RMU
REVISTA MATEMÁTICA UNIVERSITÁRIA

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

Revista Matemática Universitária,
ISSN: 2675-5254 — **DOI:** 10.21711/26755254/rmu20227

O TEOREMA ESPECTRAL E SUAS MISTERIOSAS RELAÇÕES COM O TEOREMA DA DECOMPOSIÇÃO PRIMÁRIA

RONALDO FREIRE DE LIMA

Resumo. Neste artigo, apresentamos demonstrações alternativas do Teorema Espectral e do Teorema da Decomposição Primária, mostrando que o primeiro decorre diretamente do segundo.

1. Introdução

É notório que uma parte considerável da Álgebra Linear, enquanto teoria, dedica-se ao estudo dos operadores lineares, isto é, das transformações lineares $T : V \to V$, em que V é um espaço vetorial arbitrário. (Aqui, nos restringiremos aos de dimensão finita.) É também estabelecido que a abordagem mais natural aos operadores lineares dá-se por meio de decomposições desses em "suboperadores", o que corresponde a um processo de diagonalização em blocos das matrizes que os representam.

Mais especificamente, a cada operador linear T definido num espaço vetorial real V de dimensão $n \in \mathbb{N}$, como se sabe, está associada uma família de matrizes reais $n \times n$, em que cada uma delas representa T com respeito a alguma base de V. Uma decomposição de T, então, é um processo que visa determinar, nessa família, a matriz mais simples possível, sendo o caso ótimo aquele em que essa matriz é diagonal. Nessa ocorrência, diz-se que o operador T é *diagonalizável*.

A simplicidade das matrizes diagonais, inclusive do ponto de vista operacional, concede aos operadores diagonalizáveis um status de excelência, fato que torna o resultado seguinte um dos mais notáveis da Álgebra Linear.

Teorema Espectral. *Seja V um espaço vetorial real de dimensão finita munido de um produto interno. Então, todo operador linear autoadjunto $T\colon V \to V$ é diagonalizável. Consequentemente, existe uma base ortonormal de V formada por autovetores de T.*

Data de aceitação: 21 de fevereiro de 2022.
Palavras chave. teorema espectral – teorema da decomposição primária – polinômio mínimo.

Relembremos que, dado um espaço vetorial V munido de um produto interno $\langle\, ,\, \rangle$, um operador linear $T\colon V \to V$ é dito *autoadjunto* quando cumpre a condição:

$$\langle Tv, w\rangle = \langle v, Tw\rangle \ \ \forall v, w \in V.$$

Aplicando-se a igualdade acima aos vetores de uma base ortonormal $\mathcal{B}$, de V, conclui-se facilmente que um operador $T : V \to V$ é autoadjunto se, e somente se, a matriz de T com respeito à base $\mathcal{B}$ é simétrica. Dessa forma, os operadores autoadjuntos não só são facilmente identificáveis, mas também existem em abundância. Mais que isso, o conjunto $\mathcal{A}$ formado por todos os operadores autoadjuntos $T : V \to V$ (munido das operações usuais de adição e multiplicação por escalar) constitui um espaço vetorial real, o qual é isomorfo àquele formado pelas matrizes reais simétricas de ordem $n = \dim V$. Esses fatos, dentre outros, atestam a referida notabilidade do Teorema Espectral.

Neste artigo, temos como primeiro propósito o de mostrar que o Teorema Espectral decorre diretamente de um interessante resultado sobre decomposição de operadores, conhecido como Teorema da Decomposição Primária, o qual é raramente considerado em textos introdutórios de Álgebra Linear. Assim, o nosso segundo propósito é o de resgatar o Teorema da Decomposição Primária, apresentando, inclusive, uma demonstração alternativa do mesmo, mais simples que as usuais.

