

Álgebra Linear Avançada

Decomposição Primária

Adriano Moura

Unicamp

2020

Polinômio Mínimo e Teor. da Decomposição Primária

Contexto: V é um \mathbb{F} -espaço vetorial e $T \in \text{End}_{\mathbb{F}}(V)$.

Lembre: Dado polinômio $p \in \mathcal{P}(\mathbb{F})$, $V_p := \{v \in V : p(T)(v) = 0\}$.

($p(t) = a_0 + a_1t + \cdots + a_nt^n \rightsquigarrow p(T)(v) = a_0v + a_1T(v) + \cdots + a_nT^n(v)$)

Defina $\mathcal{A}_T = \{p \in \mathcal{P}(\mathbb{F}) : p(T) = 0\}$. (conjunto aniquilador de T)

Teorema

- 1 Se $\dim(V)$ é finita, $\mathcal{A}_T \neq \{0\}$.
- 2 Se $\mathcal{A}_T \neq \{0\}$, existe único polinômio mônico $m_T \in \mathcal{P}(\mathbb{F})$ que divide todos os elementos de \mathcal{A}_T . (chamado de polinômio mínimo de T)

Teorema da Decomposição Primária (TDP)

Suponha que $\mathcal{A}_T \neq \{0\}$ e sejam p_1, \dots, p_m os fatores irredutíveis distintos de m_T em $\mathcal{P}(\mathbb{F})$. Se k_j é a multiplicidade de p_j em m_T , temos

$$V = V_{p_1}^{k_1} \oplus \cdots \oplus V_{p_m}^{k_m}.$$

Os polinômios $p_j^{k_j}$ são chamados de fatores primários (fp) de T e $V_{p_j}^{k_j}$ é dito um subespaço T -primário de V .

Diagonalização e Subespaços Invariantes

Se $V = \mathcal{P}(\mathbb{F})$ e T é o operador $f(t) \mapsto tf(t)$, $\mathcal{A}_T = \{0\}$. (Ex. 8.1.5)

Se $\mathcal{A}_T = \{0\}$, define-se $m_T = 0$. Segue que $V = V_{m_T}$.

Corolário

T é diagonalizável se, e só se, seus fatores primários tiverem grau 1.

Dem. de \Leftarrow : Se os fp tiverem grau 1, temos $m_T = \prod_{j=1}^m (t - \lambda_j)$ com $\lambda_i \neq \lambda_j$ se $i \neq j$, e o TDP diz que V é soma de autoespaços:

$$V = V_{t-\lambda_1} \oplus \cdots \oplus V_{t-\lambda_m}$$

Um subespaço W de V é dito T -invariante se $T(W) \subseteq W$.

Em particular, a restrição de T a W induz um operador linear em W dado por $w \mapsto T(w)$ para todo $w \in W$.

Lema 8.1.1

Se $S \in \text{End}_{\mathbb{F}}(V)$ satisfaz $S \circ T = T \circ S$, V_S é T -invariante.

Em particular, V_p é T -invariante para todo $p \in \mathcal{P}(\mathbb{F})$.

Generalizando a Noção de Autoespaço

Objetivo – descrever o conjunto $\{p \in \mathcal{P}(\mathbb{F}) : V_p \neq \{0\}\}$. Observe que

$$(1) \quad V_p \subseteq V_{fp} \quad \text{para quaisquer} \quad f, p \in \mathcal{P}(\mathbb{F}).$$

Em particular,

$$V_{p^k} \subseteq V_{p^{k+1}} \quad \text{para qualquer} \quad k \geq 0.$$

Isso implica que o conjunto

$$V_p^\infty := \bigcup_{k \geq 0} V_{p^k}$$

é um subespaço (T -invariante) de V . Para $p(t) = t - \lambda$ com $\lambda \in \mathbb{F}$, o espaço V_p^∞ é chamado de autoespaço generalizado associado a λ .

