# Álgebra Linear Avançada

## Decomposição Cíclica

Daniel Miranda Machado

29 de novembro de 2020

UFABC

Embora, em geral, o polinômio característico de transformação linear $T\colon V \to V$ possa ser decomposto como um produto de potências de polinômios irredutíveis sobre $\mathbb{K}[x]$, digamos $c_T = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, os polinômios irredutíveis $p_j$ não precisam ser lineares.

Em outras palavras, os autovalores de $T$ não precisam pertencer ao corpo $\mathbb{K}$. Portanto, é natural procurar uma forma canônica para $T$ nesse caso geral.

Neste vídeo apresentamos a Decomposição Cíclica e no próximo a Forma Canônica Racional.

# Forma Racional

Seja $T : V \to V$ um operador linear em um espaço vetorial de dimensão finita. Mostraremos que existe uma base $\underline{B}$ de $V$, na qual $[T]_{\underline{B}}$ é uma matriz na forma canônica racional:

$$\begin{bmatrix} C_{p_1}(\lambda_1) & 0 & \dots & 0 \\ 0 & C_{p_2}(\lambda_2) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & C_{p_r} \end{bmatrix} \quad \text{com} \quad C_{p_1} = \begin{bmatrix} 0 & 0 & 0 & 0 & -a_{i0} \\ 1 & 0 & 0 & 0 & -a_{i1} \\ 0 & 1 & 0 & 0 & -a_{i2} \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & 1 & -a_{i\,k-1} \end{bmatrix}$$

onde $C_{p_i}$ é uma matriz companheira para algum polinômio $p_i(x) = a_{ik}x^k + \cdots + a_{i1}x + a_{i0} \in \mathbb{K}[x]$.

Vamos agora focar em um tipo particular de subespaço invariante. Suponha que $V$ seja um espaço vetorial de dimensão finita e que $T\colon V \to V$ seja um operador linear. É fácil ver que a interseção de qualquer família de subespaços de $V$ invariantes por $T$ também é um subespaço de $V$ invariante por $T$.

Disso segue imediatamente que para cada subconjunto $A$ de $V$ existe um menor subespaço invariante por $T$ que contém $A$, ou seja, a interseção de todos os subespaços invariante por $T$ que contêm $A$. Denotaremos esse subespaço por $Z_A^T$. No caso em que $A = \{\mathbf{v}\}$, escreveremos $Z_{\mathbf{v}}^T$ ou simplesmente $Z_{\mathbf{v}}$ quando $T$ for claramente subentendido.

**Definição**

*Seja $T: V \to V$ um operador linear então o* ***subespaço $T$-cíclico*** *de $V$ gerado por* $\mathbf{v}$, *e denotado por $Z_{\mathbf{v}}$, é o menor subespaço invariante por $T$ que contém* $\mathbf{v}$.

## Exemplo

Seja a transformação linear $T\colon \mathbb{K}^3 \to \mathbb{K}^3$ definida por

$$T(x,\ y,\ z) = (y + 2z,\ -2z,\ x)$$

Considere o vetor $(1, 0, 0)$. Temos $T(1, 0, 0) = (0, 0, 1)$ e $T^2(1, 0, 0) = T(0, 0, 1) = (2, 0, 1)$, e assim

$$Z_{(1,0,0)} = \{(x,\ 0,\ z); x,\ z \in \mathbb{K}\}.$$

O subespaço $Z_{\mathbf{v}}$ pode ser caracterizado do seguinte modo.

**Teorema**

*Sejam $V$ um espaço vetorial de dimensão finita sobre um corpo $\mathbb{K}$ e $T\colon V \to V$ um operador linear. Então, para cada $\mathbf{v} \in V$,*

$$Z_{\mathbf{v}} = \{p(T)(\mathbf{v}); p \in \mathbb{K}[x]\}.$$

# Demonstração

É fácil ver que o conjunto $W = \{p(T)(\mathbf{v}) \;\; p \in \mathbb{K}[x]\}$ é um subespaço de $V$ que contém $\mathbf{v}$. Como $T$ comuta com $p(T)$, esse subespaço é $T$-invariante.

