Well orderings are everywhere

Renan Maneli Mezabarba

5 de novembro de 2015

1 Introdução

Apresentaremos duas aplicações de métodos básicos de Teoria dos Conjuntos na Matemática: uma aplicação do axioma da escolha no estudo de módulos livres, e uma aplicação de recursão transfinita em teoria da medida.

2 Módulos livres

Informalmente, um **módulo M sobre um anel**[1] R (um **R-módulo**) é simplesmente um espaço vetorial sobre R. Formalmente, dizemos que espaços vetoriais são módulos sobre corpos e daí as terminologias se encaixam. Como ocorre com os corpos, um anel R é um R-módulo sobre si mesmo e, mais ainda, os **R-submódulos de R** são exatamente os seus **ideais**[2]. Um módulo é **livre** se ele possui um conjunto gerador linearmente independente, *a.k.a.* **base**.

Uma vantagem sobre módulos livres é que eles são completamente determinados pelas cardinalidades de suas bases. De fato, quaisquer duas bases de um R-módulo livre têm a mesma cardinalidade[3] − que daí é denotada por $\dim_R M$, a **dimensão de M** − e, se dois R-módulos livres têm a mesma dimensão, então são isomorfos.

Sabemos que (em ZFC) módulos sobre corpos são livres. Uma possível demonstração consiste em tomar uma boa ordem $\preceq$ para o seu k-módulo M (onde k é um corpo), e notar que $B_M = \{x \in M : x \notin \langle y \in M : y \prec x\rangle\}$ é

[1] Comutativo, com unidade.

[2] Subconjuntos fechados por combinações R-lineares.

[3] É possível provar diretamente, mas podemos usar um argumento rápido via produto tensorial: se $M = \bigoplus_{i\in I} R = \bigoplus_{j\in J} R$, então tensorisando por R/m (para qualquer ideal maximal m de R) temos $M/mM \cong \bigoplus_{i\in I} R/m \cong \bigoplus_{j\in J} R/m$, um isomorfismo entre R/m-módulos, i.e., um isomorfismo entre R/m-espaços vetoriais. Daí, $|I| = |J|$.

uma base. Podemos tentar repetir o mesmo argumento para um R-módulo N, na esperança de que B_N seja uma base para N. Contudo, embora B_N seja um gerador maximal para N, não há como garantir sua independência linear! De fato, tomando uma combinação R-linear $\sum_{i\leq n}\alpha_i x_i = 0$, com $\alpha_i \neq 0$ e $x_i \in B_N$ para todo $i \leq n$ (e supondo $x_0 \prec x_1 \prec \cdots \prec x_n$), não podemos necessariamente multiplicar a expressão por α_n^{-1} para obter $x_n \in \langle x_0, \ldots, x_{n-1}\rangle$, contrariando assim a hipótese $x_n \in B_N$.

Um exemplo, um pouco frustrante mas ainda válido, é considerar o $\mathbb{Z}$-módulo $M = \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$: $\{\overline{1}\}$ é um conjunto gerador de M, mas não é $\mathbb{Z}$-linearmente independente, pois $2 \neq 0$ e $2 \cdot \overline{1} = \overline{0}$.

Agora, se N é um R-submódulo livre de um R-módulo livre M de dimensão finita m, então $\dim_R N \leq m$. O problema? Não há garantias de que se N for R-submódulo de um R-módulo livre M, então N será livre! Por exemplo: para $R = \mathbb{R}[x, y]$, temos $\dim_R \mathbb{R}[x, y] = 1$, mas $(x, y) := \{fx + gy : f, g \in \mathbb{R}[x, y]\}$ não é livre[4]!

De fato, mais geralmente, se D for um **domínio**[5], então os únicos submódulos livres de D são os ideais principais, i.e., os ideais gerados por um único elemento: se um conjunto de geradores B de um submódulo I de D contém dois elementos não nulos, digamos a e b, então $a \cdot b + (-b) \cdot a = 0$ é uma combinação não trivial, mostrando que B é l.d.

Contudo, as coisas se comportam bem se R for um **domínio de ideais principais**: um domínio no qual todo ideal é principal.

Teorema 1. *Sejam R um D.I.P. e M um R-módulo livre. Se $N \subset M$ é um R-submódulo de M, então N é livre e* $\dim_R N \leq \dim_R M$.

