A DECOMPOSIÇÃO PRIMÁRIA

DANIEL V. TAUSK

Ao longo de todo o texto, K denota um corpo e $K[X]$ denota o anel de polinômios com coeficientes em K. Recordamos que, dados polinômios $p_1(X), \ldots, p_k(X) \in K[X]$ não todos nulos, então o *máximo divisor comum* desses polinômios, denotado por $\mathrm{mdc}\big(p_1(X), \ldots, p_k(X)\big)$, é o único polinômio mônico $p(X) \in K[X]$ satisfazendo as seguintes condições:

(a) $p(X)$ é um divisor comum de $p_1(X)$, ..., $p_k(X)$, isto é:
$$p(X)|p_i(X), \quad i = 1, \ldots, k;$$
(b) se $\tilde{p}(X) \in K[X]$ é um divisor comum de $p_1(X)$, ..., $p_k(X)$, então $\tilde{p}(X)|p(X)$.

Vale o *Teorema de Bezout*: dados $p_1(X), \ldots, p_k(X) \in K[X]$ não todos nulos, então existem $q_1(X), \ldots, q_k(X) \in K[X]$ tais que:
$$\mathrm{mdc}\big(p_1(X), \ldots, p_k(X)\big) = q_1(X)p_1(X) + \cdots + q_k(X)p_k(X).$$

A existência do máximo divisor comum, bem como o Teorema de Bezout, são conseqüências simples do fato que todo ideal de $K[X]$ é principal (i.e., gerado por um único elemento): de fato, basta verificar que o (único) gerador mônico do ideal gerado por $p_1(X)$, ..., $p_k(X)$ é o (único) máximo divisor comum de $p_1(X)$, ..., $p_k(X)$. O fato de que todo ideal de $K[X]$ é principal é, por sua vez, conseqüência simples do algorítmo de divisão de Euclides: dado um ideal não nulo de $K[X]$, tomamos um elemento não nulo dentro desse ideal com grau mínimo e, usando o algorítmo de divisão, mostramos que todos os elementos do ideal são múltiplos desse elemento de grau mínimo.

O seguinte resultado é um corolário simples do Teorema de Bezout.

Proposição 1. *Sejam $p(X), q_1(X), q_2(X) \in K[X]$ e suponha que:*
$$\mathrm{mdc}\big(p(X), q_1(X)\big) = 1.$$
Se $p(X)$ divide $q_1(X)q_2(X)$, então $p(X)$ divide $q_2(X)$.

Demonstração. Pelo Teorema de Bezout, existem $r(X), s(X) \in K[X]$ tais que:
$$r(X)p(X) + s(X)q_1(X) = 1;$$
multiplicando ambos os lados da igualdade por $q_2(X)$, obtemos:
$$r(X)p(X)q_2(X) + s(X)q_1(X)q_2(X) = q_2(X).$$
Do fato que $p(X)$ divide $r(X)p(X)q_2(X)$ e $s(X)q_1(X)q_2(X)$ segue a conclusão. □

Date: 12 de junho de 2014.

Definição 2. Dizemos que um polinômio $p(X) \in K[X]$ é *irredutível* (em $K[X]$) se $\text{grau}\big(p(X)\big) \geq 1$ e se dados $p_1(X)$ e $p_2(X)$ em $K[X]$ tais que:

$$p(X) = p_1(X)p_2(X),$$

então $\text{grau}\big(p_1(X)\big) = 0$ ou $\text{grau}\big(p_2(X)\big) = 0$. Em outras palavras, um polinômio $p(X) \in K[X]$ é irredutível se tiver grau maior ou igual a 1 e se seus únicos divisores forem os polinômios de grau zero e os polinômios da forma $c\,p(X)$, com $c \in K \setminus \{0\}$.

Evidentemente, todo polinômio de grau 1 é irredutível. Além do mais, é fácil provar por indução no grau que todo polinômio de grau maior ou igual a 1 se escreve como um produto finito de polinômios irredutíveis. Se o polinômio é mônico, esses fatores irredutíveis podem ser escolhidos mônicos também.

