# SUBESPAÇOS CÍCLICOS

DANIEL V. TAUSK

Ao longo de todo o texto, $K$ denota um corpo, $K[X]$ denota o anel de polinômios com coeficientes nesse corpo, $V$ denota um espaço vetorial sobre $K$ (não necessariamente de dimensão finita) e $T : V \to V$ denota um operador linear. Recordamos que um subespaço $W$ de $V$ é dito *$T$-invariante* se $T[W] \subset W$; nesse caso, $T|_W$ denota o operador linear em $W$ obtido pela restrição do domínio e do contra-domínio de $T$ a $W$. Se $m \geq 1$ é um inteiro, então $T^m$ denota a $m$-ésima potência de $T$ com repeito à operação de composição de operadores; $T^0$ denota o operador identidade $\mathrm{I} : V \to V$.

**Definição 1.** Dado um vetor $v \in V$, então o *subespaço $T$-cíclico* de $V$ (ou simplesmente *subespaço cíclico*, quando $T$ estiver subentendido) gerado por $v$, denotado por $Z(v;T)$, é o subespaço de $V$ gerado pelo conjunto:

$$\big\{T^m(v) : m \geq 0\big\}.$$

Quando $V = Z(v;T)$, dizemos que $v$ é um *vetor cíclico* para o operador $T$.

É fácil ver que:

$$Z(v;T) = \big\{p(T)(v) : p(X) \in K[X]\big\}.$$

**Exercício 2.** Dado $v \in V$, mostre que $Z(v;T)$ é o menor subespaço $T$-invariante de $V$ contendo $v$, isto é:

(i) $Z(v;T)$ é um subespaço $T$-invariante de $V$ e $v \in Z(v;T)$;
(ii) se $W$ é um subespaço $T$-invariante de $V$ e $v \in W$, então $W$ contém $Z(v;T)$.

Note que $v$ é sempre um vetor cíclico para o operador $T|_{Z(v;T)}$.

**Exercício 3.** Dado $v \in V$, mostre que o conjunto:

$$\big\{p(X) \in K[X] : p(T)(v) = 0\big\} \tag{1}$$

é um ideal de $K[X]$.

**Exercício 4.** Seja $v \in V$ e suponha que a seqüência $\big(T^m(v)\big)_{m\geq 0}$ seja linearmente independente (de modo que ela é então uma base do subespaço cíclico $Z(v;T)$). Mostre que o ideal (1) é nulo.

Vejamos agora o que acontece quando a seqüência $\big(T^m(v)\big)_{m\geq 0}$ é linearmente dependente.

---

*Date*: 15 de junho de 2014.

**Proposição 5.** *Seja $v \in V$. Suponha que a seqüência $\big(T^m(v)\big)_{m\geq 0}$ seja linearmente dependente (isso é necessariamente verdade, por exemplo, se $V$ tiver dimensão finita). Nesse caso, existe um inteiro $k \geq 0$ tal que a seqüência $\big(T^m(v)\big)_{0\leq m\leq k}$ é linearmente dependente. Denote por $k$ o menor inteiro não negativo com essa propriedade. Temos que existem (e são únicos) escalares $a_i \in K$, $i = 0, 1, \ldots, k-1$, tais que:*

$$T^k(v) = \sum_{i=0}^{k-1} a_i T^i(v). \tag{2}$$

*Além do mais, vale que:*

(a) *a seqüência $\big(T^m(v)\big)_{0\leq m\leq k-1}$ é uma base do subespaço cíclico $Z(v;T)$ e portanto $Z(v;T)$ tem dimensão $k$;*

(b) *o ideal (1) é não nulo e o polinômio:*

$$p(X) = X^k - \sum_{i=0}^{k-1} a_i X^i \in K[X] \tag{3}$$

*é o gerador mônico desse ideal.*

*Demonstração.* Se uma família de vetores é linearmente dependente, então alguma subfamília finita dela é linearmente dependente também; assim, existe um inteiro $k \geq 0$ tal que $\big(T^m(v)\big)_{0\leq m\leq k}$ é linearmente dependente. Denotamos por $k \geq 0$ o menor inteiro com essa propriedade. Como $\big(T^m(v)\big)_{0\leq m\leq k-1}$ é linearmente independente e $\big(T^m(v)\big)_{0\leq m\leq k}$ é linearmente dependente, temos que existem (e são únicos) escalares $a_i \in K$, $i = 0, 1, \ldots, k-1$, tais que (2) vale. Daí, se $p(X)$ é definido como em (3), então $p(T)(v) = 0$. Do fato que $\big(T^m(v)\big)_{0\leq m\leq k-1}$ é linearmente independente, segue imediatamente que o ideal (1) não contém polinômios não nulos de grau menor do que $k$. Isso completa a demonstração do item (b). Para demonstrar o item (a), resta ver que $\big\{T^m(v) : 0 \leq m \leq k-1\big\}$ gera $Z(v;T)$. Todo elemento de $Z(v;T)$ é da forma $\tilde{p}(T)(v)$, com $\tilde{p}(X) \in K[X]$. Usando o algorítmo de divisão de Euclides, obtemos $q(X), r(X) \in K[X]$ tais que:

$$\tilde{p}(X) = q(X)p(X) + r(X), \tag{4}$$

sendo que $r(X)$ tem grau menor do que $k$. Avaliando os dois lados de (4) em $T$ e depois em $v$, obtemos:

$$\tilde{p}(T)(v) = r(T)(v),$$

já que $p(T)(v) = 0$. Do fato que $r(X)$ tem grau menor do que $k$ segue que $r(T)(v)$ pertence ao subespaço gerado por $\big\{T^m(v) : 0 \leq m \leq k-1\big\}$. Isso completa a demonstração. □

