O Teorema da Decomposição Primária

Marcones de Oliveira Silva marcones.silva@ifsertao-pe.edu.br
Instituto Federal do Sertão Pernambucano - IFSertãoPE, Santa Maria da Boa Vista, PE, Brasil

Thiago Amaral Melo Lima thiago.amaral@ifsertao-pe.edu.br
Instituto Federal do Sertão Pernambucano - IFSertãoPE, Salgueiro, PE, Brasil

Deivid Santos de Almeida deivid.almeida@arapiraca.ufal.br
Universidade Federal de Alagoas - UFAL, Arapiraca, AL, Brasil

Resumo

O objetivo deste trabalho é apresentar de uma forma detalhada o Teorema da Decomposição Primária. Esse teorema é um dos resultados mais importantes da álgebra linear, pois afirma que qualquer espaço vetorial de dimensão finita é a soma direta dos espaços característicos associados aos seus respectivos valores característicos. Tal resultado tem inúmeras consequências, especialmente no estudo dos espaços soluções das equacões diferenciais ordinárias. A demonstração do Teorema da Decomposição Primária será feita utilizando, principalmente, os conceitos de subespacos invariantes, polinômio mínimo e projeção além de outros resultados que nos ajudarão no encadeamento lógico da demonstração. Existe uma versão desse teorema chamada de Teorema Espectral que é utilizada quando se está trabalhando com espaços vetoriais complexos. Não utilizaremos tal denominação no desenvolvimento do presente trabalho, pois o corpo K referido ao longo do texto pode ser tanto real como complexo.

Palavras-chave

Teorema da Decomposição Primária, Espaço Vetorial, Dimensão, Espaços Característicos, Valores Característicos.

1 Introdução

O Teorema da Decomposição Primária é um dos mais importantes da álgebra linear e afirma que qualquer espaço vetorial de dimensão finita é a soma direta dos espaços característicos associados ao respectivos valores característicos. Tal teorema tem inúmeras consequências, especialmente no estudo dos espaços soluções das equações diferenciais ordinárias. A demonstraçao envolve, principalmente, os conceitos de subespaço invariante, polinômio mínimo e projeção. Geralmente, em um primeiro curso de álgebra linear são estudados os conceitos de espaço vetorial, base, dimensão e transformação linear deixando o Teorema da Decomposição Primária só para os alunos que fazem o famoso curso de álgebra linear 2 nas universidades federais brasileiras. Porém, mesmo para os alunos que fazem um segundo curso de álgebra linear algumas demonstrações de teoremas não ficam muito claras porque alguns passos são omitidos pelos autores do livro texto, dificultando assim o aprendizado da matéria.

Portanto, o principal objetivo deste trabalho é demonstrar detalhadamente e sem qualquer omissão de alguma etapa, o Teorema da Decomposição Primária de modo que até um aluno que não cursou álgebra linear 2 consiga entender a demonstração sem maiores problemas, obviamente já tendo estudado o curso de álgebra linear 1.

2 Preliminares

Nesta seção abordaremos a definição de polinômio em uma variável x com coeficientes em um corpo K qualquer e suas várias consequências.

2.1 Polinômios

Seja K um corpo e S o conjunto dos inteiros não-negativos. O conjunto de todas as funções de S em K é um espaço vetorial sobre K. Indicaremos este espaço vetorial por K^∞. Os vetores em K^∞ são, portanto, seguências infinitas $f = (f_0, f_1, f_2, ...)$ de escalares f_i em K. Se $g = (g_0, g_1, g_2, ...)$ com g_i em K e a, b são escalares em K, $af + bg$ é a sequência dada por

$$ag + bg = (af_0 + bg_0, af_1 + bg_1, af_2 + bg_2, ...).$$

Definimos um produto em K^∞ associando a cada par de vetores $f, g \in K^\infty$ o vetor fg que é dado por

$$(fg)_n = \sum_{i=0}^{n} f_i g_{n-i}, n = 0, 1, 2, ...$$

Potanto, $fg = (f_0g_0, f_0g_1 + f_1g_0, f_0g_2 + f_1g_1 + f_2g_0, ...)$.

Definição 2.1. *Seja $K[x]$ o subespaço de K^∞ gerado pelos vetores $1, x, x^2, ...$ Um elemento de $K[x]$ é dito um* **polinômio sobre** K.

Como $K[x]$ consiste de todas as combinações lineares (finitas) de x e suas potências, um vetor não-nulo f em K^∞ é um polinômio se, e somente se, existe um inteiro $n \geq 0$ tal que $f_n \neq 0$ e tal que $f_k = 0$ para todos os inteiros $k > n$. Este inteiro é denominado o **grau de f**. Indicamos o grau de um polinômio por ∂f e não atribuímos nenhum grau ao polinômio nulo. Se f é um polinômio não-nulo de grau n temos que $f = f_0x^0 + f_1x + ... + f_nx^n, f_n \neq 0$.

Os escalares $f_0, f_1, f_2, ..., f_n$ são chamados os **coeficientes** de f e podemos dizer que f é um polinômio com coeficientes em K. Denominaremos os polinômios da forma cx^0 de **polinômios constantes** e os indicaremos por c. Um polinômio não-nulo f de grau n tal que $f_n = 1$ é dito um polinômio **unitário ou mônico**.

Identificamos 1 com a sequência $(1, 0, 0, ..., 0, ...)$ e de um modo geral, $a \in K$ com a sequência $(a, 0, 0, ..., 0, ...)$.

Representamos a sequência $(0, 1, 0, ..., 0, ...)$ por x de modo que:

$x^2 = x \cdot x = (0, 0, 1, 0, ..., 0, ...)$

$x^3 = x \cdot x^2 = (0, 0, 0, 1, 0, ..., 0, ...)$

$\vdots$

$x^n = x \cdot x^{n-1} = (0, 1, 0, ..., 0, ...) \cdot (\underbrace{0, 0, 0, ..., 1}_{n-posicao}, 0, ...) = (\underbrace{0, 0, 0, ..., 1}_{n+1-posicao}, 0, ...).$

Dessa forma, para qualquer polinômio $(a_0, a_1, ..., a_m, ...)$ temos: $(a_0, a_1, ..., a_m, ...) = (a_0, 0, 0, ..., 0, ...) + (0, a_1, 0, ..., 0, ...) + (0, 0, a_2, 0, ..., 0, ...) + ... + (0, 0, 0, ..., a_m, 0, ...) + ... = a_0(1, 0, 0, ..., 0, ...) + a_1(0, 1, 0, ..., 0, ...) + a_2(0, 0, 1, 0, ..., 0, ...) + ... + a_m(0, 0, 0, ..., 1, 0, ...) = a_0 + a_1x + a_2x^2 + ... + a_mx^m + ...$

Definimos, a seguir, o ideal de polinômios.