Exercício 3. Sejam $p(X)$ e $q(X)$ em $K[X]$ com $p(X)$ irredutível. Mostre que se $p(X)$ não divide $q(X)$, então $\text{mdc}\big(p(X), q(X)\big) = 1$.

O seguinte resultado é corolário imediato da Proposição 1 e do resultado do Exercício 3.

Corolário 4. *Sejam $p(X), q_1(X), q_2(X) \in K[X]$. Se $p(X)$ é irredutível e $p(X)$ divide $q_1(X)q_2(X)$, então ou $p(X)$ divide $q_1(X)$, ou $p(X)$ divide $q_2(X)$. Mais geralmente, se $p(X) \in K[X]$ é irredutível e divide um produto $q_1(X) \cdots q_n(X)$, com $q_i(X) \in K[X]$, $i = 1, \ldots, n$, então $p(X)$ divide $q_i(X)$, para algum $i = 1, \ldots, n$.* □

Definição 5. Sejam $p(X) \in K[X]$ um polinômio irredutível e $q(X) \in K[X]$ um polinômio não nulo. A *multiplicidade* do fator irredutível $p(X)$ em $q(X)$ é o maior inteiro $k \geq 0$ tal que $p(X)^k$ divide $q(X)$. (Convencionamos que $p(X)^0 = 1$.)

Obviamente, esse maior inteiro existe, já que se $p(X)^k$ divide $q(X)$, então $k\,\text{grau}\big(p(X)\big) \leq \text{grau}\big(q(X)\big)$. Além do mais, a multiplicidade do fator irredutível $p(X)$ em $q(X)$ é não nula se e somente se $p(X)$ divide $q(X)$.

É uma conseqüência simples do algorítmo de divisão de Euclides que $a \in K$ é raiz de um polinômio $q(X) \in K[X]$ se e somente se $X - a$ divide $q(X)$. A *multiplicidade* de $a \in K$ como raiz de um polinômio não nulo $q(X) \in K[X]$ é, por definição, a multiplicidade do fator irredutível $X - a$ em $q(X)$. Essa multiplicidade é não nula se e somente se a é de fato uma raiz de $q(X)$.

Exercício 6. Sejam $p(X) \in K[X]$ um polinômio irredutível, $q(X) \in K[X]$ um polinômio não nulo e $k \geq 0$ um inteiro. Mostre que a multiplicidade do fator irredutível $p(X)$ em $q(X)$ é k se e somente se existe $r(X) \in K[X]$ tal que $q(X) = p(X)^k r(X)$ e tal que $p(X)$ não divide $r(X)$.

Exercício 7. Seja $q(X) \in K[X]$ um polinômio mônico e escreva:

$$q(X) = p_1(X)^{n_1} \cdots p_k(X)^{n_k},$$

onde $p_1(X), \ldots p_k(X) \in K[X]$ são polinômios mônicos irredutíveis distintos e $n_1, \ldots, n_k$ são inteiros positivos. Dado um polinômio irredutível mônico $p(X) \in K[X]$, mostre que:

(a) $p(X) \in \{p_1(X), \ldots, p_k(X)\}$ se e somente se $p(X)|q(X)$;
(b) se $p(X) = p_i(X)$, para algum $i = 1, \ldots, k$, então a multiplicidade do fator irredutível $p(X)$ em $q(X)$ é exatamente o expoente n_i.

(Sugestão para os itens (a) e (b): use o Corolário 4.) A partir dos resultados dos itens (a) e (b), conclua que vale a unicidade (a menos da ordem) da fatoração de $q(X)$ como produto de polinômios mônicos irredutíveis distintos. Mais precisamente, mostre que se escrevemos $q(X)$ na forma:

$$q(X) = q_1(X)^{m_1} \cdots q_l(X)^{m_l},$$

com $q_1(X), \ldots, q_l(X) \in K[X]$ polinômios mônicos irredutíveis distintos e $m_1, \ldots, m_l$ inteiros positivos, então vale que:

(c) $\{p_1(X), \ldots, p_k(X)\} = \{q_1(X), \ldots, q_l(X)\}$ (em particular $k = l$);
(d) se $p_i(X) = q_j(X)$, com $1 \leq i \leq k$, $1 \leq j \leq l$, então os expoentes n_i e m_j são iguais.