Um dos grandes atributos do Teorema da Decomposição Primária, o qual justifica plenamente o seu resgate, é a aplicabilidade. Com efeito, além do Teorema Espectral, muitos resultados fundamentais em Álgebra Linear podem ser obtidos do Teorema da Decomposição Primária. O mais imediato é a caracterização de operadores lineares diagonalizáveis como aqueles cujos polinômios mínimos são produtos de polinômios mônicos de grau 1. (A prova desse fato está contida no argumento que conclui a nossa demonstração do Teorema Espectral.)

Decorre também do Teorema da Decomposição Primária que as raízes do polinômio mínimo de um operador linear são precisamente seus autovalores, e que, para todo operador linear $T : V \to V$, existe um subespaço de V o qual é invariante por T e tem dimensão 1 ou 2. Por fim, outros importantes teoremas de decomposição podem ser estabelecidos a partir do Teorema da Decomposição Primária, tais como o Teorema da Decomposição Cíclica (cf. [2]) e o célebre Teorema (da forma canônica) de Jordan (cf. [1]).

2. Preliminares

No que se segue, denotaremos por V um espaço vetorial real arbitrário de dimensão $n \in \mathbb{N}$ e munido de um produto interno $\langle\, ,\, \rangle$. O conjunto dos polinômios de variável t e coeficientes no corpo dos reais $\mathbb{R}$ será denotado por $\mathscr{P}[t, \mathbb{R}]$.

Dados um operador linear $T : V \to V$ e um polinômio

$$p(t) := a_k t^k + a_{k-1} t^{k-1} + \cdots + a_1 t + a_0 \in \mathscr{P}[t, \mathbb{R}],$$

define-se o operador $p(T) : V \to V$ por

$$p(T) := a_k T^k + a_{k-1} T^{k-1} + \cdots + a_1 T + a_0 I,$$

em que I denota o operador identidade de V. Quando $p(T)$ é o operador nulo, o qual indicaremos por $\mathbf{0}$, diz-se que p *anula* T ou, equivalentemente, que p é um *anulador* de T.

Por exemplo, o polinômio $p(t) = t^2 + 1$ anula o operador $T : \mathbb{R}^2 \to \mathbb{R}^2$ cuja matriz com respeito à base canônica é:

$$[T] = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

De fato, identificando-se T com sua matriz $[T]$, temos que

$$p([T]) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^2 + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

donde $p(T) = \mathbf{0}$, isto é, p anula T.

Para todo operador linear $T : V \to V$, existe um polinômio $p \in \mathscr{P}[t, \mathbb{R}]$ que o anula. Para constatarmos isso, lembremos que o espaço vetorial formado pelos operadores lineares de V, o qual denotamos por $\mathscr{L}(V)$, tem dimensão n^2 (por ser isomorfo ao espaço das matrizes $n \times n$). Logo, o conjunto

$$\{I, T, T^2, \dots, T^{n^2}\},$$

por conter $n^2 + 1$ operadores, é necessariamente LD em $\mathscr{L}(V)$. Assim, existem escalares $a_0, \dots, a_{n^2} \in \mathbb{R}$, não todos nulos, para os quais a igualdade

$$a_0 I + a_1 T + \cdots + a_{n^2} T^{n^2} = \mathbf{0}$$

se cumpre, donde se conclui que o polinômio

$$p(t) = a_0 + a_1 t + \cdots + a_{n^2} t^{n^2}$$

anula o operador linear $T \in \mathscr{L}(V)$.

Definição 1. O *polinômio mínimo* de um operador linear $T \in \mathscr{L}(V)$ é o polinômio mônico de menor grau que anula T. (Lembre que um polinômio é dito *mônico* quando o coeficiente do seu termo de maior grau é 1.)