Definição 2.2. *Seja K um corpo. Um* **ideal** *em $K[x]$ é um subespaço M de $K[x]$ tal que $fg \in M$ sempre que $f \in K[x]$ e $g \in M$.*

Exemplo 2.3. Dado $d \in K[x]$, o conjunto $M = dK[x]$ de todos os múltiplos polinomiais de d é um ideal. De fato, M é não-vazio, pois contém d e se $f, g \in K[x]$ e $\alpha, \beta \in K$, então

$$\begin{aligned} \alpha(df) + \beta(dg) &= d(\alpha f + \beta g) \\ f(dg) &= d(fg) \end{aligned}$$

M é chamado o **ideal principal gerado por** d.

Teorema 2.4. *Se M é um ideal de $K[x]$, então existe um único polinômio mônico d em $K[x]$ tal que M é o ideal principal gerado por d.*

Demonstração:

Por hipótese, M contém um polinômio não-nulo. Dentre todos os polinômios não-nulos de M existe um polinômio d de grau mínimo, que podemos assumir mônico, multiplicando d pelo escalar apropriado, se necessário. Agora, se $f \in M$, então $f = dq + r$ com $r = 0$ ou $\partial r < \partial d$. Como $d \in M$, $dq \in M$ e $f - dq = r \in M$ também. Por escolha de d (não existe polinômio não-nulo em M de grau menor que d), concluímos que $r = 0$. Portanto, $M = dK[x]$.

Se $d^{'}$ fosse outro polinômio mônico em $K[x]$ tal que $M = d^{'}K[x]$, então existiriam polinômios não-nulos f, g tais que $d = d^{'}f$ e $d^{'} = dg$. Logo, $d = dgf$ e daí $\partial d =$

$\partial d + \partial f + \partial g$ donde $\partial f = \partial g = 0$. Como f, g são mônicos, segue que $f = g = 1$ e portanto, $d = d^{'}$.

Teorema 2.5. *(***Existência de M.D.C***) Sejam $p_1(x), ..., p_m(x) \in K[x] - \{0\}$ e seja o ideal $J = K[x] \cdot p_1(x) + ... + K[x] \cdot p_m(x)$ de $K[x]$ gerado pelos polinômios não-nulos $p_1(x), ..., p_m(x)$.*

Se $d(x) \in K[x]$ é tal que $J = K[x] \cdot d(x)$ então são válidas as seguintes propriedades:

(i) $\exists r_1(x), ..., r_m(x) \in K[x]$ tais que $d(x) = r_1(x) \cdot p_1(x) + ... + r_m(x) \cdot p_m(x)$;

(ii) $d(x)$ é um divisor comum de $p_1(x), p_2(x), ..., p_m(x)$;

(iii) Se $d^{'}(x)$ é um divisor comum qualquer de $p_1(x), p_2(x), ..., p_m(x)$. Então, $d^{'}(x)$ é também um divisor de $d(x)$.

Um polinômio satisfazendo as condições (ii) e (iii) chama-se um Máximo Divisor Comum (M.D.C.) de $p_1(x), p_2(x), ..., p_m(x)$.

Demonstração:

(i) Temos que:

$$J = K[x]p_1(x) + K[x]P_2(x) + ... + K[x]p_m(x) = K[x]d(x).$$

Assim,
$d(x) \in K[x]d(x) \Rightarrow d(x) \in K[x]p_1(x) + K[x]P_2(x) + ... + K[x]p_m(x) \Rightarrow$
$\Rightarrow \exists r_1(x), r_2(x), ..., r_m(x) \in K[x]$ tal que $d(x) = r_1(x)p_1(x) + r_2(x)p_2(x) + ... + r_m(x)p_m(x)$.

(ii) Temos $p_i(x) \in J = K[x]d(x) \Rightarrow p_i(x) = q_i d(x) \Rightarrow d(x)|p_i(x)$.

(iii) Seja $d^{'}(x)$ um divisor comum de $p_1(x), p_2(x), ..., p_m(x)$, então, substituindo as expressões $p_1(x) = q_1(x)d^{'}(x), p_2(x) = q_2(x)d^{'}(x), ..., p_m(x) = q_m(x)d^{'}(x)$ na expressão $d(x) = r_1(x) \cdot p_1(x) + ... + r_m(x) \cdot p_m(x)$ temos:

$d(x) = r_1(x)q_1(x)d^{'}(x) + r_2(x)q_2(x)d^{'}(x) + ... + r_m(x)q_m(x)d^{'}(x) = (r_1(x)q_1(x) + r_2(x)q_2(x) + ... + r_m(x)q_m(x))d^{'}(x) = q(x)d^{'}(x)$.

Se $p_1(x), ..., p_m(x) \in K[x] - \{0\}$, então existe um único M.D.C. mônico de $p_1(x), ..., p_m(x)$ em $K[x]$. Neste caso, dizemos o M.D.C. de $p_1(x), ..., p_m(x)$ em $K[x]$ o qual denotamos por M.D.C $\{p_1(x), ..., p_m(x)\}$ de acordo com [2].

Se M.D.C $\{p_1(x), ..., p_m(x)\}$= 1 dizemos que os polinômios são **relativamente primos em K[x]**. Nesse caso, $\exists r_1(x), ..., r_m(x) \in K[x]$ tais que $r_1(x)p_1(x) + ... + r_m(x)p_m(x) = 1$.

Definição 2.6. *Seja K um corpo. Diz-se que um polinômio f em $K[x]$ é* **redutível sobre** K *se existem polinômios g, h em $K[x]$ de grau ≥ 1 tais que $f = gh$ e, em caso contrário, diz-se que f é* **irredutível sobre K**. *Um polinômio não-constante irredutível sobre K é denominado um* **polinômio primo sobre K** *e dizemos, às vezes, que é um* **primo** *em $K[x]$.*

Teorema 2.7. *Seja f um polinômio não-constante e unitário sobre o corpo K e seja $f = p_1^{n_1} \cdot ... \cdot p_k^{n_k}$ a decomposição em fatores primos. Para cada i, $1 \leq i \leq k$, seja $f_i = \dfrac{f}{p_i^{n_i}} = \prod_{i \neq j} p_j^{r_j}$.*

Então, $f_1, ..., f_k$ são relativamente primos.

