V Bienal da SBM
Sociedade Brasileira de Matemática
UFPB - Universidade Federal da Paraíba
18 a 22 de outubro de 2010

UMA BREVE INTRODUÇÃO A ESTRUTURAS ALGÉBRICAS DE MÓDULOS SOBRE ANÉIS - GENERALIZANDO O CONCEITO DE ESPAÇO VETORIAL

L. C. R. Goulart * S. L. de Oliveira † & R. Thibes ‡

1 Módulos

Definição 1.1. *Um módulo M^1 sobre um anel R é um conjunto não vazio satisfazendo as seguintes condições:*
M1) M *é um grupo aditivo abeliano.*
M2) $r(x+y) = rx + ry, .(r+s)x = rx + sx,$
M3) $r(sx) = (rs)x,$
M4) $1.x = x$

1.0.1 Propriedades Básicas

1) $r.O = O$
2) $O.r = O$
3) $(-r)x = r.(-x) = -(r.x)$

Observação 1.1. *Às vezes, a noção de módulos se define para anéis sem unidade. Neste caso, se omite a condição M4 da definição de módulo.*

Exemplo 1.1. *Se M é um espaço vetorial sobre um corpo K, então M é um K-módulo.*

Exemplo 1.2. *Qualquer anel R é um módulo sobre si mesmo.*

Exemplo 1.3. *Se R ó um anel, então R é um R-módulo.*

Exemplo 1.4. *Seja $M_{mxn}(R)$ o conjunto das matrizes mxn com entradas em um anel R. Então M é um R-módulo.*

Exemplo 1.5. *Qualquer grupo abeliano G é sempre um Z-módulo.*

$$nx = \begin{cases} \overbrace{x + \ldots + x}^{nvezes}, n > 0 \\ \underbrace{(-x) + \ldots + (-x)}_{nvezes}, n < 0 \\ 0, n = 0 \end{cases} \tag{1.1}$$

Exemplo 1.6. *Se I é um ideal à esquerda de R, então I é um R-módulo à esquerda.*

Exemplo 1.7. *Seja G um grupo abeliano e End(G) o conjunto de todos endomorfismos de G.*

*Universidade Estadual do Sudoeste da Bahia , DEBI, BA, Brasil, lauragou@gmail.com
†Universidade Estadual do Sudoeste da Bahia , DEBI, BA, Brasil, oliveira@uesb.edu.br
‡Universidade Estadual do Sudoeste da Bahia , DEBI, BA, Brasil, thibes@uesb.edu.br
[1] Módulo significará sempre um módulo à esquerda exceto quando é dito contrário.

Afirmação: End(G) possui uma estrutura de anel.

Podemos definir em G uma estrutura de End(G)-módulo associando a cada par (f,x) End(G)xG o elemento f.x=f(x) G.

2 Álgebras

Uma álgebra sobre um anel comutativo é um módulo com uma operação binária de multiplicação de elementos que tem a propriedade distributiva e associativa quando faz sentido

Definição 2.1. *Dizemos que M é uma álgebra sobre um anel comutativo R se M é um R-módulo que também é um anel e as operações de anel e módulo são compatíveis, i.e.,*

$$r(xy) = x(ry); \forall x, y \in M \;\; e \; r \in R \tag{2.2}$$

Exemplo 2.1. *Todo anel comutativo é uma álgebra sobre si mesmo.*

Exemplo 2.2. *Qualquer anel R é sempre uma $\mathbb{Z}$-álgebra.*

Exemplo 2.3. *O anel $M_n(\mathbb{R})$ (matrizes nxn com entradas em $\mathbb{R}$) é uma R-álgebra.*

Exemplo 2.4. *O anel de polinômios $R[x]$ e o anel de séries de potências $R[[x]]$ são R-álgebras.*

Observação 2.1. *Podemos definir uma álgebra sobre um corpo e usar propriedades de espaços vetoriais. Existem propriedades que diferenciam uma álgebra sobre um anel de uma álgebra sobre um corpo.*

Proposição 2.1. *Seja K um corpo. Se A é uma K-álgebra e M tem uma estrutura de módulo sobre A, então M é um espaço vetorial sobre K.*

3 Submódulos

Assumiremos que todos os anéis envolvidos neste texto sóo comutativos. Assim, não haverá distinção entre módulos à esquerda e módulos à direita.

