UMA INTRODUÇÃO A ÁLGEBRAS

TIAGO MACEDO

RESUMO. Neste seminário vamos introduzir uma nova estrutura algébrica, álgebras. Começaremos recapitulando estruturas definidas em seminários anteriores. Em seguida, definiremos álgebras, subálgebras, ideais e morfismos e mostraremos alguns exemplos. Por fim, vamos enunciar o Teorema do Isomorfismo para álgebras.

1. Estruturas algébricas

Vamos começar relembrando algumas estruturas algébricas.

1.1. Grupos. Um grupo é um conjunto G munido de uma função

$$\begin{array}{rcl} \mu : G \times G & \longrightarrow & G \\ (a,b) & \longmapsto & a \cdot b \end{array}$$

satisfazendo

(1) Associatividade: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para quaisquer $a, b, c \in G$
(2) Existência de elemento neutro: existe $e_G \in G$ tal que
$$e_G \cdot g = g = g \cdot e_G$$
para todo $g \in G$
(3) Existência de elementos inversos: para todo $g \in G$, existe $g^\vee \in G$ tal que
$$g \cdot g^\vee = e_G = g^\vee \cdot g.$$

Um grupo (G, μ) é dito abeliano quando a função μ é comutativa, ou seja, $\mu(a,b) = \mu(b,a)$ para quaisquer $a, b \in G$.

Data: 4 de maio de 2014.

1.2. **Anéis e Corpos.** Um anel (com unidade) é um conjunto R munido de duas funções

$$\begin{array}{rcl} \sigma : R \times R & \longrightarrow & R \\ (r,s) & \longmapsto & r+s \end{array} \qquad \begin{array}{rcl} \mu : R \times R & \longrightarrow & R \\ (r,s) & \longmapsto & r \cdot s \end{array}$$

satisfazendo as seguintes condições

(1) (R, σ) é um grupo abeliano
(2) $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ para quaisquer $r, s, t \in R$
(3) $r \cdot (s + t) = r \cdot s + r \cdot t$ para quaisquer $r, s, t \in R$
(4) $(s + t) \cdot r = s \cdot r + t \cdot r$ para quaisquer $r, s, t \in R$
(5) Existe $e \in R$ tal que $e \cdot r = r = r \cdot e$ para qualquer $r \in R$.

Um anel (R, σ, μ) é dito comutativo quando a função μ é comutativa, ou seja, $\mu(r,s) = \mu(s,r)$ para quaisquer $r, s \in R$. Um anel (R, σ, μ) é dito corpo quando $(R \setminus \{0\}, \mu)$ é um grupo (abeliano).

A partir de agora, vamos supor que todo anel é comutativo.

1.3. **Módulos e Espaços vetoriais.** Um módulo sobre um anel (R, σ_R, μ) é um conjunto M munido de duas funções

$$\begin{array}{rcl} \sigma_M : M \times M & \longrightarrow & M \\ (m,n) & \longmapsto & m+n \end{array} \qquad \begin{array}{rcl} \upsilon : R \times M & \longrightarrow & M \\ (r,m) & \longmapsto & r \cdot m \end{array}$$

satisfazendo as seguintes condições

(1) (M, σ_M) é um grupo abeliano
(2) $\sigma_R(r,s) \cdot m = \sigma_M(r \cdot m, s \cdot m)$ para quaisquer $r, s \in R, m \in M$
(3) $r \cdot (m + n) = r \cdot m + r \cdot n$ para quaisquer $r \in R, m, n \in M$
(4) $\upsilon((r \cdot s), m) = \upsilon(r, \upsilon(s, m))$ para quaisquer $r, s \in R, m \in M$
(5) $e \cdot m = m$ para todo $m \in M$.

Um R-módulo M é dito um espaço vetorial quando R é um corpo.