Demonstração:

Temos que:

$f_1 = p_2^{n_2} \cdot ... \cdot p_k^{n_k}$

$f_2 = p_1^{n_1} \cdot p_3^{n_3} \cdot ... \cdot p_k^{n_k}$

$f_3 = p_1^{n_1} \cdot p_2^{n_2} \cdot p_4^{n_4} \cdot ... \cdot p_k^{n_k}$

$\vdots$

$f_k = p_1^{n_1} \cdot p_2^{n_2} \cdot ... \cdot p_{k-1}^{n_{k-1}}$

Não existe um fator em comum nas decomposições dos polinômios $f_1, f_2, ..., f_k$. Logo, o M.D.C.$\{f_1, f_2, ..., f_k\}$= 1 e portanto, $f_1, f_2, ..., f_k$ são relativamente primos.

Definição 2.8. *O corpo K é dito* **algebricamente fechado** *se todo polinômio primo sobre K tem grau 1.*

Dizer que K é algebricamente fechado significa que todo polinômio não-constantte irredutível sobre K é da forma $x-c$. Dessa forma, pode-se dar uma definição equivalente de um corpo algebricamente fechado como um corpo K tal que todo polinômio não-constante f em $K[x]$ possa ser expresso na forma

$$f = c(x - c_1)^{n_1} \cdot ... \cdot (x - c_k)^{n_k}$$

onde c é um escalar, $c_1, ..., c_k$ são elementos distintos de K e $n_1, ..., n_k$ são inteiros positivos.

O corpo R dos números reais não é algebricamente fechado porque o polinômio $x^2 + 1$ é irredutível sobre R, mas não tem grau 1, ou porque não existe um número real c tal que $c^2 + 1 = 0$. O chamado **Teorema Fundamental da Álgebra** afirma que o corpo C dos números complexos é algebricamente fechado. A demonstração de tal teorema pode ser encontrada em [1].

3 Resultados Principais

A demonstração do Teorema da Decomposição Primária necessita dos conceitos de polinômio mínimo e projeção. Por isso, é muito importante estudar todos os teoremas relacionados a esses dois conceitos.

3.1 Polinômio Característico

Definição 3.1. *Seja V um espaço vetorial sobre o corpo K e seja T um operador linear sobre V. Um* **valor característico** *de T é um escalar c em K tal que exista um vetor não-nulo α em V com $T\alpha = c\alpha$. Se c é um valor característico de T, então*

(a) Todo $\alpha \in V$ tal que $T\alpha = c\alpha$ é chamado **vetor característico de T associado ao valor característico** *c;*

(b) A coleção de todos os α tais que $T\alpha = c\alpha$ é denominado **espaço característico associado a** *c.*

Vamos definir agora o **polinômio característico de um operador T**.

Definição 3.2. *Seja T um operador linear sobre um espaço vetorial V de dimensão finita e B uma base de V. O polinômio $p(t) = det([T]_B - tI) = a_0 + a_1t + a_2t^2 + ... + a_nt^n$ é chamado o* **polinômio característico de T***, onde $[T]_B$ é a matriz que representa o operador T na base B e I é a matriz identidade.*

Definição 3.3. *Seja T um operador linear sobre o espaço V de dimensão finita. Dizemos que T é diagonalizável se existe uma base de V formada por vetores característicos de T.*

Teorema 3.4. *Se w_i for um vetor característico de um operador linear sobre V associado ao valor característico $c_i \in K$, e se $c_i \neq c_j$ para $i \neq j$, então o conjunto $\{w_1, w_2, ..., w_k\}$ é linearmente independente.*

Demonstração:

Faremos indução no número k de elementos do conjunto $\{w_1, w_2, ..., w_k\}$. Se $k = 1$, o resultado é verdadeiro. Suponhamos verdadeiro para $k - 1$ vetores e consideremos o caso de k vetores. Então,

$$(*) \qquad \alpha_1 w_1 + \alpha_2 w_2 + ... + \alpha_k w_k = \overrightarrow{0}$$

Aplicando T em $(*)$, obtemos:

$$\alpha_1 T w_1 + \alpha_2 T w_2 + ... + \alpha_k T w_k = \overrightarrow{0}.$$

Mas, $Tw_i = c_i w_i$. Assim,

$$\alpha_1 c_1 w_1 + \alpha_2 c_2 w_2 + ... + \alpha_k c_k w_k = \overrightarrow{0}.$$

Por outro lado, multiplicando $(*)$ por c_k, vem:

$$\alpha_1 c_k w_1 + \alpha_2 c_k w_2 + ... + \alpha_k c_k w_k = \overrightarrow{0}.$$

Subtraindo as duas últimas equações, concluímos que,

$$\alpha_1(c_1 - c_k)w_1 + \alpha_2(c_2 - c_k)w_2 + ... + \alpha_{k-1}(c_{k-1} - c_k)w_{k-1} = \overrightarrow{0}.$$

Como $c_i - c_k \neq 0$ para todo $i = 1, ..., k-1$, a hipótese de indução garante que $\alpha_i = 0$ para $i \in \{1, ..., k-1\}$. Então, como $\alpha_1 w_1 + \alpha_2 w_2 + ... + \alpha_k w_k = \overrightarrow{0}$, concluímos que $\alpha_k = 0$ e que $\{w_1, w_2, ..., w_k\}$ é linearmente independente.

Corolário 3.5. *Seja V um espaço vetorial de dimensão n. Se o operador linear T sobre V possui n valores característicos distintos, então ele é diagonalizável.*

Demonstração:

Sejam $c_1, c_2, ..., c_n$ os n valores característicos de T e $w_1, ..., w_n$ vetores característicos respectivamente correspondentes. Segue do resultado anterior que $\{w_1, ..., w_n\}$ é um subconjunto linearmente independente de V, logo é uma base de V.

3.2 Polinômios Anuladores

Ao tentarmos analisar um operador linear T, é de grande utilidade conhecermos a classe dos polinômios que anulam T. Suponhamos que T seja um operador linear sobre V onde V é um espaço vetorial sobre o corpo K. Se p for um polinômio sobre K, então $p(T)$ será novamente um operador linear sobre V. Então,

$$\begin{aligned} (p+q)(T) &= p(T) + q(T) \\ (pq)(T) &= p(T)q(T). \end{aligned}$$

Portanto, a coleção de polinômios p que anulam T, no sentido de que $p(T) = 0$ é um ideal de polinômios em $K[x]$. De acordo com o *Teorema* 2.4, todo ideal de polinômios consiste de todos os múltiplos de algum polinômio unitário fixo, o gerador do ideal. Portanto, podemos associar ao operador T um polinômio unitário p com essa propriedade: se f é um polinômio sobre K, então $f(T) = 0$ se, e somente se, $f = pg$, onde g é algum polinômio sobre K.

