Nacional de La Plata.

[2] M.F. Atiyah, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[3] Arnaldo Garcia, Yves Lequain, *Elementos de Álgebra*, (Projeto Euclides) Rio de Janeiro, RJ: IMPA, 2003, 2ª ed.

[4] T.W.Hungerford, *Álgebra*, Springer-Verlag.