Suponha agora que $U$ seja um subespaço invariante por $T$ que contenha $\mathbf{v}$. Então, claramente, $U$ contém $T^k(\mathbf{v})$ para todos os inteiros não negativos $k$ e, consequentemente, $p(T)(\mathbf{v})$ para cada polinômio $p \in \mathbb{K}[x]$. Assim, $U$ contém $W$. Portanto, $W$ é o menor subespaço invariante por $T$ que contém $\mathbf{v}$ e, portanto, coincide com $Z_{\mathbf{v}}$.

Nosso objetivo imediato é descobrir uma base para o subespaço $Z_{\mathbf{v}}$. Para esse propósito, considere a sequência

$$\mathbf{v},\ T(\mathbf{v}),\ T^2(\mathbf{v}),\ \ldots,\ T^r(\mathbf{v}),\ \ldots$$

de elementos em $Z_{\mathbf{v}}$. Claramente, existe um menor número inteiro positivo $k$, de modo que $T^k(\mathbf{v})$ é uma combinação linear dos elementos que o precedem nesta lista, digamos

$$T^k(\mathbf{v}) = \lambda_0\mathbf{v} + \lambda_1 T(\mathbf{v}) + \cdots + \lambda_{k-1}T^{k-1}(\mathbf{v})$$

e $\{\mathbf{v}, T(\mathbf{v}), \ \ldots, T^{k-1}(\mathbf{v})\}$ é então um subconjunto linearmente independente de $Z_{\mathbf{v}}$.

Escrevendo $a_j = -\lambda_j$ para $i = 0, \ldots, k-1$ deduzimos que o polinômio

$$m_{\mathbf{v}} = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} + x^k$$

é o polinômio mônico de menor grau tal que $m_{\mathbf{v}}(T)(\mathbf{v}) = \mathbf{0}$.

**Definição**

*Seja* $\mathbf{v} \in V$. *Então o conjunto*

$$\{p(X) \in \mathbb{K}[X] : p(T)(v) = 0\}$$

*é um ideal de* $\mathbb{K}[X]$ *e seu gerador mônico* $m_{\mathbf{v}}$ *é dito* $T$-***aniquilador*** *de* $\mathbf{v}$.

O $T$-**aniquilador** de $\mathbf{v}$ também será denotado por $\mathrm{Ann}(v; T)$

### Exemplo

Seja $T$ a transformação apresentada no Exemplo 1. Nesse exemplo tínhamos que se $\mathbf{u} = (0, 0, 1)$ então $T^2\mathbf{u} = 2\,\mathrm{I}\,\mathbf{u} + T\mathbf{u}$ e logo o $T$-aniquilador de $\mathbf{u}$ é o polinômio $m_{\mathbf{v}} = x^2 - x - 2 = (x-2)(x+1)$.

## Teorema

*Sejam $V$ um espaço vetorial de dimensão finita e $T : V \to V$ uma transformação linear. Se $\mathbf{v} \in V$ tem $T$-aniquilador*

$$m_{\mathbf{v}} = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} + x^k$$

*Então o conjunto*

$$\underline{B}_{\mathbf{v}} = \{\mathbf{v},\ T(\mathbf{v}),\ \ldots,\ T^{k-1}(\mathbf{v})\}$$

*é uma base de $Z_{\mathbf{v}}$ e, portanto, $\dim Z_{\mathbf{v}} = \deg m_{\mathbf{v}}$.*

## Teorema (cont)

*Além disso, se $T\restriction_{Z_{\mathbf{v}}}: Z_{\mathbf{v}} \to Z_{\mathbf{v}}$, é a transformação linear induzida no $T$-subespaço invariante $Z_{\mathbf{v}}$ , então a matriz de $T\restriction_{Z_{\mathbf{v}}}$ em relação à base ordenada $\underline{B}_{\mathbf{v}}$ é*

$$C_{m_{\mathbf{v}}} = \begin{bmatrix} 0 & 0 & 0 & 0 & -a_0 \\ 1 & 0 & 0 & 0 & -a_1 \\ 0 & 1 & 0 & 0 & -a_2 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & 1 & -a_{k-l} \end{bmatrix}$$

*Finalmente, o polinômio mínimal de $T\restriction_{Z_{\mathbf{v}}}$ é $m_{\mathbf{v}}$.*

# Demonstração

Claramente, $\underline{B}_{\mathbf{v}}$ é linearmente independente e $T^k(\mathbf{v}) \in \langle \underline{B}_{\mathbf{v}} \rangle$. Provaremos por indução que, de fato, $T^n(\mathbf{v}) \in \langle B \rangle$ para todo $n$.