Definição 3.6. *Seja T um operador linear sobre um espaço vetorial V de dimensão finita sobre o corpo K. O* **polinômio mínimo** *de T é o gerador mônico de menor grau do ideal dos polinômios que anulam T.*

Lema 3.7. *Suponhamos que $T\alpha = c\alpha$. Se f é um polinômio arbitrário, então $f(T)\alpha = f(c)\alpha$*

Demonstração:

Primeiramente, mostraremos que se $T\alpha = c\alpha$, então $T^n\alpha = c^n\alpha$, $\forall n \geq 2$ e $n \in N$.

A prova será feita por indução sobre n.

Note que se $n = 2$, então,

$$T^2\alpha = T(T\alpha) = T(c\alpha) = c(T\alpha) = c^2\alpha.$$

Suponha o resultado válido para $n-1$, então, $T^{n-1}\alpha = c^{n-1}\alpha \Rightarrow T(T^{n-1}\alpha) = T^n\alpha = c^{n-1}T\alpha = c^{n-1}(c\alpha) = c^n\alpha$.

Logo, $T^n\alpha = c^n\alpha$.

Seja $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ um polinômio de grau n. Então, $f(T) = a_0I + a_1T + a_2T^2 + ... + a_nT^n \Rightarrow f(T)\alpha = a_0\alpha + a_1T\alpha + a_2T^2\alpha + ... + a_nT^n\alpha = a_0\alpha + a_1(c\alpha) + a_2(c^2\alpha) + ... + a_n(c^n\alpha) = (a_0\alpha + a_1c + a_2c^2 + ... + a_nc^n)\alpha = f(c)\alpha$.

Logo, $f(T)\alpha = f(c)\alpha$.

Em outras palavras, o teorema afirma que o valor característico do operador linear $f(T)$ é $f(c)$.

Teorema 3.8. *Seja T um operador linear sobre o espaço vetorial $n-$dimensional V. Os polinômios característico e mínimo de T possuem as mesmas raízes, a menos de multiplicidades.*

Demonstração:

Seja p o polinômio mínimo de T. Seja c um escalar. Queremos mostrar que $p(c) = 0$ se, e somente se, c é um valor característico de T.

Primeiramente, suponhamos $p(c) = 0$. Então, $p = (x-c)q$ onde q é um polinômio. Como $\partial q < \partial p$, a definição de polinômio mínimo p nos diz que $q(T) \neq 0$. Escolhamos um vetor β tal que $q(T)\beta \neq 0$. Seja $\alpha = q(T)\beta$, então $0 = p(T)\beta = (T-cI)q(T)\beta = (T-cI)\alpha$ e assim, c é um valor característico de T.

Suponhamos, agora, que c seja um valor característico de T, digamos, $T\alpha = c\alpha$

com $\alpha \neq 0$. Como observamos no lema anterior, $p(T)\alpha = p(c)\alpha$, então como $p(T) = 0$ e $\alpha \neq 0$, temos que $p(c) = 0$.

O teorema a seguir diz que o polinômio mínimo divide o polinômio característico. A demonstração pode ser encontrada em [3].

Teorema 3.9. *(* **Cayley - Hamilton***) Seja T um operador linear sobre um espaço vetorial V de dimensão finita. Se f é o polinômio caracaterístico de T, então $f(T) = 0$; em outras palavras, o polinômio mínimo divide o polinômio característico de T.*

Definição 3.10. *Seja V um espaço vetorial e T um operador linear sobre V. Se W é um subespaço de V, dizemos que W é* **invariante sob T** *se para cada vetor α em W, o vetor $T\alpha$ está em W, isto é, se $T(W)$ está contido em W.*

Quando o subespaço W é invariante sob T, então T induz um operador linear T_w sobre o espaço W. O operador linear T_w é definido por $T_w\alpha = T(\alpha)$, para α em W, mas T_w é bem diferente de T uma vez que seu domínio é W e não V.

3.3 Teoremas e Lemas

Nesta subseção $dimV$ e $KerT$ denotarão a dimensão de um espaço vetorial V de dimensão finita e o núcleo de um operador linear T, respectivamente.

Lema 3.11. *Seja T um operador linear sobre o espaço V de dimensão finita. Sejam $c_1, c_2, ..., c_k$ valores característicos de T e seja W_i o espaço dos vetores caracerísticos associado ao valor característico c_i. Se $W = W_1 + ... + W_k$, então $dimW = dimW_1 + ... + dimW_k$.*

Mais ainda, se B_i é uma base ordenada de W_i, então, $B = (B_1, ..., B_k)$ é uma base ordenada de W.

Demonstração:

Normalmente, quando formamos a soma W de subespaços W_i, esperamos que $dimW < (dimW_1 + ... + dimW_k)$ por causa das relações lineares que possam existir entre os vetores nos diversos espaços. Esse lema afirma que os espaços característicos associados a valores característicos distintos, são independentes um do outro.

Suponhamos que (para cada i) β_i seja um vetor em W_i e que $\beta_1 + ... + \beta_k = \overrightarrow{0}$. Mostraremos que $\beta_i = \overrightarrow{0}$ para cada i. Seja f um polinômio arbitrário. Como $T\beta_i = c_i\beta_i$, o Lema 3.7 nos diz que

$$0 = f(T)\overrightarrow{0} = f(T)(\beta_1+...+\beta_k) = f(T)\beta_1+...+f(T)\beta_k = f(c_1)\beta_1+...+f(c_k)\beta_k.$$

Escolhamos polinômios $f_1, ..., f_k$ tais que

$$f_i(c_j) = \delta_{ij} = \begin{cases} 1 & , \quad i = j \\ 0 & , \quad i \neq j. \end{cases}$$

Então, $\overrightarrow{0} = f_i(T)\overrightarrow{0} = \sum_j \delta_{ij}\beta_j = \beta_i$.