**Definição 6.** Seja $v \in V$. Se o ideal (1) é não nulo, então o seu único gerador mônico é denotado por $\mathrm{Ann}(v;T)$ e é chamado o *$T$-aniquilador* do vetor $v$.

A próxima proposição é um corolário simples do resultado do Exercício 4 e da Proposição 5.

**Proposição 7.** *Dado $v \in V$, são equivalentes as seguintes condições:*

(a) *a seqüência $\big(T^m(v)\big)_{m\geq 0}$ é linearmente dependente;*

(b) *$v$ possui um $T$-aniquilador (isto é, o ideal (1) é não nulo);*

(c) *$Z(v;T)$ tem dimensão finita.*

*Além do mais, se $v$ possui um $T$-aniquilador, então o grau de $\mathrm{Ann}(v;T)$ é igual à dimensão de $Z(v;T)$.*

*Demonstração.* As implicações (a)⇒(b) e (a)⇒(c) seguem da Proposição 5, a implicação (b)⇒(a) segue do resultado do Exercício 4 e a implicação (c)⇒(a) é óbvia. A última afirmação do enunciado também segue da Proposição 5. □

**Exercício 8.** Mostre que se $T$ admite um polinômio minimal $m_T(X)$, então todo vetor $v \in V$ admite um $T$-aniquilador e esse $T$-aniquilador divide $m_T(X)$.

**Exercício 9.** Mostre que o vetor nulo $0 \in V$ admite um $T$-aniquilador e que esse $T$-aniquilador é o polinômio $1 \in K[X]$. Mostre que se um vetor não nulo $v \in V$ admite um $T$-aniquilador, então esse $T$-aniquilador tem grau positivo.

**Exercício 10.** Seja $v \in V$. Para um polinômio $p(X) \in K[X]$, mostre que são equivalentes as seguintes condições:

(a) $p(T)(v) = 0$;

(b) $p(T)|_{Z(v;T)} = 0$;

(c) $p\big(T|_{Z(v;T)}\big) = 0$.

Conclua que $v$ admite um $T$-aniquilador se e somente se $T|_{Z(v;T)}$ admite um polinômio minimal e que, quando ambos existem, o $T$-aniquilador de $v$ e o polinômio minimal de $T|_{Z(v;T)}$ são iguais. Em particular, se $v$ é um vetor cíclico para $T$, então $v$ admite um $T$-aniquilador se e somente se $T$ admite um polinômio minimal e $m_T(X) = \mathrm{Ann}(v;T)$ quando ambos existem.

**Definição 11.** Seja $v \in V$. Se a seqüência $\big(T^m(v)\big)_{m\geq 0}$ for linearmente independente, então ela é chamada a *base $T$-cíclica* do subespaço $Z(v;T)$ gerada por $v$; se ela for linearmente dependente e se $k \geq 0$ é o menor inteiro tal que $\big(T^m(v)\big)_{0\leq m\leq k}$ é linearmente dependente, então a *base $T$-cíclica* de $Z(v;T)$ gerada por $v$ é $\big(T^m(v)\big)_{0\leq m\leq k-1}$ (veja Proposição 5).

**Definição 12.** Seja $p(X) = X^k - \sum_{i=0}^{k-1} a_i X^i \in K[X]$ um polinômio mônico, com $a_0, a_1, \ldots, a_{k-1} \in K$. A *matriz companheira* de $p(X)$ é matriz $k \times k$ com entradas em $K$ definida por:

$$C(p) = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{k-1} \end{pmatrix}.$$

Mais precisamente, temos:

$$[C(p)]_{ij} = \begin{cases} 1, & \text{se } 1 \leq j \leq k-1 \text{ e } i = j+1, \\ a_{i-1}, & \text{se } j = k, \\ 0, & \text{em todos os outros casos.} \end{cases}$$

**Exercício 13.** Suponha que $v \in V$ admita um $T$-aniquilador e seja $\mathcal{B}$ a base $T$-cíclica gerada por $v$ do espaço $Z(v;T)$. Mostre que a matriz que representa $T|_{Z(v;T)}$ na base $\mathcal{B}$ é precisamente a matriz companheira do polinômio $\mathrm{Ann}(v;T)$.