A afirmação é verdadeira para $n = 1, \ldots, k$ suponha que $n > k$ e $T^{n-i}(\mathbf{v}) \in \langle \underline{B}_{\mathbf{v}} \rangle$. Então $T^{n-i}(\mathbf{v})$ é uma combinação linear de $\mathbf{v}, T(\mathbf{v}), \ldots$, $T^{k-i}(\mathbf{v})$ e assim $T^n(\mathbf{v})$ é combinação linear de $T(\mathbf{v}), T^2(\mathbf{v}), \ldots, T^k(\mathbf{v})$, e logo $T^n(\mathbf{v}) \in \langle B \rangle$.

É imediato a partir dessa observação que $p(T)(\mathbf{v}) \in \langle \underline{B}_{\mathbf{v}} \rangle$ para cada polinômio $p$. Portanto, $Z_{\mathbf{v}} \subseteq \langle \underline{B}_{\mathbf{v}} \rangle$ de onde temos igualdade, pois a demonstração da inclusão inversa é direta.

Consequentemente, $\underline{B}_{\mathbf{v}}$ é uma base de $Z_{\mathbf{v}}$.

Agora como

$$
\begin{aligned}
T\restriction_{Z_{\mathbf{v}}}(\mathbf{v}) &= T(\mathbf{v}) \\
T\restriction_{Z_{\mathbf{v}}}[T(\mathbf{v})] &= T^2(\mathbf{v}) \\
&\vdots \\
T\restriction_{Z_{\mathbf{v}}}[T^{k-2}(\mathbf{v})] &= T^{k-1}(\mathbf{v}) \\
T\restriction_{Z_{\mathbf{v}}}[T^{k-1}(\mathbf{v})] &= T^{k}(\mathbf{v}) = -a_0\mathbf{v} - a_1T(\mathbf{v}) - \cdots - a_{k-1}T^{k-1}(\mathbf{v})
\end{aligned}
$$

é claro que a matriz de $T\restriction_{Z_{\mathbf{v}}}$ em relação à base $\underline{B}_{\mathbf{v}}$ é a matriz acima $C_{m_\lambda}$ acima.

Por fim, suponha que o polinômio mínimal de $T\restriction_{Z_{\mathbf{v}}}$ seja

$$m_{T\restriction_{Z_{\mathbf{v}}}} = b_0 + b_1 x + \cdots + b_{r-1}x^{r-1} + x^r$$

Então

$$0 = m_{T\restriction_{Z_{\mathbf{v}}}}(T)(\mathbf{v}) = b_0\mathbf{v} + b_1 T(\mathbf{v}) + \cdots + b_{r-1}T^{r-1}(\mathbf{v}) + T^r(\mathbf{v})$$

Logo $T^r(\mathbf{v})$ é combinação linear de $\mathbf{v}, T(\mathbf{v}), \ldots, T^{r-1}(\mathbf{v})$ e, portanto, $k \leq R$. Mas $m_{T\restriction_{Z_\mathbf{v}}}$ é a transformação nula em $Z_\mathbf{v}$, bem como o é $m_\mathbf{v}(T\restriction_{Z_\mathbf{v}})$. Consequentemente, temos $m_{T\restriction_{Z_\mathbf{v}}}|m_\mathbf{v}$ e, portanto, $r \leq k$. Assim, $r = k$ e $m_{T\restriction_{Z_\mathbf{v}}} = m_\mathbf{v}$.

# Exemplo

Seja $T$ a transformação apresentada no Exemplo 1. No Exemplo 1 mostramos que o $T$-aniquilador de $\mathbf{v}$ é o polinômio $m_{\mathbf{v}} = (x-2)(x+1)$. Nesse caso o polinômio mínimal de $T$ é $m_T = -(x-2)(x+1)(x+2)$ e logo $m_{\mathbf{v}}$ divide $m_T$

# Exemplo

Seja $T$ o operador que na base canônica $\underline{\mathrm{B}}$ é representado pela matriz

$$[T]_{\underline{\mathrm{B}}} = \begin{bmatrix} -2 & 3 & 6 \\ -2 & 2 & 5 \\ -1 & 1 & 3 \end{bmatrix}$$

Vamos calcular o aniquilador de $\mathbf{v}_1 = [1, 1, 0]$. Observamos que $\mathbf{v}_2 = T\mathbf{v}_1 = [1, 0, 0]$ $\mathbf{v}_3 = T^2\mathbf{v}_1 = T\mathbf{v}_2 = [-2, -2, -1]$ $\mathbf{v}_4 = T^3\mathbf{v} = [-8, -5, -3]$. Os vetores $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ são linearmente independentes e formam uma base de $Z_{\mathbf{v}} = V$.