Seja, agora, B_i uma base ordenada de W_i e seja B a sequência $B = (B_1, ..., B_k)$. Então, B gera o subespaço $W = W_1 + ... + W_k$. Também, B é uma sequência de vetores linearmente independentes, pelo seguinte: Considere a relação linear entre os vetores de B da forma $\beta_1 + ... + \beta_k = \overrightarrow{0}$, onde β_i é alguma combinação linear dos vetores de B_i. Pelo que acabamos de ver, sabemos que $\beta_i = \overrightarrow{0}$ para cada i. Como cada B_i é linearmente independente, vemos que existe apenas a relação linear trivial entre os vetores em B.

Teorema 3.12. *Seja T um operador linear sobre um espaço vetorial V de dimensão finita. Sejam $c_1, ..., c_k$ valores característicos distintos de T e seja W_i o núcleo de $(T - c_iI)$. As seguintes afirmações são equivalentes:*

(i) T é diagonalizável;

(ii) O polinômio característico de T é $p(x) = (x - c_1)^{d_1} \cdot ... \cdot (x - c_k)^{d_k}$ e $dimW_i = d_i$, $i = 1, ..., k$;

(iii) $dimW_1 + ... + dimW_k = dimV$.

Demonstração:

((i) ⇒(ii)). Se T é diagonalizável, então T possui uma representação matricial em blocos na forma

$$[T] = \begin{bmatrix} c_1I_1 & 0 & 0 & \cdots & 0 \\ 0 & c_2I_2 & 0 & \cdots & 0 \\ 0 & 0 & c_3I_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & c_kI_k \end{bmatrix}$$

em relação a alguma base B de V onde I_j é a $d_j \times d_j$ matriz identidade.

A partir dessa matriz verificamos dois fatos. Primeiro, o polinômio característico de T é o produto de fatores lineares (possivelmente repetidos): $p(x) = (x - c_1)^{d_1} \cdot ... \cdot (x - c_k)^{d_k}$. O segundo fato que observamos a partir da matriz $[T]$ é de que d_i, o número de vezes que c_i é repetido como raiz de p, é igual à dimensão do espaço dos vetores característicos associado ao valor característico c_i. Isto acontece porque a nulidade da matriz é igual ao número de zeros que ela possui na sua diagonal principal, e a matriz $[T - c_iI]_B$ tem d_i zeros na sua diagonal principal.

((ii) ⇒(iii)). Se $p(x) = (x - c_1)^{d_1} \cdot ... \cdot (x - c_k)^{d_k}$ então $dimV = \partial p(x) = d_1 + d_2 + ... + d_k$.

((iii) ⇒(i)). Suponhamos (iii). Pelo lema anterior, devemos ter $V = W_1 + W_2 + ... + W_k$, então existe uma base formada por vetores característicos que gera V. Logo, T será diagonalizável.

Definição 3.13. *Sejam $W_1, ..., W_k$ subespaços do espaço vetorial V. Dizemos que $W_1, ..., W_k$ são independentes se $\alpha_1 + ... + \alpha_k = \overrightarrow{0}$, α_i em W_i, implica que cada α_i é nulo.*

O significado da independência é o seguinte: Seja $W = W_1 + ... + W_k$ o subespaço gerado por $W_1, ..., W_k$. Cada vetor α em W pode ser expresso com uma soma $\alpha = \alpha_1 + ... + \alpha_k$, α_i em W_i.

Se $W_1, ..., W_k$ forem independentes, então a expressão para α será única, pois, se $\alpha = \alpha_1 + ... + \alpha_k = \beta_1 + ... + \beta_k$, β_i em W_i, então $\overrightarrow{0} = (\alpha_1 - \beta_1) + ... + (\alpha_k - \beta_k)$, logo, $\alpha_i - \beta_i = \overrightarrow{0}$, $i = 1, ..., k$. Assim, quando $W_1, ..., W_k$ são independentes, podemos operar com os vetores de W como k-uplas $(\alpha_1, ..., \alpha_k)$, α_i em W_i, da mesma maneira como operamos com vetores em R^k com k-uplas de números.

Lema 3.14. *Seja V um espaço vetorial de dimensão finita. Sejam $W_1, ..., W_k$ subespaços de V e seja $W = W_1 + W_2 + ... + W_k$. As seguintes condições são equivalentes:*

(a) $W_1, ..., W_k$ são independentes;

(b) Para cada j, $2 \leq j \leq k$, temos $W_j \cap (W_1 + ... + W_{j-1}) = \overrightarrow{0}$;

(c) Se B_i é uma base ordenada de W_i, $1 \leq i \leq k$, então a sequência $B = (B_1, ..., B_k)$ é uma base ordenada de W.

Demonstração:

((a) ⇒ (b)). Seja α um vetor na interseção $W_j \cap (W_1 + ... + W_{j-1})$. Então, existem vetores $\alpha_1, ..., \alpha_{j-1}$, com α_i em W_i, tais que $\alpha = \alpha_1 + ... + \alpha_{j-1}$. Como $\alpha_1 + ... + \alpha_{j-1} + (-\alpha) + \overrightarrow{0} + ... + \overrightarrow{0} = \overrightarrow{0}$ e como $W_1, ..., W_k$ são independentes, então $\alpha_1 = \alpha_2 = ... = \alpha_{j-1} = \alpha = \overrightarrow{0}$.

((b) ⇒ (a)). Suponhamos $\alpha_1 + ... + \alpha_k = \overrightarrow{0}$ com α_i em W_i.

Seja j o maior inteiro i tal que $\alpha_i \neq 0$. Então, $\alpha_1 + ... + \alpha_j = \overrightarrow{0}$ com $\alpha_i \neq 0$. Logo, $\alpha_j = -\alpha_1 - ... - \alpha_{j-1}$ é um vetor não-nulo em $W_j \cap (W_1 + ... + W_{j-1})$. Vamos mostrar agora que (a) é equivalente a (c).

((a) ⇒ (c)). Seja B_i uma base de W_i, $1 \leq i \leq k$ e seja $B = (B_1, ..., B_k)$. Se $\beta_1 +$

$... + \beta_k = \overrightarrow{0}$ é uma relação linear entre os vetores de B onde β_i é alguma combinação linear dos vetores de B_i, então cada $\beta_i = \overrightarrow{0}$, pois $W_1, ..., W_k$ são independentes. Como cada B_i é independente, a única relação existente entre os vetores de B é a trivial.Temos também que B gera W, pois $W = W_1 + ... + W_k$.

((c) ⇒ (a)). Seja $W = W_1 + ... + W_k$ onde $B = (B_1, ..., B_k)$ é uma base de W e B_i é uma base de W_i.