Definição 3.1. *Seja M um R-módulo. Um subconjunto $N \subset M$ não vazio é dito um submódulo de M se: $rx+sy \in N$ para todo $x, y \in N$ e $r, s \in R$.*

Em outras palavras, um submódulo com as operações herdadas do módulo, é também um R-módulo.

Observação 3.1. *N é um submódulo de M se as seguintes condições são satisfeitas:*
i) N é um subgrupo aditivo de M.
ii) N é fechado em relação em relação à multiplicação por escalar.

Observação 3.2. *Ao admitirmos que o anel é comutativo ganhamos algumas propriedades. Por exemplo, se estamos com um módulo livre, podemos falar em dimensão se o anel é comutativo.*

Observação 3.3. *Se M é uma R-álgebra, diremos que $N \subset M$ é uma subálgebra se N for um submódulo que também é um subanel.*

Exemplo 3.1. *Seja V um espaço vetorial sobre um corto $\mathbb{K}$. Um subconjunto $S \subseteq V$ é um submódulo sse S é um subspaço de V.*

Exemplo 3.2. *Seja G um grupo abelinao. Então os $\mathbb{Z}-$submódulos de G são precisamente seus subgrupos.*

Exemplo 3.3. *Seja R um anel. Os $R-$submódulos de R são precisamente os ideais á esquerda.*

Exemplo 3.4. *Sejam M_1, M_2 submódulos de um $MR-$módulo. Então o conjunto $N_1 + N_2 = \{n_1 + n_2, n_1 \in N_1$ e $n_2 \in N_2\}$ também é um submódulo M denominado submódulo soma de N_1 e N_2.*

Exemplo 3.5. *Seja S um subconjunto de M um $R-$módulo. Então , $(S) = \{\sum_{i=1}^{n} r_i s_i \mid n \in \mathbb{N}; r_i \in R$ e $s_i \in S\}$ é um submódulo denominado submódulo gerado por S.*

4 Homomorfismo de Módulos

Definição 4.1. *Sejam M_1 e $M-2$ $R-$módulos. Uma aplicação $\varphi : M_1 \to M_2$ é um homomorfismo de $R-$módulos se:*

i) $\varphi(x+y) = \varphi(x) + \varphi(y), \forall x, y \in M_1$

ii) $\varphi(rx) = r\varphi(x), \forall x \in M_1$ e $\forall r \in R$

Exemplo 4.1. *R um corpo. É um homomorfismo de R-módulos $\Leftrightarrow$ é uma transformações lineares*

Exemplo 4.2. *Os homomorfismos de grupos abelianos são homomorfismos entre os $\mathbb{Z}-$módulos*

Exemplo 4.3. *Homorfimso canônico*

N é um submódulo de M um $R-$módulo

$$\begin{aligned} \varphi_0 : M &\longrightarrow M/N \\ x &\longmapsto x + N \end{aligned} \tag{4.3}$$

Exemplo 4.4. [Homotetia]

M é um $R-$módulo e $r \in R$

$$\varphi_r : M \mapsto M/\varphi_r(x) = rx \tag{4.4}$$

R comutativo $\Rightarrow \varphi_r$ é um homomorfismo de $R-$módulos

$$\varphi_r(x+y) = r(x+y) = rx + ry = \varphi_r(x) + \varphi_r(y) \tag{4.5}$$

$$\varphi_r(ax) = r(ax) = (ra)x = (ar)x = a(rx) = a\varphi_r(x) \tag{4.6}$$

4.1 Teoremas Fundamentais para Módulos

Sejam M_1, M_2 $R-$módulos e N um submódulo de M_1. Considere $\varphi : M_1 \to M_2$ um homomorfismos de $R-$módulos tal que o kernel contém N. Então existe um único $\bar{\varphi} : M_1/N \to M_2$ homomorfismo de $R-$módulos tal que $\bar{\varphi}(x+N) = \varphi(x)$