Demonstração. Seja B uma base para M e fixemos uma boa ordenação para B, digamos $B = \{x_\alpha : \alpha < \kappa\}$. Defina então

$$M'_\alpha := \langle x_\beta : \beta < \alpha\rangle \text{ e } M_\alpha := M'_\alpha \oplus \langle x_\alpha\rangle.$$

Note que $M = \bigcup_{\alpha<\kappa} M_\alpha$. Agora, chamando por $N'_\alpha = N \cap M'_\alpha$ e $N_\alpha = N \cap M_\alpha$, temos $N'_\alpha = N \cap M'_\alpha = N \cap (M_\alpha \cap M'_\alpha) = N_\alpha \cap M'_\alpha$, logo

$$\frac{N_\alpha}{N'_\alpha} = \frac{N_\alpha}{N_\alpha \cap M'_\alpha} \cong \frac{N_\alpha + M'_\alpha}{M'_\alpha} \subset \frac{M_\alpha}{M_{\alpha'}} \cong R,$$

donde segue que $N_\alpha/N_{\alpha'}$ é isomorfo a um submódulo de R, o qual é principal por hipótese. Assim, $N_\alpha/N'_\alpha = 0$, ou N_α/N'_α é isomorfo a um ideal principal

[4]Não confundir com $\mathbb{R}[x, y]$ visto como $\mathbb{R}$-espaço vetorial, neste caso $\dim_{\mathbb{R}} \mathbb{R}[x, y] = \aleph_0$!

[5]Um anel em que $\alpha\beta = 0$ com $\alpha \neq 0$ implica $\beta = 0$. É o caso de $\mathbb{R}[x, y]$, por exemplo.

de R e, por conseguinte, $N_\alpha/N_{\alpha'}$ é isomorfo a R (como R-módulos!)[6]. Nesta situação, afirmamos que existe $n_\alpha \in N_\alpha \setminus \{0\}$ tal que $N_\alpha = N'_\alpha \oplus \langle n_\alpha \rangle$. Como a demonstração desse resultado usa somente uma generalização do Teorema do Núcleo e da Imagem, assumiremos a existência de tal n_α e prosseguiremos com a demonstração.

Afirmamos que $B' = \{n \in N : \exists \alpha < \kappa (n = n_\alpha)\}$ é uma base para N. Uma vez verificada tal afirmação, teremos o resultado provado, pois $|B'| \leq |B|$.

Para cada $m \in M$, seja $\mu(m) = \min\{\alpha < \kappa : m \in M_\alpha\}$. Em particular, note que se $n \in N'_\alpha$, então $\mu(n) < \alpha$. Se $N' = \langle B' \rangle \subsetneq N$, então existe $\gamma = \min\{\mu(n) : n \in N \setminus N'\}$, e podemos tomar $u \in N \setminus N'$ tal que $\mu(u) = \gamma$. Ora, $u \in N \cap M_\gamma = N_\gamma$ e $N_\gamma = N'_\gamma$ ou $N_\gamma = N'_\gamma \oplus \langle n_\gamma \rangle$: como o primeiro caso contraria a minimalidade de γ, necessariamente existem únicos $n' \in N'_\gamma$ e $r \in R \setminus \{0\}$ tais que $u = n' + r n_\gamma$. Note que $n' \notin N'$ e, por $n' \in N'_\gamma$ temos $\mu(n') < \gamma$, o que contraria a minimalidade de γ.

Resta provar a independência linear: ora, se $r_1 n_{\alpha_1} + \cdots + r_m n_{\alpha_m} = 0$, com $\alpha_1 < \cdots < \alpha_m$ e $r_i \neq 0$ para todo i, então $r_m n_{\alpha_m} \in \langle n_{\alpha_m} \rangle \cap N'_{\alpha_m}$, o que contraria o fato de que $N_{\alpha_m} \cap \langle n_{\alpha_m} \rangle = 0$. □

Observação 2. *Vale frisarmos algumas coisas:*

1. Na demonstração acima, se $\gamma = 0$, então $N'_0 = 0$ e assim resta somente $N_0 = \langle n_0 \rangle$.

2. Se M é um R-módulo livre, então qualquer sequência exata curta

$$0 \to N \hookrightarrow N' \twoheadrightarrow M \to 0$$

   cinde, o que significa, entre outras coisas, que $N' = N \oplus M$.