Seja $\beta_1 + ... + \beta_k = \overrightarrow{0}$ uma relação linear entre os vetores de B onde β_i é alguma combinação linear dos vetores de B_i. Como $B = (B_1, ..., B_k)$ é uma base de W, então $\beta_i = 0$. Logo, $W_1, ..., W_k$ são independentes.

Se uma (e portanto todas) das três condições do lema acima é válida, diremos que a soma $W = W_1 + ... + W_k$ é **direta** ou que W é a **soma direta** de $W_1, ..., W_k$ e escreveremos $W = W_1 \bigoplus ... \bigoplus W_k$.

3.4 Projeções

Definição 3.15. *Se V é um espaço vetorial, uma projeção de V é um operador linear $E : V \to V$ tal que $E^2 = E$.*

Suponhamos que E seja uma projeção. Sejam $Im(E)$ a imagem de E e $Ker(E)$ o núcleo de E.

1 - O vetor β está na imagem $Im(E)$ se, e somente se, $E\beta = \beta$. Se $\beta = E\alpha$, então $E\beta = E^2\alpha = E\alpha = \beta$. Reciprocamente, se $\beta = E\beta$, então β está na imagem de E.

2 - $V = Im(E) \bigoplus Ker(E)$. Todo $\alpha \in V$ escreve-se como soma $\alpha = (\alpha - E\alpha) + E\alpha$, onde $E\alpha$, evidentemente, pertence a $Im(E)$ e, como $E(\alpha - E\alpha) = E\alpha - EE\alpha = E\alpha - E\alpha = \overrightarrow{0}$, vemos que $\alpha - E\alpha \in Ker(E)$. Portanto, $V = Im(E) + Ker(E)$. Se $\beta \in Im(E) \cap Ker(E)$, por um lado tem-se $E\beta = \overrightarrow{0}$ e, por outro lado, $E\beta = \beta$, logo $\beta = \overrightarrow{0}$. Assim, $Im(E) \cap Ker(E) = \overrightarrow{0}$ e tem-se a soma direta $V = Im(E) \bigoplus Ker(E)$.

3 - A única expressão de α como uma soma de vetores em $Im(E)$ e $Ker(E)$ é $\alpha = (\alpha - E\alpha) + E\alpha$.

4 - Se W e Z são subespaços de V tais que $V = W \bigoplus Z$, então cada vetor $v \in V$ se escreve de forma única como $v = w + z$ onde $w \in W$ e $z \in Z$, portanto, podemos definir um operador $E : W \bigoplus Z \to V$ por $E(w + z) = w$. Então, E é um operador linear bem definido e temos $E^2v = E(Ev) = Ew = w = Ev$. Se $W = Im(E)$ e $Z = Ker(E)$, então E é chamado **projeção sobre W segundo Z**.

Teorema 3.16. *Se $V = W_1 \bigoplus ... \bigoplus W_k$, então existem k operadores $E_1, ..., E_k$ sobre V tais que* *(i) cada E_i é uma projeção $E_i^2 = E_i$;*

(ii) $E_iE_j = \overrightarrow{0}$, se $i \neq j$;

(iii) $I = E_1 + ... + E_k$;

(iv) a imagem de E_i é W_i.

Reciprocamente, se $E_1, ..., E_k$ são k operadores lineares sobre V que satisfazem as condições (i),(ii) e (iii) e se indicamos por W_i a imagem de E_i, então $V = W_1 \bigoplus ... \bigoplus W_k$.

Demonstração:

($\Rightarrow$) Suponhamos $V = W_1 \bigoplus ... \bigoplus W_k$. Para cada j definiremos um operador E_j sobre V. Sejam α e β em V, digamos $\alpha = \alpha_1 + ... + \alpha_k$ e $\beta = \beta_1 + ... + \beta_k$ com α_i, β_i em W_i. Definamos $E_j\alpha = \alpha_j$. Então, E_j é uma regra bem definida. Temos que E_j é linear, pois $E_j(c\alpha + \beta) = c\alpha_j + \beta j = cE_j\alpha + E_j\beta$.

A imagem de E_j é W_j e $E_j^2 = E_j$, pois $E_j(E_j\alpha) = E_j\alpha_j = E_j\alpha$. O núcleo de E_j é o subespaço $(W_1 + ... + W_{j-1} + W_{j+1}) + ... + W_k$, pois a afirmação de que $E_j\alpha = \overrightarrow{0}$ significa que $\alpha_j = \overrightarrow{0}$, isto é, que α é na realidade uma soma de vetores dos espaços W_i com $i \neq j$. Em termos das projeções E_j temos $\alpha = E_1\alpha + ... + E_k\alpha$ para cada vetor α em V. Então, $I\alpha = (E_1 + ... + E_k)\alpha$ o que implica que $I = E_1 + ... + E_k$ onde I é o operador linear idêntico.

Notemos também que se $i \neq j$, então $E_iE_j = \overrightarrow{0}$, pois a imagem de E_j é o subespaço W_j que está contido no núcleo de E_i.

($\Leftarrow$)Suponhamos que $E_1, ..., E_k$ sejam operadores lineares sobre V que satisfaçam as três primeiras condições e seja W_i a imagem de E_i.

Temos que $V = W_1 + ... + W_k$, pois pela condição (iii) temos $\alpha = E_1\alpha + ... + E_k\alpha$ para cada α em V e $E_i\alpha$ está em W_i. Esta expressão para α é única, porque se $\alpha = \alpha_1 + ... + \alpha_k$ com α_i em W_i, digamos $\alpha_i = E_i\beta_i$, então, usando (i) e (ii), temos

$$E_j\alpha = \sum_{i=1}^{k} E_j\alpha_i = \sum_{i=1}^{k} E_jE_i\beta_i = E_j^2\beta_j = E_j\beta_j = \alpha_j.$$

Isto mostra que V é a soma direta dos W_i, ou seja, $V = W_1 \bigoplus ... \bigoplus W_k$.

Teorema 3.17. *Seja T um operador linear sobre um espaço V de dimensão finita n, onde $c_1, ..., c_k$ são valores característicos distintos de T. Então, os espaços característicos W_i associados aos valores característicos c_i são independentes.*

Demonstração:

Considere a equação:

$$(*) \qquad \alpha_1 + ... + \alpha_k = \overrightarrow{0}, \alpha_i \in W_i, i = 1, ..., k.$$

Precisamos mostrar que $\alpha_i = \overrightarrow{0}, \forall i \in \{1, ..., k\}$.