Lema 8. *Sejam $k \geq 1$ um inteiro e $f_1(X), \ldots, f_k(X) \in K[X]$ polinômios tais que:*

$$\mathrm{mdc}\big(f_i(X), f_j(X)\big) = 1,$$

para todos $i, j = 1, \ldots, k$ com $i \neq j$. Para cada $i = 1, \ldots, k$, defina:

$$F_i(X) = \prod_{\substack{j=1 \\ j \neq i}}^{k} f_j(X) \in K[X].$$

Vale então que $\mathrm{mdc}\big(F_1(X), \ldots, F_k(X)\big) = 1$.

Demonstração. Como todo polinômio de grau maior ou igual a 1 tem um divisor irredutível, é suficiente mostrar que $F_1(X), \ldots, F_k(X)$ não possuem um divisor irredutível comum. Suponha por absurdo que exista um polinômio irredutível $p(X) \in K[X]$ que seja divisor comum dos polinômios $F_1(X), \ldots, F_k(X)$. Como $p(X)$ divide $F_1(X)$, pelo Corolário 4, $p(X)$ divide $f_i(X)$, para algum $i = 2, \ldots, k$. Mas $p(X)$ também divide $F_i(X)$ e, novamente pelo Corolário 4, segue que $p(X)$ divide $f_j(X)$, para algum $j = 1, \ldots, k$, com $j \neq i$. Isso contradiz o fato que $\mathrm{mdc}\big(f_i(X), f_j(X)\big) = 1$. □

No que segue, V denota sempre um espaço vetorial sobre K, não necessariamente de dimensão finita. Vamos agora demonstrar o resultado principal deste texto.

Proposição 9. *Sejam $T : V \to V$ um operador linear, $k \geq 0$ um inteiro e $f_1(X), \ldots, f_k(X) \in K[X]$ polinômios tais que:*

$$\operatorname{mdc}\big(f_i(X), f_j(X)\big) = 1,$$

para todos $i, j = 1, \ldots, k$ com $i \neq j$. Seja $f(X) = \prod_{i=1}^{k} f_i(X)$. Vale que:

(a) *a soma dos espaços $\operatorname{Ker}\big(f_i(T)\big)$, $i = 1, \ldots, k$, é direta;*

(b) *se $f(T) = 0$, então:*

$$V = \bigoplus_{i=1}^{k} \operatorname{Ker}\big(f_i(T)\big)$$

e os operadores de projeção correspondentes à essa decomposição em soma direta de V são polinômios em T.

Demonstração. Defina $F_i(X) \in K[X]$, $i = 1, \ldots, k$, como no enunciado do Lema 8. Pelo Lema 8 e pelo Teorema de Bezout, existem polinômios $g_1(X), \ldots, g_k(X) \in K[X]$ tais que:

$$g_1(X)F_1(X) + \cdots + g_k(X)F_k(X) = 1.$$

Daí:

$$g_1(T) \circ F_1(T) + \cdots + g_k(T) \circ F_k(T) = \mathrm{I}, \tag{1}$$

onde I denota o operador identidade de V. Sejam dados $x_i \in \operatorname{Ker}\big(f_i(T)\big)$, $i = 1, \ldots, k$, tais que:

$$x_1 + \cdots + x_k = 0. \tag{2}$$

Devemos mostrar que $x_i = 0$, para todo $i = 1, \ldots, k$. Obviamente, vale que

$$F_i(T)(x_j) = 0, \tag{3}$$

para $i, j = 1, \ldots, k$ com $i \neq j$, já que $f_j(T)(x_j) = 0$ e o operador linear $F_i(T)$ é igual à composição de um operador linear com $f_j(T)$. Avaliando os dois lados de (1) em x_i e usando (3), obtemos:

$$\big(g_i(T) \circ F_i(T)\big)(x_i) = x_i, \tag{4}$$

para todo $i = 1, \ldots, k$. Agora, aplicando $F_i(T)$ aos dois lados de (2) e usando novamente (3), vem:

$$F_i(T)(x_i) = 0, \tag{5}$$

e de (4) e (5) obtemos que $x_i = 0$, para todo $i = 1, \ldots, k$. Isso conclui a demonstração do item (a). Assuma agora que $f(T) = 0$. Nesse caso:

$$f_i(T) \circ g_i(T) \circ F_i(T) = g_i(T) \circ f(T) = 0,$$

de modo que, para todo $x \in V$, temos:

$$\big(g_i(T) \circ F_i(T)\big)(x) \in \operatorname{Ker}\big(f_i(T)\big), \tag{6}$$

para todo $i = 1, \ldots, k$. Usando (1) vem:

$$x = \big(g_1(T) \circ F_1(T)\big)(x) + \cdots + \big(g_k(T) \circ F_k(T)\big)(x), \tag{7}$$

para todo $x \in V$. De (6) e (7) segue que $V = \bigoplus_{i=1}^{k} \operatorname{Ker}\big(f_i(T)\big)$. Segue também que o i-ésimo operador de projeção correspondente a essa decomposição em soma direta de V é $g_i(T) \circ F_i(T) = (g_i F_i)(T)$. Isso completa a demonstração. □

Seja $T : V \to V$ um operador linear. Recorde que, se existe um polinômio não nulo $p(X) \in K[X]$ tal que $p(T) = 0$, então o *polinômio minimal* de T, denotado por $m_T(X)$, é o único gerador mônico do ideal não nulo formado pelos polinômios $p(X) \in K[X]$ tais que $p(T) = 0$. A existência de um polinômio não nulo $p(X) \in K[X]$ tal que $p(T) = 0$ é garantida, por exemplo, se V tem dimensão finita, já que nesse caso a seqüência infinita $(T^m)_{m \geq 0}$ formada pelas potências de T é necessariamente linearmente dependente no espaço vetorial dos operadores lineares em V.

Corolário 10 (decomposição primária)**.** *Seja $T : V \to V$ um operador linear. Assuma que T admita um polinômio minimal $m_T(X)$ e escreva:*

$$m_T(X) = p_1(X)^{n_1} \cdots p_k(X)^{n_k},$$

onde os polinômios $p_1(X), \ldots, p_k(X) \in K[X]$ são mônicos, irredutíveis e distintos e $n_1, \ldots, n_k$ são inteiros positivos. Vale que:

$$V = \bigoplus_{i=1}^{k} \operatorname{Ker}\big(p_i(T)^{n_i}\big).$$

Além do mais, os operadores de projeção correspondentes à essa decomposição em soma direta de V são polinômios em T.

Demonstração. Basta aplicar a Proposição 9 definindo $f_i(X) = p_i(X)^{n_i}$, para todo $i = 1, \ldots, k$. □

Corolário 11. *Assuma que* $\dim(V) < +\infty$. *Seja $T : V \to V$ um operador linear. Temos que T é diagonalizável se e somente se o seu polinômio minimal é um produto de polinômios mônicos de grau* 1 *distintos.*

Demonstração. Suponha que T seja diagonalizável e seja $\mathcal{B}$ uma base de V tal que a matriz $[T]_{\mathcal{B}}$ seja diagonal. Sejam $\lambda_1, \ldots, \lambda_k \in K$ os elementos distintos da diagonal de $[T]_{\mathcal{B}}$. Dado um polinômio $p(X) \in K[X]$, temos:

$$[p(T)]_{\mathcal{B}} = p\big([T]_{\mathcal{B}}\big);$$

segue que $p(T) = 0$ se e somente se $p(\lambda_1) = \cdots = p(\lambda_k) = 0$, isto é, se e somente se:

$$(X - \lambda_1) \cdots (X - \lambda_k) | p(X).$$

Daí o polinômio minimal de T é $(X - \lambda_1) \cdots (X - \lambda_k)$. Reciprocamente, supondo que $m_T(X) = (X - \lambda_1) \cdots (X - \lambda_k)$, com $\lambda_1, \ldots, \lambda_k \in K$ distintos,

então o Corolário 10 nos dá:

$$V = \bigoplus_{i=1}^{k} \mathrm{Ker}(T - \lambda_i \mathrm{I}).$$

Daí, se $\mathcal{B}_i$ é uma base de $\mathrm{Ker}(T - \lambda_i \mathrm{I})$, então $\mathcal{B} = \bigcup_{i=1}^{k} \mathcal{B}_i$ é uma base de V e $[T]_{\mathcal{B}}$ é diagonal. □