Temos para $\mathbf{v}_4$ a seguinte relação linear $1\mathbf{v}_1 + 3T\mathbf{v}_1 - 3T^2\mathbf{v}_1 + T^3\mathbf{v}_1 = 0$. Logo $m_{\mathbf{v}} = -1 + 3x - 3x^2 + x^3$.

Nessa base temos

$$\begin{bmatrix} -2 & 3 & 6 \\ -2 & 2 & 5 \\ -1 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & -2 \\ 1 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & -3 \\ 0 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 1 & -2 \\ 1 & 0 & -2 \\ 0 & 0 & -1 \end{bmatrix}$$

## Definição

*Se $V$ é um espaço vetorial de dimensão finita e $T\colon V \to V$ é linear, então um subespaço $W$ de $V$ é dito $T$-cíclico se é $T$-invariante e possui uma base no formato $\{\mathbf{v}, T(\mathbf{v}), \ldots, T^m(\mathbf{v})\}$. Essa base é denominada **base cíclica** e $\mathbf{v}$ é denominado **vetor $T$-cíclico** para $W$.*

- O Teorema 4 mostra que $\mathbf{v} \in V$ é um vetor cíclico para o subespaço $Z_{\mathbf{v}}$ com base cíclica $\underline{\mathrm{B}}_{\mathbf{v}}$.
- O subespaço $Z_{\mathbf{v}}$ é denominado **subespaço cíclico de $T$** gerado por $\{\mathbf{v}\}$.

A

- matriz $C_{m_{\mathbf{v}}}$ do Teorema 4 é denominada **matriz companheira** do $T$-aniquilador $m_{\mathbf{v}}$.

# Exemplo

Um operador nilpotente $N$ com índice de nilpotência $n = \dim V$ sempre possui um vetor cíclico.

# Teorema da Decomposição Cíclica

Sejam $V$ um espaço vetorial de dimensão finita sobre um corpo $\mathbb{K}$ e $T : V \to V$ um operador linear. Então existem vetores $T$-cíclicos $\mathbf{v}_1, \ldots, \mathbf{v}_k$ tais que

$$V = \bigoplus_{j=1}^{k} Z_{\mathbf{v}_j},$$

Em particular, existe uma base de $V$ na qual a matriz de $T$ é da forma

$$\bigoplus_{i=1}^{k} C_i = \begin{bmatrix} C_{p_1} & & & \\ & C_{p_2} & & \\ & & \ddots & \\ & & & C_{p_k} \end{bmatrix}$$

e que $p_T = p_1 \cdots p_k$.

# Demonstração

A prova será feita por indução sobre $n = \dim V$. O teorema claramente vale se $n = 1$, portanto, assuma que o teorema vale para todos os operadores lineares em espaços vetoriais de dimensão menor que $n$.

Nosso objetivo é mostrar que $V = Z_{\mathbf{v}_1}$ para algum $\mathbf{v}_1 \in V$ ou que $V = Z_{\mathbf{v}_1} \oplus M$ para algum subespaço $T$-invariante $M$.

Seja $m \leq n$ a maior dimensão de um subespaço cíclico, ou seja, $\dim Z_{\mathbf{v}} \leq m$ para todos os $\mathbf{v} \in V$, e seja $\mathbf{v}_1 \in V$, de modo que $\dim Z_{\mathbf{v}_1} = m$.

Se $m = n$, então $Z_{\mathbf{v}_1} = V$ temos o que queríamos demonstrar. Caso contrário, devemos mostrar que existe um complemento $T$-invariante para

$$Z_{\mathbf{v}_1} = \langle\{\mathbf{v}_1,\ T(\mathbf{v}_1),\ \ldots,\ T^{m-1}(\mathbf{v}_1)\rangle\}$$

em $V$.