Para isso, defina o seguinte operador linear sobre V:

$$U_j = (T - c_1 I) \circ ... \circ (T - c_{j-1} I) \circ (T - c_{j+1}) \circ ... \circ (T - c_k I).$$

Mostraremos que:

(i) $U_j \alpha_i = \overrightarrow{0}$, para $i \neq j$.

Temos que $(T - c_i I)\alpha_i = T\alpha_i - c_i\alpha_i = c_i\alpha_i - c_i\alpha_i = \overrightarrow{0}$ onde os operadores $T - c_i I$ comutam.

Daí, segue-se que $U_j \alpha_i = \overrightarrow{0}, \forall i \neq j$.

(ii) $U_j \alpha_j = \prod_{i \neq j} (c_j - c_i)\alpha_j$.

Temos que $(T - c_k I)\alpha_j = T\alpha_j - c_k\alpha_j = c_j\alpha_j - c_k\alpha_j = (c_j - c_k)\alpha_j$.

Temos também que:

$(T - c_{k-1} I) \circ (T - c_k I)\alpha_j = (T - c_{k-1} I) \cdot ((c_j - c_k)\alpha_j) = (c_j - c_k) \cdot (T - c_{k-1} I)\alpha_j = (c_j - c_{k-1}) \cdot (c_j - c_k)\alpha_j$.

Logo, $U_j \alpha_j = \prod_{i \neq j} (c_j - c_i)\alpha_j$.

Aplicando U_j a ambos os membros da equação $(*)$:

$U_j(\alpha_1 + ... + \alpha_k) = U_j(\overrightarrow{0}) \Rightarrow U_j\alpha_j = \overrightarrow{0} \Rightarrow U_j\alpha_j = \prod_{i \neq j} (c_j - c_i)\alpha_j = \overrightarrow{0} \Rightarrow \alpha_j = \overrightarrow{0}$.

Como $j \in \{1, ..., k\}$ é arbitrário, concluímos $\alpha_1 = ... = \alpha_j = \overrightarrow{0}$.

Corolário 3.18. *Seja T um operador linear sobre um espaço V de dimensão finita n. Se T é diagonalizável com valores característicos distintos $c_1, ..., c_k$ então $V = W_1 \bigoplus ... \bigoplus W_k$ onde W_i é o espaço característico associado ao valor característico c_i.*

Demonstração:

Se T é diagonalizável, então existe uma base $B = \{\alpha_1, ..., \alpha_k\}$ formada por vetores característicos de T. Sabemos que $W_1 + ... + W_k \subseteq V$ e, pelo Teorema 3.12 , que $dimW_1 + ... + dimW_k = dimV$. Temos também que $W_1, ..., W_k$ são independentes pelo teorema anterior.

Portanto, $dim(W_1 \bigoplus ... \bigoplus W_k) = dimW_1 + ... + dimW_k = dimV$.

Logo, $W_1 \bigoplus ... \bigoplus W_k$ é um subespaço de V de dimensão n e assim $V = W_1 \bigoplus ... \bigoplus W_k$.

Teorema 3.19. *Seja T um operador linear sobre o espaço V e sejam $W_1, ..., W_k$ e $E_1, ..., E_k$ como no Teorema 3.16. Então, uma condição necessária e suficiente para que cada subespaço W_i seja invariante sob T é que T comute com cada uma das projeções E_i, isto é, $TE_i = E_iT$, $i = 1, ..., k$.*

Demonstração:

Suponhamos que T comute com cada E_i. Seja α em W_j. Então $E_j\alpha = \alpha$ e $T\alpha = T(E_j\alpha) = E_j(T\alpha)$ o que mostra que $T\alpha$ está na imagem de E_j, isto é, que W_j é invariante sob T.

Suponhamos agora que cada W_i seja invariante sob T. Mostraremos que $TE_j = E_jT$. Seja α um vetor arbitrário em V. Então,

$$\begin{aligned} \alpha &= E_1\alpha + ... + E_k\alpha \\ T\alpha &= TE_1\alpha + ... + TE_k\alpha \end{aligned}$$

Como $E_i\alpha$ está em W_i, que é invariante sob T, devemos ter $T(E_i\alpha) = E_i\beta_i$ para algum vetor β_i. Então,

$$E_jTE_i\alpha = E_jE_i\beta_i = \begin{cases} 0 & , \quad i \neq j \\ E_j\beta_j & , \quad i = j. \end{cases}$$

Assim, $E_jT\alpha = E_jTE_1\alpha + ... + E_jTE_k\alpha = E_j\beta_j = TE_j\alpha$. Isso vale para todo α em V, portanto, $E_jT = TE_j$.

Teorema 3.20. *Seja T um operador linear sobre um espaço V de dimensão finita. Se T é diagonalizável e $c_1, ..., c_k$ são os valores característicos distintos de T, então existem operadores lineares $E_1, ..., E_k$ sobre V tais que*

(i) $T = c_1E_1 + ... + c_kE_k$;

(ii) $I = E_1 + ... + E_k$;

(iii)$E_iE_j = \overrightarrow{0}$, se $i \neq j$;

(iv) $E_i^2 = E_i$; (E_i é projeção)

(v) A imagem de E_i é o espaço característico de T associado a c_i.

Reciprocamente, se existirem k escalares distintos $c_1, ..., c_k$ e k operadores lineares não-nulos $E_1, ..., E_k$ satisfazendo as condições (i),(ii) e (iii), então T é diagonalizável, $c_1, ..., c_k$ são os valores característicos distintos de T e as condições (iv) e (v) também são satisfeitas.

Demonstração:

($\Rightarrow$) Suponhamos que T seja diagonalizável, com valores característicos distintos $c_1, ..., c_k$. Seja W_i o espaço dos vetores característicos associado ao valor característico c_i, Então pelo Teorema 3.17 e seu colorário $V = W_1 \bigoplus ... \bigoplus W_k$. Seja $E_1, ..., E_k$ as projeções associadas a esta decomposição como no Teorema 3.16. Então, (ii),(iii),(iv) e (v) são satisfeitas. Para verificar (i) procedemos da seguinte maneira: para cada α em V, temos $\alpha = E_1\alpha + ... + E_k\alpha$. Portanto,

$$T\alpha = TE_1\alpha + ... + TE_k\alpha = c_1E_1\alpha + ... + c_kE_k\alpha.$$

Logo, $T = c_1E_1 + ... + c_kE_k$.