A existência de anuladores de um operador $T : V \to V$ assegura a existência do polinômio mínimo de T. Verifiquemos, através do algoritmo da divisão, a sua unicidade. Para tanto, suponhamos que $m_1, m_2 \in \mathscr{P}[t, \mathbb{R}]$ sejam polinômios mínimos de T. Pelo algoritmo da divisão, existem $q, r \in \mathscr{P}[t, \mathbb{R}]$, com $r = 0$ ou $\operatorname{grau}(r) < \operatorname{grau}(m_1)$, tais que $m_2 = m_1 q + r$, donde $r = m_2 - m_1 q$. Se r fosse não nulo, multiplicando-o por $c = 1/a_k$, em que a_k é o coeficiente de seu termo de maior grau, teríamos que cr seria um polinômio mônico, e também um anulador de T, já que m_1 e m_2 o são. Isso, porém, violaria a minimalidade de m_1. Assim, devemos ter $r = 0$. Daí, e do fato de m_1 e m_2 serem ambos mônicos e de mesmo grau, segue-se que $q = 1$ e, portanto, que $m_1 = m_2$.

De modo inteiramente análogo, isto é, através do algoritmo da divisão, estabelece-se a propriedade fundamental dos polinômios mínimos, a saber: *Para todo operador $T \in \mathscr{L}(\mathbb{R}^n)$, e todo anulador p de T, o polinômio mínimo m de T divide p.* Com efeito, pelo algoritmo da divisão, existem polinômios $q, r \in \mathscr{P}[t, \mathbb{R}]$, com $r = 0$ ou $\operatorname{grau}(r) < \operatorname{grau}(m)$, tais que $p = qm + r$. Argumentando como acima, concluiríamos que se r fosse não nulo, então cr seria um polinômio mônico e anulador de T, o que contradiria a minimalidade de m.

Dado $v \in V$, diz-se também que $p \in \mathscr{P}[t, \mathbb{R}]$ *anula* T *em* v, quando $p(T)v = 0$. O *polinômio mínimo de* T *em* v é então definido como o polinômio mônico de menor grau que anula T em v. Analogamente, verifica-se que o polinômio mínimo de T em v divide qualquer polinômio que anule T em v.

Denotaremos o núcleo de um operador linear $T : V \to V$ por $\ker T$, e o seu conjunto imagem por $T(V)$, isto é,

$$\ker T = \{v \in V \,;\, Tv = 0\} \quad \text{e} \quad T(V) = \{Tv \,;\, v \in V\}.$$

Verifica-se facilmente que $\ker T$ e $T(V)$ são ambos subespaços vetoriais de V, bem como que um operador linear $T : V \to V$ é injetivo se, e somente se, $\ker T = \{0\}$. Além disso, pelo Teorema do Núcleo e da Imagem,

$$\dim V = \dim \ker T + \dim T(V),$$

de modo que T é um isomorfismo (isto é, é invertível) se, e somente se, é injetivo.

Dado um operador linear $T : V \to V$, diz-se que um subespaço vetorial W de V é T-*invariante*, se $T(W) \subset W$. Note que, quando W é T-invariante, o operador linear $T|_W : W \to W$ fica bem definido.

O *autoespaço* de um operador T associado a um número real λ,

$$W_\lambda := \ker(T - \lambda I),$$

é um importante exemplo de subespaço T-invariante. Observe que todo vetor não nulo $v \in W_\lambda$ é um autovetor de T cujo autovalor associado é λ, isto é, $Tv = \lambda v$.

3. Demonstrações dos Teoremas

Inicialmente, relembremos que, pelo Teorema Fundamental da Álgebra, todo polinômio $p \in \mathscr{P}[t, \mathbb{R}]$ se decompõe de forma única como

$$p(t) = (p_1(t))^{s_1} \dots (p_k(t))^{s_k}, \;\; s_1, \dots, s_k \in \mathbb{N},$$

em que $p_1, \dots, p_k$ são polinômios irredutíveis (i.e., que não admitem divisores), de grau 1 ou 2, e distintos entre si. Nesse contexto, os polinômios $p_1, \dots, p_k$ são ditos os *fatores primos* de p.