Para construir esse complemento, consideramos a aplicação linear $\tau : V \to \mathbb{K}^m$ definida como

$$\tau(\mathbf{v}) = [f(\mathbf{v}), f(T(\mathbf{v})), \ldots, f(T^{m-1}(\mathbf{v}))]^t$$

onde $f\colon V \to \mathbb{K}$ é um funcional linear escolhido de modo que

$$\begin{aligned} f(\mathbf{v}_1) &= 0 \\ f(T(\mathbf{v}_1)) &= 0 \\ \vdots \quad & \vdots \\ f(T^{m-2}(\mathbf{v}_1)) &= 0 \\ f(T^{m-1}(\mathbf{v}_1)) &= 1. \end{aligned}$$

Observe que é possível escolher tal funcional pois os vetores $\mathbf{v}_1, T(\mathbf{v}_1), \ldots,$ $T^{m-1}(\mathbf{v}_1)$ são linearmente independentes e, portanto, parte de uma base para $V$.

Afirmamos agora que $\tau\restriction_{Z_{\mathbf{v}_1}} : Z_{\mathbf{v}_1} \to \mathbb{K}^m$ é um isomorfismo. Para demonstrar isso, encontramos a representação matricial para $\tau\restriction_{Z_{\mathbf{v}_1}}$.

Usando a base $\underline{\mathrm{B}} = \{\mathbf{v}_1, T(\mathbf{v}_1), \ldots, T^{m-1}(\mathbf{v}_1)\}$ para $Z_{\mathbf{v}_1}$ e a base canônica $\underline{\mathrm{C}} = \mathbf{e}_1, \ldots, \mathbf{e}_m$ para $\mathbb{K}^m$.

Vemos que:

$$[\tau]_{\underline{B},\underline{C}} = \begin{bmatrix} 0 & 0 & \dots & 1 \\ \vdots & & \iddots & * \\ 0 & 1 & \dots & * \\ 1 & * & * & * \end{bmatrix}$$

onde $*$ indica que não nos importamos com o valor da entrada.

Como a matriz é invertível, temos que $\tau\restriction_{Z_{\mathbf{v}_1}} : Z_{\mathbf{v}_1} \to \mathbb{K}^m$ é um isomorfismo.

Em seguida, precisamos mostrar que $\ker \tau$ é $T$-invariante. Seja $\mathbf{v} \in \ker \tau$ logo por definição

$$\tau(\mathbf{v}) = [f(\mathbf{v}), f(T(\mathbf{v})), \ldots, f(T^{m-1}(\mathbf{v}))] = [0, 0, \ldots, 0]$$

e consequentemente

$$\tau(T(\mathbf{v})) = [f(T(\mathbf{v})), f(T^2(\mathbf{v})), \ldots, f(T^{m-1}(\mathbf{v})), f(T^m(\mathbf{v}))] = [0, 0, \ldots, f(T^m(\mathbf{v}))]$$

Agora, pela definição de $m$, temos que $T^m(\mathbf{v})$ é uma combinação linear de $(\mathbf{v}), T(\mathbf{v}), \ldots, T^{m-1}(\mathbf{v})$. Isso mostra que $f(T^m(\mathbf{v})) = 0$ e, consequentemente, $T(\mathbf{v}) \in \ker \tau$.

Finalmente, mostramos que $V = Z_{\mathbf{v}_1} \oplus \ker \tau$. Vimos que $\tau\restriction_{Z_{\mathbf{v}_1}} : Z_{\mathbf{v}_1} \to \mathbb{K}^m$ é um isomorfismo. Isso implica que $Z_{\mathbf{v}_1} \cap \ker \tau = \{0\}$.

Logo

$$\begin{aligned}
\dim(V) &= \dim(\ker\tau) + \dim(\mathrm{im}\,\tau) && (1)\\
&= \dim(\ker\tau) + m && (2)\\
&= \dim(\ker\tau) + \dim(Z_{\mathbf{v}_1}) && (3)\\
&= \dim(\ker\tau + Z_{\mathbf{v}_1})\ . && (4)
\end{aligned}$$

Assim, $V = Z_{\mathbf{v}_1} + \ker\tau = Z_{\mathbf{v}_1} \oplus \ker\tau$.

Logo temos a decomposição $V = \bigoplus_{j=1}^{k} Z_{\mathbf{v}_j}$.

# Comentários Finais.