Se $T : \mathbb{F}^2 \rightarrow \mathbb{F}^2$ é dado por $T(x, y) = (y, 0)$ e $p(t) = t$ temos

$$V_p = V_T = [e_1] \quad \text{e} \quad V_{p^2} = \mathbb{F}^2 \quad (\text{pois } T^2 = 0).$$

Além disso, se $f \in \mathcal{P}(\mathbb{F})$ e $p \nmid f$, temos $V_f = \{0\}$. De fato, se $f = pq + r$ é a divisão de f por p , temos $r \in \mathbb{F} \setminus \{0\}$ e

$$\begin{aligned} f(T)(x, y) &= q(T)(T(x, y)) + r(x, y) = q(T)(y, 0) + r(x, y) \\ &= (q(0)y + rx, ry) \xrightarrow{r \neq 0} f(T)(x, y) = (0, 0) \Leftrightarrow 0 = y = x. \end{aligned}$$

Existência do Polinômio Mínimo

Se $\mathcal{A}_T \neq \{0\}$, $\exists !$ polinômio mônico que divide todo elemento de \mathcal{A}_T .

Dem.: Seja $m = \min\{k : \exists p \in \mathcal{A}_T \setminus \{0\}, \text{gr}(p) = k\} > 0$.

Tome $f, p \in \mathcal{A}_T$ com $\text{gr}(p) = m$. Escreva a divisão de f por p :

$f = qp + r$ ($\text{gr}(r) < m$). Note que $r = f - qp \in \mathcal{A}_T$

e, pela minimalidade de m , devemos ter $r = 0$ mostrando que $p|f$.

Segue que qualquer polinômio não constante de grau mínimo em \mathcal{A}_T divide qualquer polinômio de \mathcal{A}_T . Um polinômio divide outro com o mesmo grau apenas se for múltiplo escalar do outro. \square

A descrição do conjunto $\{p \in \mathcal{P}(\mathbb{F}) : V_p \neq \{0\}\}$ segue de:

Proposição 8.1.7

Se $\mathcal{A}_T \neq \{0\}$ e $p \in \mathcal{P}(\mathbb{F})$ é irredutível, $V_p \neq \{0\}$ se, e somente se, $p|m_T$.

Lema 8.1.6

Se $\text{mdc}(f, g) = 1$, a restrição de $f(T)$ a V_g é injetora.

Demonstração da Prop. 8.1.7

Dem. do Lema: Sejam $p, q \in \mathcal{P}(\mathbb{F})$ tais que $pf + qg = 1$. Então, para todo $v \in V_g$ temos

$$v = (p(T)f(T) + q(T)g(T))(v) = p(T)(f(T)(v))$$

já que $g(T)(v) = 0$. Segue que a restrição de $p(T) \circ f(T)$ a V_g é a função identidade, de onde segue o lema. □

Dem. da Prop.: Suponha que $p|m_T$ e $V_p = \{0\}$, isto é, $p(T)(u) \neq 0$ para todo $u \in V \setminus \{0\}$. Considere $f = \frac{m_T}{p}$ e observe que

$$0 = m_T(T)(v) = p(T)(f(T)(v)) \quad \text{para qualquer} \quad v \in V.$$

Como $p(T)(f(T)(v)) \neq 0$ se $f(T)(v) \neq 0$, segue que $f \in \mathcal{A}_T$, gerando uma contradição pois $\text{gr}(f) < \text{gr}(m_T)$.

Reciprocamente, se $p \nmid m_T$, então $\text{mdc}(p, m_T) = 1$ (pois p é irredutível) e segue do Lema que a restrição de $m_T(T)$ a V_p é injetora. Como $m_T(T) = 0$, concluímos que $V_p = \{0\}$.

Dimensão Finita - Como calcular m_T

Se $\dim(V) = n$ é finita, $\mathcal{A}_T \neq \{0\}$.