O Teorema da Decomposição Primária estabelece que, para todo operador linear $T : V \to V$, existe uma decomposição de V em subespaços T-invariantes, os quais são determinados pelos fatores primos do polinômio mínimo de T. (Note que os fatores primos de um polinômio mínimo são todos mônicos, uma vez que m o é.) Mais precisamente:

Teorema da Decomposição Primária. *Considere um operador linear* $T : V \to V$, *bem como a decomposição de seu polinômio mínimo* m *por fatores primos:*

$$m(t) = (p_1(t))^{s_1} \dots (p_k(t))^{s_k}, \;\; s_1, \dots, s_k \in \mathbb{N}.$$

Nessas condições, V *admite a seguinte decomposição:*

$$V = W_1 \oplus \cdots \oplus W_k \,,$$

em que W_i denota o núcleo de $p_i(T)^{s_i}$. Além disso, para todo índice $i = 1, \dots, k$, são válidas as seguintes afirmações:

- *W_i é T-invariante;*
- *O polinômio mínimo de $T|_{W_i}$ é $p_i^{s_i}$.*

Vejamos, primeiramente, que o Teorema da Decomposição Primária implica diretamente o Teorema Espectral. Antes, convém observarmos que toda potência de um operador autoadjunto T é também um operador autoadjunto, como pode ser facilmente verificado. Consequentemente, vale o mesmo para $p(T)$, qualquer que seja o polinômio $p \in \mathscr{P}[t, \mathbb{R}]$. Lembramos ainda que autovetores de um operador autoadjunto associados a autovalores distintos são, necessariamente, ortogonais.

No lema seguinte, estabelecemos algumas propriedades adicionais dos operadores autoadjuntos.

Lema 1. *São verdadeiras as seguintes afirmações a respeito de um operador autoadjunto $T : V \to V$:*

i) *Dado $k \in \mathbb{N}$, se $T^k = \mathbf{0}$, então $T = \mathbf{0}$;*
ii) *Se $p(t) = t^2 + bt + c$ é irredutível, então $p(T)$ é invertível.*

Demonstração. (i) O resultado é óbvio para $k = 1$. Suponhamo-lo verdadeiro, então, para $k \in \mathbb{N}$. Assim, supondo-se $T^{k+1} = \mathbf{0}$, para todo $v \in V$, tem-se

$$\langle T^k v, T^k v\rangle = \langle T^{k+1} v, T^{k-1} v\rangle = 0,$$

donde se obtém $T^k v = 0$ e, pela hipótese de indução, que $T = \mathbf{0}$.

(ii) Suponhamos, por absurdo, que exista um vetor $u \in V$, tal que

$$p(T)u = 0, \quad \|u\| = 1.$$

Nesse caso, uma vez que $|\langle Tu, u\rangle| \leq \|Tu\|$ (pela desigualdade de Cauchy-Schwarz) e $\langle T^2 u, u\rangle = \|Tu\|^2$ (por T ser autoajunto), para $b \geq 0$, tem-se

$$0 = \langle p(T)u, u\rangle = \|Tu\|^2 + b\langle Tu, u\rangle + c \geq \|Tu\|^2 - b\|Tu\| + c = p(-\|Tu\|).$$

Analogamente, se $b < 0$, tem-se $p(\|Tu\|) \leq 0$. Porém, sendo p um polinômio mônico quadrático e irredutível, devemos ter $p(t) > 0 \,\forall t \in \mathbb{R}$. Dessa contradição, segue-se que $\ker p(T) = \{0\}$, donde se infere que $p(T)$ é um operador injetivo e, portanto, invertível. □