3. No final da demonstração, tínhamos $r_m \neq 0$, $n_{\alpha_m} \neq 0$ e concluímos $r_m \alpha_m \neq 0$, mas a princípio nada impede que $r \cdot m \neq 0$ se $r \in R \setminus \{0\}$ e $m \neq 0$. Implicitamente usamos o fato de que existe um isomorfismo de R-módulos $\varphi : N_{\alpha_m}/N'_{\alpha_m} \to (x)$, para algum $x \neq 0$ de R, daí como para quaisquer $v \in (x) \setminus \{0\}$ vale "$rv = 0 \Rightarrow r = 0$", o mesmo deve ser válido para $N_{\alpha_m}/N'_{\alpha_m}$.

[6]Se $x \in R \setminus \{0\}$, então $\varphi : (x) \to R$ que faz $rx \mapsto r$ é um isomorfismo de R-módulos (está bem definido e é injetor pois R é domínio, é sobrejetor por definição).

3 Construção de σ-álgebras

Uma das coisas que se faz em teoria da medida é generalizar o conceito de integral. Para isso, define-se uma **medida** μ numa coleção $\mathcal{A}$ "bem comportada" de subconjuntos do seu espaço X, daí a integral de funções características de elementos de $\mathcal{A}$ é definida em termos da medida de tais elementos, e a complexidade das definições vai aumentando junto com a complexidade das funções que se deseja integrar. Assim, duas coisas são essenciais: a medida, e a família bem comportada.

Consideremos $X = \mathbb{R}^n$ e digamos que a família bem comportada seja $\mathcal{A} = \wp(\mathbb{R}^n)$. Nesse contexto, espera-se que uma medida μ seja uma função sobre os subconjuntos de $\mathbb{R}^n$ que se comporte como gostaríamos que uma medida se comportasse, isto é, $\mu : \wp(\mathbb{R}^n) \to [0, \infty]$ é uma função com as seguintes propriedades:

(i) Se $E_1, E_2, \ldots$ é uma sequência (in)finita de conjuntos disjuntos, então

$$\mu(E_1 \cup E_2 \cup \ldots) = \mu(E_1) + \mu(E_2) + \ldots$$

(ii) Se $E = F$ a menos de rotação/translação/reflexão, então $\mu(E) = \mu(F)$;

(iii) $\mu(Q) = 1$, onde Q é o cubo unitário (aberto) em $\mathbb{R}^n$ (pontos $(x_1, \ldots, x_n)$ tais que $0 \leq x_j < 1$).

Tal função, contudo, não existe em ZFC. Façamos $n = 1$ e, sobre $[0, 1)$ defina a relação de equivalência $x \sim y$ sse $x - y \in \mathbb{Q}$. Tal relação particiona $[0, 1)$ em classes de equivalência, de modo que podemos tomar um elemento de cada classe e formar um conjunto N de representantes para $\sim$. Considerando $Q = \mathbb{Q} \cap [0, 1)$, tomamos para cada $r \in Q$ o conjunto

$$N_r = \{\alpha + r : \alpha \in N \cap [0, 1 - r)\} \cup \{\alpha + r - 1 : \alpha \in N \cap [1 - r, 1)\}.$$

Podemos assim reescrever $[0, 1)$ fazendo

$$[0, 1) = \dot{\bigcup}_{r \in Q} N_r.$$

De fato, a inclusão $\supseteq$ é imediata, ao passo que se $x \in [0, 1)$, existe um único $\alpha \in N$ tal que $x - \alpha \in \mathbb{Q}$, donde segue que $x \in N_{(x-\alpha)}$ caso $x > \alpha$, ou $x \in N_{(x-\alpha+1)}$ caso $x \leq \alpha$ (neste caso, $x - \alpha + 1 = r$ é um racional e $x = \alpha + r - 1$). Para verificar que os N_r's são disjuntos, podemos avaliar caso a caso, por exemplo: se $x \in N_r \cap N_s$ com $r \neq s$ de modo que $x = \alpha + r = \alpha' + s$, para $\alpha, \alpha' \in N$ distintos, teríamos $\alpha \sim \alpha'$, o que contradiz o modo como escolhemos os elementos de N.

Agora obtemos as contradições: para qualquer $r \in Q$ temos (por (i) e (ii)):

$$\mu(N) = \mu((N\cap[0,1-r)\dot\cup(N\cap[1-r,1)) = \mu(N\cap[0,1-r))+\mu(N\cap[1-r,1)) =$$

$$= \mu(N \cap [0,1-r) + r) + \mu(N \cap [1-r,1) + (r-1)) = \mu(N_r),$$

donde segue pela forma como reescrevemos $[0,1)$ que

$$\mu([0,1)) = \sum_{r\in Q} \mu(N_r) = \sum_{r\in Q} \mu(N),$$

cujo valor é 0 (se $\mu(N) = 0$) ou ∞ (caso contrário), o que contraria a hipótese $\mu([0,1)) = 1$.