No que segue, se $T : V \to V$ é um operador linear e W é um subespaço T-invariante de V, então $T|_W$ denota o operador linear $T|_W : W \to W$ com domínio e contra-domínio iguais a W.

Exercício 12. Sejam $T : V \to V$ um operador linear e W um subespaço T-invariante de V. Mostre que se T admite um polinômio minimal, então $T|_W$ também admite um polinômio minimal e:

$$m_{(T|_W)}(X) | m_T(X).$$

Usando o Corolário 11, conclua que se $\dim(V) < +\infty$ e T é diagonalizável, então também $T|_W$ é diagonalizável.

No que segue, convencionamos que se $T : V \to V$ é um operador linear, então T^0 é o operador identidade de V.

Exercício 13. Seja $T : V \to V$ um operador linear. Dado um inteiro $k \geq 0$, mostre que $\mathrm{Ker}(T^k) \subset \mathrm{Ker}(T^{k+1})$ e que, se $\mathrm{Ker}(T^k) = \mathrm{Ker}(T^{k+1})$, então $\mathrm{Ker}(T^k) = \mathrm{Ker}(T^l)$, para todo $l \geq k$.

Exercício 14. Seja $T : V \to V$ um operador linear e sejam dados polinômios $p(X), q(X) \in K[X]$ tais que $p(T) = 0$ e $\mathrm{mdc}\big(p(X), q(X)\big) = 1$. Mostre que $q(T)$ é um isomorfismo. (Sugestão: use o Teorema de Bezout.)

Proposição 15. *Seja $T : V \to V$ um operador linear que admite um polinômio minimal $m_T(X)$. Sejam $p(X) \in K[X]$ um polinômio irredutível e $k \geq 0$ a multiplicidade do fator irredutível $p(X)$ em $m_T(X)$. Vale que:*

$$\mathrm{Ker}\big(p(T)^k\big) = \mathrm{Ker}\big(p(T)^{k+1}\big), \tag{8}$$

e, se $k \geq 1$, então:

$$\mathrm{Ker}\big(p(T)^{k-1}\big) \neq \mathrm{Ker}\big(p(T)^k\big). \tag{9}$$

Demonstração. Escreva $m_T(X) = p(X)^k q(X)$, com $q(X) \in K[X]$ tal que $p(X)$ não divide $q(X)$ (Exercício 6). Como $p(X)$ é irredutível e $p(X)$ não divide $q(X)$, segue que $\mathrm{mdc}\big(p(X), q(X)\big) = 1$ (Exercício 3). Pelo Teorema de Bezout, existem $r(X), s(X) \in K[X]$ tais que:

$$r(X)p(X) + s(X)q(X) = 1.$$

Multiplicando ambos os lados por $p(X)^k$ e avaliando em T, obtemos:

$$r(T) \circ p(T)^{k+1} + s(T) \circ p(T)^k \circ q(T) = p(T)^k.$$

Como $p(T)^k \circ q(T) = 0$, concluímos que:

$$r(T) \circ p(T)^{k+1} = p(T)^k,$$

donde segue que $\mathrm{Ker}\big(p(T)^{k+1}\big) \subset \mathrm{Ker}\big(p(T)^k\big)$. Isso prova (8). Suponha agora que $k \geq 1$. Como $p(X)^{k-1}q(X)$ é um polinômio não nulo com grau menor do que o grau de $m_T(X)$, temos $p(T)^{k-1} \circ q(T) \neq 0$; segue daí que existem elementos na imagem de $q(T)$ que não estão em $\mathrm{Ker}\big(p(T)^{k-1}\big)$. Como $p(T)^k \circ q(T) = 0$, temos que a imagem de $q(T)$ está contida em $\mathrm{Ker}\big(p(T)^k\big)$. Isso completa a demonstração de (9). □

