Aula 6

Modulos

Em algebra linear a estrutura muito importante é espaço vetorial. Em algebra comutativa é útil considerar uma generalização dessa estrutura, quando

escalares = elementos de um anel comutativo.

Deste mode recebemos o modulo.

Acontece, que sobre certos aneis tem interpretação especial: (por exemplo)

a) [modulos sobre $\mathbb{Z}$] = [grupos abelianos],

b) [modulos sobre $K[x]$, k-corpo] = [Espaços vetoriais V, sobre k, com transf. linear $T: V \to V$].

Definições e fatos básicos

Def. [Modulo].

Seja R um anel comutativo. Um R-modulo M é um grupo abeliano com uma aplicação

$$\cdot : R \times M \longrightarrow M,$$ que satisfaz:

a) $(a+b)\cdot m = a\cdot m + b\cdot m$

b) $a\cdot(m+n) = a\cdot m + a\cdot n$

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

d) $1\cdot m = m$, para todos $a, b \in R$; $n, m \in M$.

Exemplos:

a) Um ideal $I \lhd R$ e um R-modulo.

b) Se $R = k$ - um corpo, assim um R-modulo é um espaço vetorial.

c) Obvialmente o conjunto $\{0\}$ é um modulo.

d) para $n > 0$, o conjunto

$$R^n = \{(a_1, \dots, a_n) \mid a_1, \dots, a_n \in R\}$$ é R-modulo,

com adição em componentes e multiplicação por escalares.

Mais geral, se N, M dois R-modulos, $\Rightarrow M \times N$ é tmb.

Definição [Submodulo, soma, quociente].

Seja M um R-modulo.

a) Um submodulo de M é conjunto $N \subset M$ que satisfaz:

$m+n \in N$ e $a \cdot m \in N$, para todos: $\begin{matrix} m,n \in N \\ a \in R. \end{matrix}$

b) Para todo subconjunto $S \subset M$, o conjunto

$$\langle S \rangle := \left\{ a_1 m_1 + \dots + a_n m_n \;\middle|\; \begin{matrix} n \in \mathbb{N}; \\ a_1, \dots, a_n \in R;\ m_1, \dots, m_n \in S \end{matrix} \right\}$$

é menor submodulo de M que contem S.

$\langle S \rangle$ é chamado submodulo gerado por S.

Modulo M é chamado finitamente gerado se $M = \langle S \rangle$, para um conjunto finito $S \subset M$.

c) Para os submodulos $N_1, \dots, N_n \subseteq M$, a soma

$$N_1 + \dots + N_n = \{ m_1 + \dots + m_n \mid m_i \in N_i,\ 1 \le i \le n \}$$

é obvialmente um submodulo de M.

Se todo $m \in N_1 + \dots + N_n$ apresenta-se na maneira unica como $m = m_1 + \dots + m_n$ com $m_i \in N_i$, dizemos que soma $N_1 + \dots + N_n$ é soma direta e escrevemos como $N_1 \oplus \dots \oplus N_n$.

d) Se $N \leq M$ um submodulo, o conjunto

$$M/N := \{\bar{x} \mid x \in M\}, \text{ com } \bar{x} := x + N$$

de clases de equivalência é um modulo [Ex. p/ casa], chamado <u>modulo quociente</u>.

<u>Exercicio</u> [p/ casa].

Seja N um submodulo de um R-modulo M.
Mostre:

a) Se N e M/N são finitamente gerados $\Rightarrow$ M tmb é finit. gerado.

b) Se M é f.g. $\Rightarrow$ M/N tmb f.g.

c) Se M é f.g., N não precisa ser f.g.

<u>Definição</u> [Morfismos]. Sejam M, N dois R-modulos.

a) Um <u>morfismo</u> [ou R-<u>modulo homomorfismo</u>] de M ao N é uma mapa $\varphi: M \to N$ tal que $\varphi(m+n) = \varphi(m) + \varphi(n)$, e

$$\varphi(am) = a\varphi(m)$$

para todos $m, n \in M$ e $a \in R$.

O conjunto de todos tais morfismos será denotado por $\mathrm{Hom}_R(M, N)$ (ou somente $\mathrm{Hom}(M, N)$).

Obs. $\mathrm{Hom}_R(M,N)$ é um R-módulo de novo.

b) Um morfismo $\varphi: M \to N$ é chamado isomorfismo, se φ é bijetivo.

Neste caso $\varphi^{-1}: N \to M$ é homomorfismo também [Ex p/ casa]. Dizemos que N, M são isomorfos ($N \simeq M$) se existir isomorfismo entre eles.

Exemplos

a) Para todo ideal $I \trianglelefteq R$ a mapa quociente

$$\varphi: R \to R/I \quad a \mapsto \bar{a}$$

é homomorfismo sobrejetor. (R-módulos)

b) Se M, N dois $\mathbb{Z}$-módulos, assim M, N grupos abelianos e todo homomorfismo $\varphi: M \to N$ de módulos é um homomorfismo dos grupos abelianos.

c) Para todo R-módulo M, temos $\mathrm{Hom}_R(R,M) \simeq M$.