2. Definições e exemplos de álgebras

Definição 1. Seja (R, σ_R, μ_R) um anel. Uma R-álgebra é um conjunto A munido de três funções

$$\begin{array}{rcl} \sigma_A : A \times A & \longrightarrow & A \\ (a,b) & \longmapsto & a+b \end{array} \qquad \begin{array}{rcl} \mu_A : A \times A & \longrightarrow & A \\ (a,b) & \longmapsto & a \cdot b \end{array} \qquad \begin{array}{rcl} \upsilon_A : R \times A & \longrightarrow & A \\ (r,a) & \longmapsto & r.a \end{array}$$

satisfazendo as seguintes condições

(1) $(A, \sigma_A, \upsilon_A)$ é um R-módulo
(2) (A, σ_A, μ_A) é um anel
(3) $r.(a \cdot b) = (r.a) \cdot b = a \cdot (r.b)$ para quaisquer $r \in R, a, b \in A$.

Uma R-álgebra A é dita comutativa quando o anel (A, σ_A, μ_a) é comutativo. Uma R-álgebra A é dita de divisão quando o anel (A, σ_A, μ_a) é um corpo.

Exemplo 2. Considere $R = A = \mathbb{Z}$, $\sigma : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ a soma usual e $\mu = \upsilon : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ o produto usual de números inteiros. Nós já sabemos que $(\mathbb{Z}, \sigma)$ é um grupo abeliano, portanto $(\mathbb{Z}, \sigma, \upsilon)$ é um $\mathbb{Z}$-módulo. Nós sabemos ainda que $(\mathbb{Z}, \sigma, \mu)$ é um anel comutativo. Do Ensino Fundamental, nós sabemos também que $z_1(z_2z_3) = (z_1z_2)z_3 = z_2(z_1z_3)$ para quaisquer $z_1, z_2, z_3 \in \mathbb{Z}$. Poranto $\mathbb{Z}$ é uma $\mathbb{Z}$-álgebra comutativa.

Em geral, todo anel (comutativo) R é uma R-álgebra. Em particular, todo corpo (comutativo, incluindo $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$) é uma álgebra sobre si mesmo.

Exemplo 3. Considere $n > 0$ e $\mathbb{k}$ um corpo. Considere $\mathfrak{gl}_n(\mathbb{k})$ o conjunto de matrizes de ordem $n \times n$ e entradas em $\mathbb{k}$

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}, \qquad a_{ij} \in \mathbb{k}.$$

Nós já sabemos que $\mathfrak{gl}_n(\mathbb{k})$ munido da soma usual e multiplicação usual de matrizes é um anel (não comutativo). Nós também sabemos que munido da soma usual de matrizes e da multiplicação escalar dada por

$$\lambda . \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} \lambda a_{11} & \cdots & \lambda a_{1n} \\ \vdots & & \vdots \\ \lambda a_{n1} & \cdots & \lambda a_{nn} \end{pmatrix}, \quad \forall\ \lambda, a_{ij} \in \Bbbk$$

$\mathfrak{gl}_n(\Bbbk)$ é um $\Bbbk$-espaço vetorial.

Para verificar que $\mathfrak{gl}_n(\Bbbk)$ é uma $\Bbbk$-álgebra, basta mostrar que

$$\lambda.(A \cdot B) = (\lambda.A) \cdot B = A \cdot (\lambda.B),$$

para quaisquer $\lambda \in \Bbbk, A, B \in \mathfrak{gl}_n(\Bbbk)$. Multiplicando as matrizes, observamos que:

- A entrada (i,j) da matriz $\lambda.(A \cdot B)$ é $\lambda \left(\sum_{k=1}^n a_{ik} b_{kj} \right)$
- A entrada (i,j) da matriz $(\lambda.A) \cdot B$ é $\sum_{k=1}^n (\lambda a_{ik}) b_{kj}$
- A entrada (i,j) da matriz $A \cdot (\lambda.B)$ é $\sum_{k=1}^n a_{ik} (\lambda b_{kj})$.

Como vimos que $\Bbbk$ é uma $\Bbbk$-álgebra, segue que essas entradas são todas iguais. Com isso, concluímos que $\mathfrak{gl}_n(\Bbbk)$ é uma $\Bbbk$-álgebra não comutativa.