Dem.: Se $T = 0$, então $\mathcal{A}_T = \{p \in \mathcal{P}(\mathbb{F}) : p(0) = 0\} \neq \{0\}$.

Suponha então que $T \neq 0$ e lembre que $\dim(\text{End}_{\mathbb{F}}(V)) = n^2$.

Logo, a família $(T^k)_{k=0,\dots,n^2}$ é l.d..

Como a subfamília formada por $T^0 = \text{Id}_V$ é l.i., existe $1 \leq m \leq n^2$ mínimo tal que a subfamília $(T^k)_{k=0,\dots,m}$ seja l.d..

Sejam então $a_0, \dots, a_{m-1} \in \mathbb{F}$ tais que

$$T^m = a_0 \text{Id}_V + \dots + a_{m-1} T^{m-1} \quad \text{e} \quad f(t) = t^m - \sum_{k=0}^{m-1} a_k t^k.$$

Segue que $f(T) = 0$ e, portanto, $f \in \mathcal{A}_T \setminus \{0\}$. □

Exercício: Mostre que $m_T = f$ sendo f como na demonstração. Como usar este fato e representações matriciais de T para calcular m_T ?

Subespaços Cíclicos

Dado $v \in V$, considere a sequência de vetores

$v_0 = v, v_1 = T(v), \dots, v_k = T^k(v), \dots$ chamada T -ciclo gerado por v .

Notação: $\mathcal{C}_T^\infty(v) = (v_k)_{k \geq 0}$, $\mathcal{C}_T^m(v) = v_0, v_1, \dots, v_{m-1}$. Defina

$$C_T(v) = [\mathcal{C}_T^\infty(v)] \quad \text{subespaço } T\text{-cíclico gerado por } v$$

Se $\dim(V)$ é finita, existe $m \geq 0$ mínimo tal que $\mathcal{C}_T^{m+1}(v)$ é l.d.. Note que $m \geq 1$ se $v \neq 0$. Em particular, $\mathcal{C}_T(v) := \mathcal{C}_T^m(v)$ é base de $C_T(v)$ e v_m é combinação linear dos vetores l.i. v_0, \dots, v_{m-1} , digamos

$$v_m = a_0 v_0 + \dots + a_{m-1} v_{m-1} = \sum_{k=0}^{m-1} a_k T^k(v).$$

Definindo $m_{T,v}(t) = t^m - a_{m-1}t^{m-1} - \dots - a_1 t - a_0$,

temos

$$m_{T,v}(T)(v) = v_m - \sum_{k=0}^{m-1} a_k T^k(v) = 0,$$

mostrando que $v \in V_{m_{T,v}}$. Como $V_{m_{T,v}}$ é T -invariante, segue que

$$C_T(v) \subseteq V_{m_{T,v}}.$$

Subespaços Cíclicos e Divisores de m_T

Simplificando a notação: m_v ao invés de $m_{T,v}$.

Proposição

Para todo $v \in V$, $m_v | m_T$.

Dem.: Sendo V_{m_v} T -invariante, podemos considerar o operador induzido

$$S : V_{m_v} \rightarrow V_{m_v}, \quad v \mapsto T(v).$$

Note que $m_v \in \mathcal{A}_S$ e, portanto, $m_S | m_v$.

De fato, $m_v = m_S$ pois, se fosse $\text{gr}(m_S) = m' < m$, seguiria que $v_0, \dots, v_{m'}$ seria l.d., contradizendo a minimalidade de m .

A proposição segue pois, obviamente $m_T \in \mathcal{A}_S$. □

Estudar Exemplo 8.1.10.

Este é um momento ideal para uma pausa no desenvolvimento da teoria.

O material estudado já fornece ao aluno informação suficiente para trabalhar nos exercícios 8.1.1 a 8.1.13. É fortemente recomendável que isso seja feito antes de prosseguir com a teoria. Os demais exercícios da Seção 8.1 dependem da noção de polinômio característico, que é o ponto culminante da próxima sequência de slides.