Demonstração do Teorema Espectral. Consideremos a decomposição do polinômio mínimo m de T por fatores primos:

$$m(t) = (p_1(t))^{s_1}(p_2(t))^{s_2}\dots(p_k(t))^{s_k}, \ s_i \in \mathbb{N}, \ i = 1, \dots k,$$

lembrando que cada p_i é um polinômio mônico irredutível de grau 1 ou 2. Designando-se por W_i o núcleo de $(p_i(T))^{s_i}$, segue-se do Teorema da Decomposição Primária que W_i é T-invariante e que vale a igualdade

$$W = W_1 \oplus \dots \oplus W_k.$$

Além disso, $m_i := (p_i)^{s_i}$ é o polinômio mínimo do operador (autoadjunto)

$$T_i = T|_{W_i} : W_i \to W_i.$$

Em particular, $p_i(T_i)$ é autoadjunto e

$$m_i(T_i) = (p_i(T_i))^{s_i} = \mathbf{0} \;\; \forall i = 1, \dots k.$$

Segue-se dessa última igualdade e do Lema 1-(i) que $p_i(T_i) = \mathbf{0}$, donde se infere que p_i é o polinômio mínimo de T_i, isto é, $s_i = 1$. Além disso, pelo Lema 1-(ii), p_i tem grau 1, uma vez que $p_i(T_i)$ não é invertível. Dessa forma, o polinômio mínimo de T se escreve como

$$m(t) = (t - \lambda_1) \dots (t - \lambda_k), \;\; \lambda_i \in \mathbb{R}, \;\; i = 1, \dots, k,$$

donde $W_i = \ker(T - \lambda_i I) = W_{\lambda_i}$ e, portanto,

$$V = W_{\lambda_1} \oplus \dots \oplus W_{\lambda_k}.$$

Conclui-se facilmente dessa última igualdade e da T-invariância dos autoespaços W_{λ_i} que o operador T é diagonalizável, bem como que $\lambda_1, \dots, \lambda_k$ são seus autovalores. Além disso, uma vez que autovetores de T em diferentes autoespaços são ortogonais, tomando-se uma base ortonormal em cada um dos autoespaços W_{λ_i}, obtém-se uma base ortonormal de V formada por autovetores de T. $\square$

Passemos à demonstração do Teorema da Decomposição Primária, na qual faremos uso do seguinte

Lema 2. *Para quaisquer operadores lineares $T_1, \dots, T_k \colon V \to V$, tem-se*

$$\dim\ker(T_1 T_2 \dots T_k) \le \dim\ker T_1 + \dim\ker T_2 + \dots + \dim\ker T_k.$$

Demonstração. Pelo Princípio da Indução, basta considerarmos o caso $k = 2$. Fazendo-se $K := \ker(T_1 T_2)$, é imediato que $T_2(K) \subset \ker T_1$. Daí, e do Teorema do Núcleo e da Imagem, tem-se

$$\dim K = \dim T_2(K) + \dim\ker T_2|_K \le \dim\ker T_1 + \dim\ker T_2,$$

como queríamos demonstrar. $\square$

Demonstração do Teorema da Decomposição Primária. Vejamos, inicialmente, que

$$W_i := \ker p^{s_i}(T) \ne \{0\} \;\; \forall i = 1, \dots, k.$$

Supondo, por absurdo, que $W_i = \{0\}$ para algum i, temos que $p_i(T)^{s_i} : V \to V$ é um isomorfismo. Claramente, os operadores $p_j(T)^{s_j}$ comutam, donde podemos supor, sem perda de generalidade, que $i = k$. Agora, existe $w \in V$, tal que $p_1(T)^{s_1} \dots p_{k-1}(T)^{s_{k-1}} w \ne 0$. Caso contrário, $p_1^{s_1} \dots p_{k-1}^{s_{k-1}}$ seria o polinômio mínimo de T. Porém, sendo $p_k(T)^{s_k}$ um isomorfismo, existe $v \in V$, tal que $p_k(T)^{s_k} v = w$. Logo,

$$m(T)v = p_1(T)^{s_1} \dots p_{k-1}(T)^{s_{k-1}} p_k(T)^{s_k} v = p_1(T)^{s_1} \dots p_{k-1}(T)^{s_{k-1}} w \ne 0,$$

o que, obviamente, é uma contradição. Assim, $W_i \ne \{0\} \, \forall i = 1, \dots, k$.