Exemplo 4. Anel de polinômios. Considere um anel R e o conjunto $R[x]$ formado por elementos da forma

$$p(x) = r_0 + r_1 x + \cdots + r_n x^n,$$

onde $n \geq 0$ e $r_0, r_1, \ldots, r_n \in R$. Definindo a soma como

$$\sigma_{R[x]}(a_0 + a_1 x + \cdots + a_n x^n, b_0 + b_1 x + \cdots + b_n x^n) = c_0 + c_1 x + \cdots + c_n x^n,$$

onde $c_i = a_i + b_i$, para todo $i = 0, 1, \ldots, n$, o produto como

$$\mu_{R[x]}(a_0 + a_1 x + \cdots + a_n x^n, b_0 + b_1 x + \cdots + b_n x^n) = c_0 + c_1 x + \cdots + c_{n+m} x^{n+m},$$

onde $c_i = \sum_{k=0}^i a_k b_{i-k}$, para todo $i = 0, 1, \ldots, n+m$, e a multiplicação escalar como

$$\upsilon_{R[x]}(r, a_0 + a_1 x + \cdots + a_n x^n) = c_0 + c_1 x + \cdots + c_n x^n,$$

onde $c_i = r a_i$, para todo $i = 0, 1, \ldots, n$, obtemos uma R-álgebra.

3. Morfismos de álgebras

Definição 5. Dados um anel R e duas R-álgebras A e B, um morfismo de R-álgebras é uma função $\varphi : A \to B$ tal que

(1) φ é um homomorfismo de anéis
(2) φ é um morfismo de R-módulos.

Um homomorfismo φ é dito isomorfismo, quando φ também for uma bijeção.

Exemplo 6. Dado um anel R e uma R-álgebra A, considere a função $id_A : A \to A$ dada por $id_A(a) = a$ para todo $a \in A$. Essa função, que é chamada de identidade, é um morfismo de R-álgebras. De fato, nós sabemos que id_A é um morfismo de anéis e de R-módulos.

Exemplo 7. Considere um anel R, três R-álgebras A, B, C e dois morfismos de R-álgebras $\varphi : A \to B$ e $\psi : B \to C$. A função $(\psi\circ\varphi) : A \to C$ é um morfismo de R-álgebras. De fato, como φ e ψ são morfismos de anéis, então $(\psi\circ\varphi)$ é um morfismo de anéis e, como φ e ψ são morfismos de R-módulos, então $(\psi \circ \varphi)$ é um morfismo de R-módulos.

4. Teorema do isomorfismo para álgebras

Definição 8. Dado um morfismo de R-álgebras $\varphi : A \to B$, definimos:

(a) O núcleo de φ como o conjunto $\ker\varphi = \{a \in A : \varphi(a) = 0_B\} \subseteq A$.
(b) A imagem de φ como o subconjunto

$$im(\varphi) = \{b \in B : b = \varphi(a) \text{ para algum } a \in A\} \subset B.$$

Dada uma R-álgebra $(A, \sigma, \mu, \upsilon)$, um subconjunto $B \subseteq A$ é dito uma R-subálgebra de A quando B for um subanel do anel (A, σ, μ) e um submódulo do R-módulo (A, σ, υ).

Dada uma R-álgebra $(A, \sigma, \mu, \upsilon)$, um subconjunto $I \subseteq A$ é dito um ideal de A quando I for um ideal do anel (A, σ, μ) e um submódulo do R-módulo (A, σ, υ).

Dados uma R-álgebra A e um ideal $I \subseteq A$, a álgebra quociente A/I é definida como o anel quociente A/I, munido da estrutura de R-módulo quociente A/I.

Teorema 9 (do Isomorfismo)**.** Se $\varphi : A \to B$ é um morfismo de R-álgebras, então

(1) $\ker \varphi \subseteq A$ é um ideal,
(2) $im(\varphi) \subseteq B$ é uma subálgebra,
(3) $R/\ker \varphi$ é isomorfo a $im(\varphi)$.