Para as próximas demonstrações, é crucial que o aluno esteja confortável com as noções de soma direta e correspondentes projeções. Assim, recomenda-se revisar a Seção 5.3 bem como os Exercícios 6.3.6 e 6.3.7.

Coprimidade \Rightarrow Soma Direta

Proposição 8.1.11

Se $p_1, \dots, p_m \in \mathcal{P}(\mathbb{F})$ são dois a dois relativamente primos, a soma $V_{p_1}^\infty + \dots + V_{p_m}^\infty$ é direta.

Dem.: Tome $v_j \in V_{p_j}^\infty \setminus \{0\}$, $1 \leq j \leq m$. Objetivo: mostrar que v_1, \dots, v_m é l.i.. Faremos por indução em m que obviamente começa quando $m = 1$. Suponha então que $a_1, \dots, a_m \in \mathbb{F}$ satisfazem $a_1 v_1 + \dots + a_m v_m = 0$ e, por hip. de indução, que v_1, \dots, v_{m-1} seja l.i.. Para cada $1 \leq j \leq m$, escolha k_j tal que $p_j^{k_j}(T)(v_j) = 0$, considere

$$p = \prod_{j=1}^{m-1} p_j^{k_j}$$

e observe que

$$0 = p(T)(a_1 v_1 + \dots + a_m v_m) = a_m p(T)(v_m).$$

Como a restrição de $p_j^{k_j}(T)$ a $V_{p_m}^{k_m}$ é injetora para $j \neq m$, segue que $p(T)(v_m) \neq 0$ e, portanto, $a_m = 0$. A hipótese de indução agora implica que $a_j = 0$ para todo j .

Decompondo V

Proposição 8.1.12

Sejam $f_1, \dots, f_m \in \mathcal{P}(\mathbb{F})$ dois a dois relativamente primos e $f = f_1 \cdots f_m$. Então, $V_f = V_{f_1} \oplus \cdots \oplus V_{f_m}$.

Dem.: Faremos para $m = 2$. O caso geral segue por indução em m . Segue de (1) que $V_{f_1} + V_{f_2} \subseteq V_f$. Acabamos de ver que a soma é direta.

Sejam $g_1, g_2 \in \mathcal{P}(\mathbb{F})$ t.q. $g_1 f_1 + g_2 f_2 = 1$ e defina $h_j = g_j f_j$ e $P_j = h_j(S)$, sendo S o operador linear induzido por T em V_f . Então $f \in \mathcal{A}_S$, $P_1 + P_2 = \text{Id}_{V_f}$ e

$$P_1 P_2 = g_1(S) f_1(S) g_2(S) f_2(S) = g_1(S) g_2(S) f_1(S) f_2(S) = 0 = P_2 P_1.$$

Em particular, $P_j^2 = P_j - P_i P_j = P_j$ se $\{i, j\} = \{1, 2\}$ e $\text{Im}(P_j) \subseteq V_{f_i}$. Pelo Exercício 6.3.7, $V_f = \text{Im}(P_2) \oplus \text{Im}(P_1) \subseteq V_{f_1} \oplus V_{f_2} \subseteq V_f$. \square

O TDP segue desta proposição com $f_j = p_j^{k_j}$ pois $V = V_{m_T}$.

Estudar o Exemplo 8.1.15

Quebras em Soma de Subespaços Cíclicos

Proposição 8.1.17

Se $p \in \mathcal{P}(\mathbb{F})$ é irredutível e $\dim(V_p)$ é finita, existem $l \geq 0$ e $v_1, \dots, v_l \in V_p$ tais que $V_p = C_T(v_1) \oplus \dots \oplus C_T(v_l)$.

O principal Teorema da Seção 8.2 (Teorema da Decomposição Cíclica) é uma forte generalização desta proposição.