Suponhamos, agora, que exista um vetor não nulo $w \in W_i \cap W_j$, $i \ne j$. Nesse caso, $p_i^{s_i}$ e $p_j^{s_j}$ anulam T em w e, portanto, o polinômio mínimo de T em w divide ambos, o que é absurdo, visto que $p_i^{s_i}$ e $p_j^{s_j}$ são primos entre si. Logo,

$$W_i \cap W_j = \{0\} \; \forall i \ne j \in \{1, \dots, k\}.$$

Além disso, temos

$$V = \ker m(T) = \ker(p_1(T)^{s_1} \dots p_k(T)^{s_k}),$$

o que, juntamente com o Lema 2, nos dá

$$\dim V = \dim \ker m(T) \leq \dim W_1 + \cdots + \dim W_k = \dim (W_1 \oplus \cdots \oplus W_k),$$

donde $V = W_1 \oplus \cdots \oplus W_k$.

Segue-se facilmente da comutatividade de T com $p_i(T)^{s_i}$ que cada subespaço W_i é T-invariante. De fato, dado $v \in W_i$, tem-se

$$p_i(T)^{s_i} T v = T p_i(T)^{s_i} v = 0,$$

o que implica $Tv \in W_i$.

Provemos, finalmente, que o polinômio mínimo de $T|_{W_i}$, o qual denotaremos por m_i, é $p_i^{s_i}$. Supondo-se, sem perda de generalidade, que $i = 1$, definamos o polinômio

$$p = m_1 p_2^{s_2} \dots p_k^{s_k}$$

e vejamos que o mesmo anula T. De fato, tomando-se $v = w_1 + \cdots + w_k \in V$, $w_i \in W_i$, e lembrando-se que $p_j^{s_j}(T) w_j = 0$, tem-se

$$\begin{aligned} p(T)v &= m_1(T) p_2^{s_2}(T) \dots p_k^{s_k}(T)(w_1 + \cdots + w_k) \\ &= m_1(T) p_2^{s_2}(T) \dots p_k^{s_k}(T)(w_1 + \cdots + w_{k-1}) + \\ &\quad\; m_1(T) p_2^{s_2}(T) \dots p_k^{s_k}(T) w_k \\ &= m_1(T) p_2^{s_2}(T) \dots p_k^{s_k}(T)(w_1 + \cdots + w_{k-1}). \end{aligned}$$

Repentindo-se esse procedimento $k-1$ vezes, chega-se facilmente a:

$$\begin{aligned} p(T)v &= m_1(T) p_2^{s_2}(T) \dots p_k^{s_k}(T) w_1 = p_2^{s_2}(T) \dots p_k^{s_k}(T) m_1(T) w_1 \\ &= p_2^{s_2}(T) \dots p_k^{s_k}(T) m_1(T|_{W_1}) w_1 = 0. \end{aligned}$$

Desta forma, p anula T e, portanto, m divide p. Em particular, $p_1^{s_1}$ divide m_1. Porém, uma vez que W_1 é o núcleo de $p_1^{s_1}(T)$, temos que

$$p_1^{s_1}(T|_{W_1}) = p_1^{s_1}(T)|_{W_1} = \mathbf{0},$$

isto é, $p_1^{s_1}$ anula $T|_{W_1}$. Logo, pela minimalidade de m_1, devemos ter $p_1^{s_1} = m_1$. □

Referências

[1] K. Hoffman, R. Kunze: Linear Algebra, Prentice-Hall (1971).

[2] H. G. Jacob: Another proof of the rational decomposition theorem. Amer. Math. Monthly. 1131–1134 (1973).

UFRN-CCET-Departamento de Matemática
Lagoa Nova, Natal, RN
59072-970
Email address: ronaldo.freire@ufrn.br, zabumbe@gmail.com