Teorema 4.1 (1º Teorema do Homorfismo). *Se $\varphi : M_1 \to M_2$ é um homomorfismo de $R-$módulos com kernel N, então $Im\varphi \simeq M_1/N$.*

Teorema 4.2 (2º Teorema do Homorfismo).

$$(S+T)/T \simeq S/(S \cap T) \tag{4.7}$$

$$x \in \ker\varphi \subset S \Leftrightarrow x + T = T \Leftrightarrow x \in T \Leftrightarrow x \in S \cap T \tag{4.8}$$

É claro que Im $\varphi = S + T/T$.

Teorema 4.3 (3º Teorema do Homorfismo). *Se N é um submódulo de L e L é um submódulo de M então*

$$M/L \simeq (M/N)/(L/N) \tag{4.9}$$

4.2 Anulador

Seja M um $R-$módulo.

Definição 4.2. *O conjunto $R-$módulo $Ann(M) = \{r \in R \mid rm = 0, \forall m \in M\}$ é chamado de anulador do módulo M.*

Exemplo 4.5. *Considere $M = |_n$ o $\mathbb{Z}-$módulo e fica claro que $Ann(\mathbb{Z}_n) = n\mathbb{Z}$.*

Exemplo 4.6. *Sejam $\mathbb{K}$ um anel de divisão e $M_2(\mathbb{K})$ o anel das matrizes. Consideremos $I = \{A \in M_2(\mathbb{K})/a_{11} = a_{22} = a_{21} = 0$ e $a_{12} \neq 0\}$*

Logo

$$B.A = 0 \Rightarrow b_{11}.a_{12} = 0 \text{ e } b_{21}.a_{12} = 0 \Rightarrow b_{11} = 0 \text{ e } b_{21} = 0 \tag{4.10}$$

Portanto

$$Ann(I) = \{A \in M_2\mathbb{K}/b_{11} = 0 \text{ e } b_{21} = 0\} \tag{4.11}$$

Observação 4.1. *A definição de anulador é usada em ideais primitivos, radical de Jacobson, entre outras coisas.*

5 Produto de Módulos

Seja R um anel e considere $\{M_i \mid i \in I\}$ uma família de de $R-$módulos á esquerda indexada pelo conjunto I.

Considere $M = \prod_{i \in I} M_i$ o produto cartesiano dos membros da família, i.e., o conjunto de todas as sequências $(a_i)_{i \in I}$ onde $a_i \in M)i$ para cada $i \in I$.

Podemos introcuzir em M uma estrutura de $R-$módulo definindo as seguintes operações:

$$\text{i)}\ \ (a_i)_{i \in I} + (b_i)_{i \in I} = (a_i + b_i)_{i \in I} \tag{5.12}$$

$$\text{ii)}\ \ r(a_i)_{i \in I} = (ra_i)_{i \in I} \tag{5.13}$$

O $R-$módulo definido anteriormente é chamado de produto direto da família $\{M_i\}_{i \in I}$.

6 Soma de Módulos

Seja R um anel e considere $\{M_i; i \in I\}$ uma família de $R-$módulos à esquerda indexada pelo conjunto I.

6.1 Soma Direta Externa

A soma direta externa $M_i (i \in I)$ é definida como sendo o conjunto de todas as sequências (a_i) onde $a_i = 0$ com exceção de um número finito de índices e é denotado por $\bigoplus_{i \in I} M_i$

$$(a_i) + (b_i) = (a_i + b_i) \tag{6.14}$$

$$r.(a_i) = (r.a_i) \tag{6.15}$$

Observação 6.1. *A soma direta externa é um submódulo do produto direto.*

É claro que quando o conjunto de índices é finito, as duas definições são coincidentes.

6.2 Soma Direta Interna

O $R-$módulo M é uma soma direta interna dos submódulos M_i se para cada $x \in M$ temos que $x = x_{i_1} + \ldots + x_{i_n}$ com $x_{i_j} \in M_{i_j}$ com $j = 1, \ldots, n$

Observação 6.2. *Soma direta interna quer dizer que cada elemento é escrito de maneira única por um número finito de elementos e já na externa isso não precisa ser verdade.*

7 Módulos Simples

Seja M um $R-$módulo. Diremos que M é simples quando M só tem os submódulos triviais.