Lema 8.1.16

Se $p \in \mathcal{P}(\mathbb{F})$ é irredutível e $u, v \in V$ satisfazem $m_u = m_v = p$, exatamente uma das duas opções ocorre:

$$C_T(u) = C_T(v) \quad \text{ou} \quad C_T(u) \cap C_T(v) = \{0\}.$$

Dem. do Lema: Exercício.

Exercício (8.1.10): Mostre que $C_T(v) = \{p(T)(v) : p \in \mathcal{P}(\mathbb{F})\}$.

Um subespaço W é dito T -cíclico se $W = C_T(v)$ para algum $v \in V$.

Quebras em Soma de Subespaços Cíclicos

p irredutível e $\dim(V_p) < \infty \Rightarrow$ existem $l \geq 0$ e $v_1, \dots, v_l \in V_p$ t.q.
 $V_p = C_T(v_1) \oplus \dots \oplus C_T(v_l)$.

Dem.: Suponha que tenhamos encontrado vetores $v_1, \dots, v_k \in V_p$, t.q. a soma $C_T(v_1) + \dots + C_T(v_k)$ seja direta. Mostraremos que

$$(*) \quad C_T(v) \cap (C_T(v_1) + \dots + C_T(v_k)) = \{0\}$$

para todo $v \in V_p \setminus C_T(v_1) + \dots + C_T(v_k)$.

Supondo que isto é verdade, como $\dim(V_p)$ é finita, fica claro como escolher tal sequência de vetores começando com $v_1 \in V_p$ arbitrário.

Para demonstrar (*), suponha que $w \in C_T(v) \cap (C_T(v_1) + \dots + C_T(v_k))$ seja não nulo. Então, existem $w_j \in C_T(v_j)$ t.q. $w = w_1 + \dots + w_k$. Pelo lema anterior, $C_T(w) = C_T(v)$ e, portanto, existe $f \in \mathcal{P}(\mathbb{F})$ tal que $v = f(T)(w)$ (Exercício 8.1.10). Mas então,

$$v = f(T)(w_1) + \dots + f(T)(w_k) \in C_T(v_1) + \dots + C_T(v_k),$$

contradizendo nossa hipótese sobre v .

Subespaços Primários e o Grau do seu Polinômio Primo

Proposição 8.1.18

Se $p \in \mathcal{P}(\mathbb{F})$ é irreduzível e $\dim(V_p^\infty)$ é finita, $\text{gr}(p) \mid \dim(V_p^\infty)$. Além disso,

$$\frac{\dim(V_p^\infty)}{\text{gr}(p)} \geq \min\{k : V_p^\infty = V_{p^k}\}$$

valendo a igualdade se, e somente se, V_p^∞ for T -cíclico.

Dem.: Defina $m = \min\{k : V_p^\infty = V_{p^k}\}$. Começemos com o caso que V_p^∞ é T -cíclico. Seja S o operador induzido por T em $V_p^\infty = V_{p^m}$ e note que $m_S = p^m$. Além disso, se v satisfaz $V_p^\infty = C_T(v)$, segue que $m_v = m_S = p^m$. Como $\dim(C_T(v)) = \text{gr}(m_v) = m \text{gr}(p) \Rightarrow \square$.

Agora procedemos por indução em $n = \dim(V_p^\infty)$. Para $n = 1$ é claro.

Suponha $n > 1$ e enunciemos a hip. de indução precisamente:

Se S é um operador linear num espaço vetorial W t.q. $\dim(W_{p(S)}^\infty) < n$,

$$\text{gr}(p) \mid \dim(W_{p(S)}^\infty) \quad \text{e} \quad \frac{\dim(W_{p(S)}^\infty)}{\text{gr}(p)} \geq \min\{k : W_{p(S)}^\infty = W_{p^k}\}.$$

Para $m = 1$, o caso cíclico junto com a Prop. 8.1.17 completam a dem.