Moral da história: se desejamos uma "medida" bem comportada num conjunto X, não podemos esperar medir tudo... Daí vem a ideia das σ-álgebras.

Uma **álgebra** num conjunto X é uma família $\mathcal{A}$ de subconjuntos de X fechada por complementar e por reuniões finitas (logo, por interseções − via De Morgan); $\mathcal{A}$ é uma **σ-álgebra** sobre X se, além de ser uma álgebra sobre X, for fechada por reuniões enumeráveis (logo, por interseções enumeráveis). Em particular, como $\wp(X)$ é uma σ-álgebra e a interseção de σ-álgebras é σ-álgebra, segue que para um dado $E \subset X$ existe a menor σ-álgebra que contém E, denotada por $\sigma(E)$.

Caso X seja um espaço topológico, podemos considerar sobre X a menor σ-álgebra que contenha todos os abertos de X, a chamada **σ-álgebra de Borel**, que denotaremos por $\mathscr{B}_X$. Em particular, caso $\mathcal{B}$ seja uma base enumerável para a topologia de X, vale $\sigma(\mathcal{B}) = \mathscr{B}_X$.

Proposição 3. *Seja $\mathcal{M}$ uma σ-álgebra infinita sobre X.*

(a) $\mathcal{M}$ contém uma sequência infinita de conjuntos disjuntos;

(b) $|\mathcal{M}| \geq |\wp(\mathbb{N})|$.

Demonstração. (a). Afirmamos que se $\mathcal{N}$ é uma σ-álgebra infinita sobre um conjunto Y, então existe $A \in \mathcal{N} \setminus \{\emptyset, Y\}$ tal que $\mathcal{N}_A := \{E \cap A : E \in \mathcal{N}\} \subset \mathcal{N}$ é infinito: de fato, dado $A \in \mathcal{N} \setminus \{\emptyset, Y\}$, $\mathcal{N}_A$ ou $\mathcal{N}_{Y\setminus A}$ devem ser infinitos, caso contrário, dado $B \in \mathcal{N}$ podemos fazer $B = (B \cap A) \cup (B \cap (Y \setminus A))$, o que acarretaria que $\mathcal{N}$ é finito.

Agora, se $E \in \mathcal{N}$, então $\mathcal{N}_E$ é uma σ-álgebra sobre E.

Assim, se $\mathcal{M}$ é uma σ-álgebra infinita sobre X, então existe $E_0 \in \mathcal{M} \setminus \{\emptyset, X\}$ tal que $\mathcal{M}_{E_0} \subset \mathcal{M}$ é uma σ-álgebra infinita sobre E_0; repetindo o argumento para E_0, vemos que existe $E_1 \in \mathcal{M}_{E_0} \setminus \{\emptyset, E_0\}$ tal que $(\mathcal{M}_{E_0})_{E_1} \subset$

$\mathcal{M}_{E_0} \subset \mathcal{M}$ é uma σ-álgebra infinita sobre E_1. Procedendo indutivamente, obtemos uma família $\{E_n\}_{n\in\mathbb{N}} \in \mathcal{N}^{\mathbb{N}}$ estritamente decrescente com respeito a inclusão. Daí basta definir $U_n = E_n \setminus E_{n+1} \in \mathcal{M}$ para cada $n \in \mathbb{N}$.

(b). Defina $\varphi : \wp(\mathbb{N}) \to \mathcal{M}$ por $\varphi(N) = \bigcup_{n\in N} U_n$, onde U_n é uma sequência com a propriedade (a), que garante a injetividade de φ. □

Assim, para $X = \mathbb{R}$ por exemplo, podemos considerar $\mathcal{B}$ uma base enumerável para a topologia de X, de modo que $\aleph_0 = |\mathcal{B}| \leq |\sigma(\mathcal{B})|$, e a proposição acima acarreta que $|\sigma(\mathcal{B})| \geq \mathfrak{c}$. Agora, construiremos $\sigma(\mathcal{B})$ explicitamente, a fim de limitar a cardinalidade de $\sigma(\mathcal{B})$ superiormente.