Definição 16. Sejam $T : V \to V$ um operador linear e $\lambda \in K$. O λ-*autoespaço generalizado* de T é o subespaço de V definido por:

$$\bigcup_{k=0}^{\infty} \mathrm{Ker}(T - \lambda \mathrm{I})^k.$$

Obviamente, se $\lambda \in K$ não é um autovalor de T então $T - \lambda\mathrm{I}$ é injetor e portanto o λ-autoespaço generalizado de T é nulo.

Corolário 17. *Seja $T : V \to V$ um operador linear que admite um polinômio minimal $m_T(X)$ e seja $\lambda \in K$. Se $k \geq 0$ é a multiplicidade de λ como raiz de $m_T(X)$, então o λ-autoespaço generalizado de T é* $\mathrm{Ker}(T - \lambda\mathrm{I})^k$.

Demonstração. Como k é a multiplicidade do fator irredutível $X - \lambda$ em $m_T(X)$, a conclusão segue diretamente da Proposição 15 e do resultado do Exercício 13. □

Exercício 18. Seja $T : V \to V$ um operador linear que admite um polinômio minimal $m_T(X)$. Sejam $p(X) \in K[X]$ um polinômio irredutível e $k \geq 0$ a multiplicidade do fator irredutível $p(X)$ em $m_T(X)$. Se

$$W = \mathrm{Ker}\big(p(T)^k\big),$$

mostre que o polinômio minimal de $T|_W$ é precisamente $p(X)^k$. (Sugestão: use a Proposição 15.)

Exercício 19. Seja $T : V \to V$ um operador linear que admite um polinômio minimal $m_T(X)$. Seja $p(X) \in K[X]$ um polinômio irredutível. Mostre que são equivalentes:

(a) $p(X)$ não divide $m_T(X)$;
(b) $p(T)$ é um isomorfismo;
(c) $p(T)$ é injetor;
(d) $p(T)$ é sobrejetor.

(Sugestão: para mostrar que (a) implica (b), use o resultado do Exercício 14. Para mostrar que (c) implica (a) e que (d) implica (a), note que se escrevemos $m_T(X) = p(X)q(X)$, então $p(T) \circ q(T) = q(T) \circ p(T) = 0$ e $q(T) \neq 0$.)

Exercício 20. Seja $T : V \to V$ um operador linear que admite um polinômio minimal $m_T(X)$. Mostre que $\lambda \in K$ é raiz de $m_T(X)$ se e somente se λ é um autovalor de T. (Sugestão: use o resultado do Exercício 19.)

Corolário 21. *Seja $T : V \to V$ um operador linear que admite um polinômio minimal $m_T(X)$. Se $m_T(X)$ é um produto de polinômios de grau 1 (não necessariamente distintos), então V é a soma direta dos autoespaços generalizados de T.*

Demonstração. Escreva:

$$m_T(X) = (X - \lambda_1)^{n_1} \cdots (X - \lambda_k)^{n_k},$$

com $\lambda_1, \ldots, \lambda_k \in K$ distintos e $n_1, \ldots, n_k$ inteiros positivos. Pelo resultado do Exercício 20, $\lambda_1, \ldots, \lambda_k$ são precisamente os autovalores de T e segue do Corolário 17 que os autoespaços generalizados correspondentes a esses autovalores são $\mathrm{Ker}(T - \lambda_i \mathrm{I})^{n_i}$, $i = 1, \ldots, k$. A conclusão segue do Corolário 10. □

Observação 22. A hipótese de que $m_T(X)$ é um produto de polinômios de grau 1 é válida, por exemplo, se o corpo K for *algebricamente fechado*, isto é, se todo polinômio não constante com coeficientes em K possui raiz em K. Este é o caso, por exemplo, do corpo dos números complexos.