Exemplo 7.1. *1) Um grupo abeliano G é um $\mathbb{Z}$-módulo simples se e somente se G*

2) Um espaço vetorial V é simples se e somente se $\dim V = 1$.
é cí)clico de ordem primo. ($G \simeq \mathbb{Z}_p$

Proposição 7.1. *Um $R-$módulo simples é necessariamente cíclico.*

Observação 7.1. *Um módulo simples também é chamado de módulo irredutível.*

Afirmação : Sejam $\mathbb{K}$ um corpo e $i \in \{1, \ldots, n\}$. O ideal (à esquerda) de matrizes colunas $L_i = \left\{ \begin{pmatrix} 0 & \ldots & 0 & a_{1i} & 0 & \ldots & 0 \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \ldots & 0 & a_{ni} & 0 & \ldots & 0 \end{pmatrix}, a_{ji} \in \mathbb{K} \text{ para todo } j = 1, \ldots, n \right\}$ é um $M_n(\mathbb{K})-$módulo simples com a operação usual

Lema 7.1 (Lema de Schur)**.** *Se M e N são $R-$módulos simples, então qualquer homomorfismo de M para N ou é um isomorfismo ou é nulo. Em particular, o anel de endomorfismos de um módulo simples é um anel de divisão.*

Dem.:
Seja $\varphi : M \to N$ tal que $\varphi \neq 0$. Logo

$$\ker \varphi \neq M \text{ e } 0 \subsetneq \operatorname{Im} \varphi \subseteq N$$

Pela hipótese, podemos concluir que $\ker \varphi - 0$ e $\operatorname{Im} \varphi = N$, i.e., φ é um isomorfismo.

Em particular, todo endomorfismo de M não nulo é claramente inversível; e portanto, uma unidade no anel de endomorfismos $\operatorname{End}_R(M)$.

Observação 7.2. *O lema de Schur é bastante utilizado na teoria de representações de grupos e álgebras, por exemplo.*

Como veremos no exemplo a seguir, a recíproca do Lema de Schur não é verdadeira em geral.

Exemplo 7.2. *Seja M um espaço vetorial sobre um corpo $\mathbb{K}$ de dimensão 2.*

Considere $R = \{T : M \to M / T(m_1) = am_1 \text{ e } T(m_2) = bm_1 + cm_2\}$, onde $\{m_1, m_2\}$ é uma base de M.

Dado $m = xm_1 + ym_2$ com $x, y \in R$, teremos que $T(m) = T(xm_1 + ym_2) = xT(m_1) + yT(m_2) = x(am_1) + y(bm_1 + cm_2) \Rightarrow T(m) = (xa + yb)m_1 + (yc)m_2$.

Afirmação 1:
R é um subanel de $\operatorname{End}_R(M)$.
Sejam $T, S \in R$ tais que $T(m_1) = a_1m_1, T(m_2) = b_1m_1 + c_1m_2, S(m_1) = a_2m_1 e S(m_2) = b_2m_1 + c_2m_2$. Logo

i) $(T + S)(m_1) = T(m_1) + S(m_1) = a_1m_1 + a_2m_2 = (a_1 + a_2)m_1$

ii) $(T+S)(m_2) = T(m_2) + S(m_2) = b_1m_1 + c_1m_2 + (b_2m_1 + c_2m_2) = (b_1m + 1 + b_2m_1) + (c_1m_2 + c_2m_2) = (b_1b_2)m_1 + (c_1 + c_2)m_2$

Portanto $T + S \in R$. Além disso,

iii) $(T \circ S)(m_1) = T(S(m_1)) = T(a_2m_1) = a_1(a_2m_1) = (a_1a_2)m_1$

iv) $(T \circ S)(m_2) = T(S(m_2)) = T(b_2m_1 + c_2m_2) = b_2T(m_1) + x_2T(m_2) = b_2(a_1m_1) + c_2((b_1m_1 + c_1m_2) = (b_2a_1)m_1 + (c_2b_1)m_1 + (c_2c_1)m_2 = (b_2a_1 + c_2b_1)m_1 + (c_2c_1)m_2$