Subespaços Primários e o Grau do seu Polinômio Primo

Se $m > 1$, considere $W = V_{p^{m-1}}$ que é um subespaço T -invariante, próprio e não trivial de V_p^∞ . Seja S o operador induzido por T em W e note que $W = W_{p(S)}^\infty = V_{p^{m-1}}$. Logo a hip. de indução nos diz que

$$\text{gr}(p) \mid \dim(W) \quad \text{e} \quad \frac{\dim(W)}{\text{gr}(p)} \geq m - 1.$$

Por fim, seja R o operador em V_p^∞ induzido por $p^{m-1}(T) = p(T)^{m-1}$. Observe que $W = \mathcal{N}(R)$. Pelo Teorema 6.3.6,

$$\dim(V_p^\infty) = \dim(W) + \dim(\text{Im}(R)).$$

Logo, nos resta mostrar que $\text{gr}(p) \mid \dim(\text{Im}(R))$. Note que $\text{Im}(R)$ é T -invariante pois, se $w = R(v)$ com $v \in V_p^\infty$, como $R \circ T = T \circ R$, vale

$$T(w) = T(R(v)) = R(T(v)) \in \text{Im}(R).$$

Além disso, $\text{Im}(R) \subseteq V_p$ pois, se $v \in V_p^\infty$, $p(T)(R(v)) = p^m(T)(v) = 0$. Assim, pode-se concluir a demonstração usando-se hipótese de indução com $\text{Im}(R)$ no lugar de W . □

Polinômio Característico

Se $\dim(V) = n$ é finita e $p_j^{k_j}, 1 \leq j \leq m$, são os fatores primários de T , segue que

$$\text{gr}(m_T) = \sum_{j=1}^m k_j \text{ gr}(p_j) \leq \sum_{j=1}^m \dim(V_{p_j^{k_j}}) = n.$$

pois

$$k_j = \min\{k : V_{p_j^k} = V_{p_j^{k+1}}\}.$$

Considere o número inteiro

$$n_j = \frac{\dim(V_{p_j^{k_j}})}{\text{gr}(p_j)} \geq k_j$$

e defina

$$c_T = \prod_{j=1}^m p_j^{n_j}.$$

Este polinômio é chamado de o polinômio característico de T .

Por definição, $\text{gr}(c_T) = n$ e $c_T \in \mathcal{A}_T$ (Teor. de Cayley-Hamilton!).

Chame de T_j o operador induzido por T em $V_{p_j^{k_j}}$ e note que

$$c_T = \prod_{j=1}^m c_{T_j}.$$

Determinante, Traço e Cálculo de c_T e m_T

Sejam $c_k \in \mathbb{F}$, $1 \leq k \leq n$, tais que

$$c_T(t) = t^n + \sum_{k=1}^n (-1)^k c_k t^{n-k}$$

e defina $\det(T) = c_n$ e $\text{tr}(T) = c_1$.

Veremos que $\det(T) = \det([T]_\alpha^\alpha)$ para toda base α de V e

$$(*) \quad c_T(t) = \det([T]_\alpha^\alpha - tI).$$

Ganhamos assim um novo método para encontrar m_T :

1. Calcule c_T via (*) e encontre seus fatores irredutíveis, digamos p_1, \dots, p_m . Seja n_j a multiplicidade de p_j na fatoração de c_T .
2. Seja $A = [T]_\alpha^\alpha$ e, dado $\mathbf{k} = (k_1, \dots, k_m) \in (\mathbb{Z}_{>0})^m$ com $k_j \leq n_j$, seja $p_{\mathbf{k}} = \prod_{j=1}^m p_j^{k_j}$. Entre todos os polinômios da forma $p_{\mathbf{k}}$ t.q. $p_{\mathbf{k}}(A) = 0$, aquele que tiver mínimo k_j para todo j é m_T . Para calcular cada k_j mínimo, pode-se calcular a sequência de núcleos $V_{p_j} \subseteq V_{p_j^2} \subseteq \dots \subseteq V_{p_j^{n_j}} = V_{p_j^{n_j+1}}$.