Proposição 4. *Sejam X um conjunto não vazio, $\mathcal{E} = \mathcal{E}_0 \subset \wp(X)$ e defina para cada $\alpha < \omega_1$:*

- *$\mathcal{E}_{\alpha+1}$ é a coleção das reuniões de enumeráveis elementos de $\mathcal{E}_\alpha$ bem como de complementares de elementos de $\mathcal{E}_\alpha$;*
- *se α é ordinal limite, $\mathcal{E}_\alpha = \bigcup_{\beta<\alpha} \mathcal{E}_\beta$.*

Então $\sigma(\mathcal{E}) = \bigcup_{\alpha<\omega_1} \mathcal{E}_\alpha$.

Demonstração. Como $\sigma(\mathcal{E})$ é a menor σ-álgebra que contém $\mathcal{E}$, temos $\mathcal{E}_0 \subset \sigma(\mathcal{E})$. Se $\alpha < \omega_1$ é tal que $\mathcal{E}_\beta \subset \sigma(\mathcal{E})$ para todo $\beta < \alpha$, então claramente $\mathcal{E}_\alpha \subset \sigma(\mathcal{E})$ caso α seja limite; se α for sucessor, temos $\mathcal{E}_\alpha = \mathcal{E}_{\beta+1}$, e cada elemento de $\mathcal{E}_\alpha$ é uma reunião de enumeráveis elementos de $\mathcal{E}_\beta \subset \sigma(\mathcal{E})$ ou o complementar de um elemento de $\mathcal{E}_\beta \subset \sigma(\mathcal{E})$, donde segue que $\mathcal{E}_\alpha \subset \sigma(\mathcal{E})$. Assim, por indução transfinita, segue que $\mathcal{E}_\alpha \subset \sigma(\mathcal{E})$ para todo $\alpha < \omega_1$ e a inclusão "$\subseteq$" segue-se. A outra inclusão se obtém ao provarmos que $\mathcal{N} = \bigcup_{\alpha<\omega_1} \mathcal{E}_\alpha$ é uma σ-álgebra (que contém $\mathcal{E}$). É claro que se $A \in \mathcal{N}$ então $X \setminus A \in \mathcal{N}$; agora, se $E_j \in \mathcal{E}_{\alpha_j}$ para cada $j \in \mathbb{N}$ ($\alpha_j < \omega_1$ para todo j), então temos $E = \bigcup_{j\in\mathbb{N}} E_j \in \mathcal{E}_{\sup_{j\in\mathbb{N}} \alpha_j} \subset \mathcal{N}$, pois $\alpha = \sup_{j\in\mathbb{N}} \alpha_j < \omega_1$ e $\mathcal{E}_{\alpha_j} \subset \mathcal{E}_\alpha$ para todo j. □

As duas últimas proposições acarretam que se $\aleph_0 \leq |\mathcal{E}| \leq \mathfrak{c}$, então por um lado vale $\mathfrak{c} \leq |\sigma(\mathcal{E})|$ e, por outro lado, $\sigma(\mathcal{E}) = \bigcup_{\alpha<\omega_1} \mathcal{E}_\alpha$, onde $|\mathcal{E}_\alpha| = |\mathcal{E}| \leq \mathfrak{c}$ para todo α, donde temos $|\sigma(\mathcal{E})| \leq \mathfrak{c}$. Desse modo, $|\mathscr{B}_\mathbb{R}| = \mathfrak{c}$.

É possível definir uma medida μ sobre $\mathscr{B}_\mathbb{R}$ de modo que a medida de intervalos da forma $[a, b)$ seja $b - a$. Tal medida, porém, não satisfaz uma condição de *completude*: uma medida ν sobre uma σ-álgebra $\mathcal{A}$ é completa se $\wp(A) \subset \mathcal{A}$ para todo $A \in \mathcal{A}$ tal que $\nu(A) = 0$. De fato, o conjunto de Cantor K é um fechado (logo, $K \in \mathscr{B}_\mathbb{R}$) com cardinalidade $\mathfrak{c}$ e de medida nula, donde segue que $|\wp(K)| = 2^\mathfrak{c}$ e, por conseguinte, $\wp(K) \not\subset \mathscr{B}_\mathbb{R}$. Em particular, o completamento $\mathscr{L}$ de $\mathscr{B}_\mathbb{R}$ com respeito a μ, a chamada σ-álgebra de Lebesgue, satisfaz $|\mathscr{L}| = 2^\mathfrak{c}$.

Referências

[1] Folland, G. **Real analysis: modern techniques and their applications**. 2.ed. John Wiley & Sons, New York, 1999.

[2] Rotman, J. J. **Advanced Modern Algebra**. Prentice Hall, 2003.