Portanto $T \circ S \in R$

Afirmação 2: M é um $R-$módulo à direita com o seguinte produto:

$$m.T = T(m), \forall m \in M \text{ e } T \in \text{End}_K(M) \tag{7.16}$$

Como M é um $\mathbb{K}-$ espaço vetorial, é natural que M seja um grupo aditivo abeliano.

Além disso, por ser um subanel de $\text{End}_K(M)$ temos que as outras condições são também satisfeitas; i.e., M é um $R-$módulo á direita.

Afirmação 3: M não é um $R-$módulo simples.

Vamos supor que M é um $R-$módulo simples. Considere $N =< m_1 >\subseteq M \Rightarrow < m_1 >= M$. Por outro lado, $m_2 \in M \Rightarrow m_2 = m_1.T$ para algum $T \in R$. Logo, $m_2 = m_1.T \Rightarrow T(m_1) = m_2 \Rightarrow am_1 = m_2 \Rightarrow m_2, m_1$são l.d. como elementso do $fieldK-$espaço vetorial. Contudo isso contradiz o fato de que $\{m_1, m_2\}$ é uma base de M.

Afirmação 4: $\text{End}_R(M)$ é um anel de divisão. Sejam $f \in \text{End}_R(M)$ e $m \in M$. Logo $\exists c_d \in field(K)$ tal que $m = cm_1 + dm_2$. Definimos a transformação linear T (em R) dada por $T(m_1) = 0$ e $T(m_2) = cm_1 + dm_2$, isto é, $m = m_2.T$. Assim,$f(m) = f(m_2).T = T(f(m_2)) =^2 T(a_m1 + bm_2) = aT(m_1) + bT(m_2) = a(cm_1 + dm_2) = a.m$. Portanto, como $a \in \mathbb{K}$ dado acima depende somente de $f(m_2)$ podemos concluir que

$$f(m) = a_m, \forall m \in M \tag{7.17}$$

da forma (7.17) pertencem a $\text{End}_R(M)$. Além disso, o homomorfismo $g(m) = a^{-1}m$ é a inversa do homomorfismos $f(m) = a.m$ desde que $a \neq 0$. De fato,

i) $(g \circ f)(m) = g(f(m)) = g(am) = a^{-1}(am) = (a^{-1}.a)m = 1_R.m = m$

ii) $(f \circ g)(m) = f(g(m)) = f(a^{-1}m) = a(a^{-1}.m) = (a.a^{-1})m = 1_R.m = m$

8 Módulos Finitamente Gerados

Seja M um $R-$módulo. Diremos que M é finitamente gerado quando existirem $x_1, \ldots, x_t \in M$ tais que $M = R_{x_1} + R_{x_2} + \ldots + R_{x_t}$. Neste caso, diremos que $\{x_1, \ldots, x_t\}$ é o conjunto de geradores de M. Defimos que M é cíclico quando $M = Rx$ para algum $x \in M$.

Exemplos

Exemplo 8.1. *Se M é um espaço vetorial sobre o corpo $\mathbb{K}$, então $R_{x_1} + R_{x_2} + \ldots + R_{x_t}$ é o subspaço gerado pelos vetores $x_1, \ldots, x_t \in M$*

Exemplo 8.2. *O produto direto R^n é finitamente gerado pelos elementos $e_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$ onde 1 é na décima posção e para $i = 1, \ldots, n$.*

Proposição 8.1. *Um $R-$módulo é cíclico se e somente se ele é isomorfo ao R/L para algum ideal L de R.*

[2] $f(m_2) \in M \Rightarrow \exists\, a, b \in \mathbb{K}$ tal que $f(m_2) = am_1 + bm_2$

Demonstração. Suponha que $M = Rx$ para algum $x \in M$. Seja $\varphi : R \to M/\varphi(r) = rx$ Afirmação: φ é um homomorfismo de $R-$módulos.