**Exercício 14.** Suponha que $V$ tenha dimensão finita e que $\mathcal{B} = (e_1, \ldots, e_k)$ seja uma base de $V$ tal que $[T]_{\mathcal{B}}$ é a matriz companheira de um polinômio mônico $p(X) \in K[X]$. Mostre que $e_1$ é um vetor cíclico para $T$, que $\mathcal{B}$ é a base $T$-cíclica de $V = Z(e_1;T)$ gerada por $e_1$ e que $p(X)$ é o $T$-aniquilador de $e_1$ e também o polinômio minimal de $T$. (Sugestão: para ver que $p(X)$ é o polinômio minimal de $T$, use o resultado do Exercício 10.)

**Exercício 15.** Seja $p(X)$ um polinômio mônico de grau $k \geq 0$ e seja $C(p)$ a sua matriz companheira. Considere a matriz $X\mathrm{I} - C(p)$ com entradas no anel de polinômios $K[X]$.

(a) Dado $i = 1, \ldots, k$, mostre que a matriz obtida de $X\mathrm{I} - C(p)$ pela remoção da $i$-ésima linha e da $k$-ésima coluna é da forma:

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \in M_{k-1}(K),$$

onde $A \in M_{i-1}(K)$ é uma matriz triangular inferior cujos elementos da diagonal principal são todos iguais a $X$ e $B \in M_{k-i}(K)$ é uma matriz triangular superior cujos elementos da diagonal principal são todos iguais a $-1$.

(b) Usando expansão por cofatores na última coluna, mostre que:

$$\det\big(X\mathrm{I} - C(p)\big) = p(X).$$

**Proposição 16.** *Suponha que* $\dim(V) < +\infty$ *e que* $T$ *admita um vetor cíclico. Então os polinômios minimal e característico de* $T$ *coincidem.*

*Demonstração.* Se $v \in V$ é um vetor cíclico, i.e., $V = Z(v;T)$, então o polinômio minimal $m_T(X)$ é o $T$-aniquilador de $v$ (Exercício 10). Além do mais, se $\mathcal{B}$ é a base $T$-cíclica de $V$ gerada por $v$, então a matriz $[T]_{\mathcal{B}}$ é a matriz companheira de $m_T(X) = \mathrm{Ann}(v;T)$ (Exercício 13). Daí o polinômio característico de $T$ é:

$$\det\big(X\mathrm{I} - [T]_{\mathcal{B}}\big) = \det\big(X\mathrm{I} - C(m_T)\big) = m_T(X),$$

pelo resultado do item (b) do Exercício 15. □

*Observação* 17. É um fato não trivial (conseqüência da *forma canônica racional*) que vale a recíproca da Proposição 16, isto é, supondo $\dim(V) < +\infty$, se os polinômios característico e minimal de $T$ coincidem, então $T$ admite um vetor cíclico.

**Exercício 18.** Suponha que $\dim(V) < +\infty$ e que $W$ seja um subespaço $T$-invariante de $V$. Mostre que o polinômio característico de $T|_W$ é um divisor do polinômio característico de $T$. (Sugestão: seja $\mathcal{B} = (e_i)_{1\leq i\leq n}$ uma base de $V$ tal que $\mathcal{B}' = (e_i)_{1\leq i\leq k}$ seja uma base de $W$. Note que o bloco superior esquerdo de tamanho $k \times k$ de $[T]_{\mathcal{B}}$ é a matriz que representa $T|_W$ na base $\mathcal{B}'$ e que o bloco inferior esquerdo de tamanho $(n-k) \times k$ de $[T]_{\mathcal{B}}$ é nulo.)

**Teorema 19** (Cayley–Hamilton)**.** *Suponha que* $\dim(V) < +\infty$ *e seja* $p_T(X)$ *o polinômio característico de* $T$*. Então* $p_T(T) = 0$*. Em outras palavras, o polinômio minimal* $m_T(X)$ *é um divisor de* $p_T(X)$*.*

*Demonstração.* Segue imediatamente da Proposição 16 que o teorema vale se $T$ admite um vetor cíclico. Em geral, seja $v \in V$ e vamos mostrar que $p_T(T)(v) = 0$. Seja $W = Z(v;T)$ o subespaço $T$-cíclico gerado por $v$. Daí $T|_W$ admite um vetor cíclico e portanto:

$$p_{(T|_W)}(T|_W) = 0,$$

donde:

$$p_{(T|_W)}(T)(v) = 0,$$

já que $v \in W$. A conclusão segue agora do resultado do Exercício 18. □

**Exercício 20.** Suponha que $T$ admita um polinômio minimal $m_T(X)$ e seja $p(X) \in K[X]$ um divisor mônico irredutível de $m_T(X)$. Nesse caso, $p(T)$ não é injetor (recorde Exercício 19 do texto sobre decomposição primária). Mostre que para todo $v \in \mathrm{Ker}\big(p(T)\big)$ não nulo, vale que o $T$-aniquilador de $v$ é $p(X)$. Conclua que $V$ admite um subespaço $T$-invariante cuja dimensão é o grau de $p(X)$.

**Exercício 21.** Suponha que $K = \mathbb{R}$ e que $1 \leq \dim(V) < +\infty$. Mostre que $V$ admite um subespaço $T$-invariante de dimensão 1 ou 2. (Sugestão: use o resultado do Exercício 20.)