Aplicações:

$$M \to \mathrm{Hom}_R(R,M) \quad m \mapsto (a \mapsto am)$$

e

$$\mathrm{Hom}_R(R,M) \to M \quad \varphi \mapsto \varphi(1)$$

São morfismos de módulos inversos um para outro.

Obs. Observe que $\mathrm{Hom}_R(M,R) \neq M$ em geral.

Por exemplo, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}) = 0$.

Obs. 2 [Núcleos e Imagens].

Seja $\varphi: M \to N$ um homomorfismo de R-módulos

a) para todo submódulo $M' \leq M$ a imagem $\varphi(M')$ é um submódulo em N.

$\Rightarrow$ $\varphi(M)$ é submódulo em N tmb chamado imagem de φ.

b) Mostre que $\varphi^{-1}(N')$ é um submódulo em M para todo submódulo $N' \leq N$.

Em particular, $\varphi^{-1}(0)$ é submódulo em M chamado núcleo de φ.

Proposição [Teoremas de Isomorfismo].

a) Para todo morfismo $\varphi: M \to N$, temos isomorf

$M/\ker\varphi \to \mathrm{Im}\,\varphi$, dado por $\overline{m} \mapsto \varphi(m)$

b) Dados R-módulos $N' \leq N \leq M$, temos

$$(M/N')/(N/N') \simeq M/N.$$

c) Dados 2 submodulos N, N' de M, temos:

$$(N+N')/N' \simeq N/(N \cap N')$$

Prova [Ex. p/ casa].

Todos conceitos até agora parecidos ao espaços vetoriais. Os conceitos novos que vamos ver, reflecter o fato de existência dos ideais não-triviais em R.

Def. [IM, modulo quocientes, aniquiladores].

Seja M um R-modulo.

(a) Para todo $I \trianglelefteq R$ defina:

$$IM := \langle \{ am \mid a \in I, m \in M \} \rangle$$
$$= \left\{ \sum a_i m_i + \dots + a_n m_n \mid a_i \in I, m_i \in M \right\}.$$

Observe que IM é um submodulo em M e M/IM é um R/I-modulo na maneira obvia.

(b) Se $N, N' \subseteq M$ dois submodulos, defina modulo quociente: Como:

$$N' : N := \{ a \in R \mid aN \subset N' \} \trianglelefteq R.$$

Se $N'=0$, temos o que chama-se aniquilador

$$\operatorname{ann}_R N := \{ a \in R \mid aN = 0 \} \trianglelefteq R.$$

Exemplos:

a) Se N, N' e M são submodulos em R, i.e. ideais em R, assim

$I \cdot M$ e $N' : N$ exatamente corresponde ao produto e quociente dos ideais.

b) Se $I \trianglelefteq R \Rightarrow \operatorname{ann}_R(R/I) = I$.

Def. Um modulo M é chamado fiel se $\operatorname{Ann}(M) = 0$

Obs. Se M g.g. R-modulo, assim M é fiel, como $R/\operatorname{Ann}_R(M)$.

Modulos finitamente gerados.

Def. Um R-modulo livre é modulo isomorfo a $\bigoplus_{i \in I} M_i$, onde cada $M_i \simeq R$, como modulo.

Um R-modulo livre f.g. é isomorfo a

$R^n = \underbrace{R \oplus \dots \oplus R}_{n\text{-vezes}}$, para algum $n > 0$.

Proposição Seja M um R-modulo, assim:

M é f.g $\Longleftrightarrow$ M isomorfo a um quociente de R^n, para algum $n > 0$.

Prova

[⇒] Sejam $m_1, \dots, m_n$ os geradores de M.

Defina $f: R^n \longrightarrow M$, por

$$(a_1, \dots, a_n) \longmapsto a_1 m_1 + \dots + a_n m_n$$

$\Rightarrow f$ é sobrejetor e logo $M \simeq \dfrac{R^n}{\ker f}$.

[⇐] Temos que $R^n/N \overset{\varphi}{\simeq} M$ para algum R-modulo N, logo existe um homomorfismo sobrejetor

$$f: R^n \longrightarrow M, \text{ onde } f = \pi \circ \varphi$$

com $\pi: R^n \longrightarrow R^n/N$ a projeção canônica.

Se $e_i = (0, \dots, 0, \underset{\uparrow}{1}, 0, \dots, 0)$

i-esima posição.

$\Rightarrow e_i$ geram R^n, ou seja $R^n = Re_1 + \dots + Re_n$

Como f é sobrejetor $\Rightarrow f(R^n) = M =$

$$= Rf(e_1) + \dots + Rf(e_n)$$

Logo $f(e_i)$ geram M. ▨