- $\varphi(r+s) = (r+s)x = rx + sx = \varphi(r) + \varphi(s)$
- $\varphi(ar) = (ar)x = a(rx) = a\varphi(r)$

Observemos que φ é sobrejetora. Pelo 1º Teorema do Isomorfismo temos que $R/_{\ker\varphi} \simeq M$. □

Proposição 8.2. *Um $R-$módulo M é finitamente gerado se e somente se existe $\varphi : R^n \to M$ epimorfismo para algum inteiro positivo n.*

Demonstração. ($\Rightarrow$) Sejam $x_1, \ldots, x_n$ os geradores de M e defina $\varphi : R^n \to M$ tal que $\varphi((r_1, \ldots, r_n)) = r_1x_1 + \ldots + r_tx_n$.

Afirmação: φ é um homomorfismo de $R-$módulos.

$$\begin{aligned} & \varphi((r_1,\ldots,r_n)+(s_1,\ldots,s_n))\varphi((r_1+s_1,\ldots,r_n+s_n)) = \\ = \ & (r_1+s_1)x_1+\ldots+(r_n+s_n)x_n = (r_1x_1+s_1x_1)+\ldots+(r_nx_n+s_nx_n) = \\ = \ & (r_1x_1+\ldots+r_nx_n+(s_1x_1+\ldots+s_nx_n) = \varphi((r_1,\ldots,r_n)+\varphi((s_1,\ldots,s_n)) \end{aligned} \tag{8.18}$$

$$\begin{aligned} \varphi(a(r_1,\ldots,r_n) &= \varphi(ar_1,\ldots,ar_n) = (ar_1)x_1+\ldots+(ar_n)x_n = \\ &= a(r_1x_1)+\ldots+(a(r_nx_n) = a(r_1x_1+\ldots+r_nx_n) = a\varphi(r_1,\ldots,r_n) \end{aligned} \tag{8.19}$$

É claro que φ é sobrejetora. ($\Leftarrow$) Suponhamos que $\varphi : R^n \to M$ é um epimorfimso. Afirmação: M é gerado por $\varphi(e_1), \ldots, \varphi(e_n)$.

Seja $M \in M$. Logo $\exists\, r = r_1e_1 + \ldots + r_ne_n \in R^n$ tal que $\varphi(n) = m$.

Assim, $m = \varphi(r) = \varphi(r_1e_1 + \ldots + r_ne_n) = r_1\varphi(e_1) + \ldots + r_n\varphi(e_n)$.

Portanto M é finitamente gerado. □

9 Módulos Livres

Um conjunto de elementos $\{x_1, \ldots, x_n\}$ em um $R-$módulo M é independente sobre R se $r_1x_1 + \ldots + r_nx_n = 0 \Rightarrow r_1 = r_2 = \ldots = r_n = 0$.

Dizemos que $B = \{x_1, \ldots, x_n\}$ é uma base quando B é independente sobre R e $M = Rx_1 + \ldots + Rx_n$.

Um módulo é dito livre quando ele tem uma base. (Ou seja, um módulo livre se comporta quase como um espaço vetorial).

Observe que um módulo finitamente gerado não precisa ser um módulo livre. $\mathbb{Z}_6 = \mathbb{Z}\bar{3} + \mathbb{Z}\bar{2}$ é um $\mathbb{Z}-$módulo finitamente gerado, mas não é um módulo livre.

Exemplo 9.1. *Para $\mathbb{K}$ um corpo, todo espaço vetorial de dimensão finita sobre $\mathbb{K}$ é um $R-$módulo finitamente gerado livre.*

Exemplo 9.2. *R^n é um $R-$módulo finitamente gerado e livre.*

Proposição 9.1. *Todo $R-$módulo livre é isomorfo a R^n para algum inteiro positivo.*

Demonstração. Segue da proposição (8.2) □

Em particular, um grupo abeliano é um $\mathbb{Z}-$módulo livre se e somente se ele é soma direta de cópias de $\mathbb{Z}$.