($\Leftarrow$) (a) $E_i^2 = E_i$. Sabemos que $I = E_1 + ... + E_k$, então

$$\begin{aligned} E_iI &= E_i(E_1 + ... + E_k) \\ E_i &= E_iE_i = E_i^2 \end{aligned}$$

(b) Cada c_i é um valor característico de T. Basta mostrar que $TE_i = c_iE_i$.

Por hipótese,

$$\begin{aligned} T &= c_1E_1 + ... + c_kE_k \\ TE_i &= (c_1E_1 + ... + c_kE_k)E_i \\ TE_i &= c_iE_iE_i = c_iE_i^2 = c_iE_i. \end{aligned}$$

(c) T é diagonalizável. Temos que $I = E_1 + ... + E_k$. Seja $\alpha \in V \Rightarrow I\alpha = \alpha = E_1\alpha + ... + E_k\alpha$ onde cada $E_i\alpha \in Im(E_i)$.

Portanto, $V = Im(E_1) + ... + Im(E_k)$ onde $TE_i\alpha = c_iE_i\alpha$.

Logo, $E_i\alpha$ é um vetor característico de T associado a c_i onde $Im(E_i) \subseteq W_i$.

Considere $B = (B_1, ..., B_k)$ onde B_i é uma base de $Im(E_i)$. Então, B é uma base de V constituída de vetores característicos, porque $Im(E_i) \subseteq W_i$. Logo, T é diagonalizável.

Já demonstramos no item (c) que $Im(E_i) \subseteq W_i$. Vamos provar agora que $W_i \subseteq Im(E_i)$.

Seja $\alpha \in W_i$, então $(T - c_iI)\alpha = T\alpha - c_i\alpha = (c_1E_1\alpha + ... + c_kE_k\alpha) - (c_iE_1\alpha + ... + c_iE_k\alpha) = (c_1 - c_i)E_1\alpha + ... + (c_k - c_i)E_k\alpha = \sum_{j=1}^{k}(c_j - c_i)E_j\alpha = \overrightarrow{0}$.

Logo, $(c_j - c_i)E_j\alpha = \overrightarrow{0}$ para cada j, então $E_j\alpha = \overrightarrow{0}$, $j \neq i$.

Como $\alpha = E_1\alpha + ... + E_k\alpha$ e $E_j\alpha = \overrightarrow{0}$ para $j \neq i$, temos que $\alpha = E_i\alpha$,demonstrando que α está na imagem de E_i.

Logo, $W_i = Im(E_i)$.

4 Resultados e Discussão

Vamos a partir de agora iniciar a demonstração do Teorema da Decomposição Primária. Tudo que foi feito até agora teve como objetivo oferecer os subsídios necessários para que a demonstração aqui exposta tivesse o melhor embasamento teórico possível.

Teorema 4.1. *(***Teorema da Decomposição Primária***) Seja T um operador linear sobre o espaço vetorial V de dimensão finita sobre o corpo K. Seja p o polinômio mínimo de T. Suponha que p se fatore da seguinte forma:*

$$p = p_1^{r_1} \cdot ... \cdot p_k^{r_k}$$

onde p_i são polinômios mônicos irredutíveis e os r_i são inteiros positivos. Então:

(a) $V = W_1 \bigoplus ... \bigoplus W_k$, onde $W_i = Ker(p_i(T)^{r_i}), i = 1, ..., k$;

(b) Cada W_i é invariante sob T;

(c) Se T_i é o operador induzido sobre W_i por T, então o polinômio mínimo de T_i é $p_i^{r_i}$.

Demonstração:

Defina $f_i = \dfrac{p}{p_i^{r_i}} = p_1^{r_1} \cdot ... \cdot p_{i-1}^{r_{i-1}} \cdot p_{i+1}^{r_{i+1}} \cdot ... \cdot p_k^{r_k} = \prod_{i \neq j} p_j^{r_j}$. Os polinômios $f_1, ..., f_k$ são primos entre si.

Logo, existem polinômios $g_1, ..., g_k$ tais que:

$$f_1g_1 + ... + f_kg_k = 1 \Rightarrow f_1(T)g_1(T) + ... + f_k(T)g_k(T) = I$$

Defina $E_i = f_i(T)g_i(T)$. De $f_1(T)g_1(T) + ... + fk(T)g_k(T) = I$ obtemos

$E_1 + ... + E_k = I$. Afirmamos que $E_iE_j = \overrightarrow{0}$, se $i \neq j$. Para ver isso, observe que $\exists q \in K[x]$ tal que $f_if_j = qp$, onde p é o polinômio mínimo.

Logo, $f_i(T)f_j(T) = q(T)p(T) = \overrightarrow{0}$.

Note agora que: $E_iE_j = f_i(T)g_i(T)f_j(T)g_j(T) = f_i(T)f_j(T)g_i(T)g_j(T) = \overrightarrow{0}$, pois $f_i(T)f_j(T) = \overrightarrow{0}$.

Afirmamos que $E_i^2 = E_i, \forall i = 1, ..., k$.

De fato, sabemos que $E_1 + ... + E_k = I \Rightarrow E_i \cdot (E_1 + ... + E_k = E_iI) \Rightarrow E_iE_i = E_i \Rightarrow E_i^2 = E_i, i = 1, ..., k$.

Seja $\alpha \in V \Rightarrow \alpha = E_1\alpha + ... + E_k\alpha \Rightarrow V = Im(E_1) \bigoplus ... \bigoplus Im(E_k)$ de acordo com o *Teorema* 2.24.

Mostraremos que $ImE_i = Ker(p_i(T)^{r_i})$.

(i) $Im(E_i) \subseteq Ker(p_i(T)^{r_i})$.

Considere $\alpha \in Im(E_i)$, portanto, $E_i\alpha = \alpha$. Então, $p_i(T)^{r_i}\alpha = p_i(T)^{r_i}(E_i(\alpha)) = p_i(T)^{r_i}(f_i(T)g_i(T)(\alpha)) = \overrightarrow{0}$, pois $p_i(T)^{r_i}f_i(T) = p(T) = \overrightarrow{0}$.

(ii) $Ker(p_i(T)^{r_i}) \subseteq Im(E_i)$.

Considere $\alpha \in Ker(p_i(T)^{r_i}$. Afirmamos que $E_j\alpha = \overrightarrow{0}$ se $j \neq i$, pois $\alpha \in Ker(p_i(T)^{r_i})$.

De fato, $E_j\alpha = f_j(T)g_j(T)(\alpha) = q(T)p_i(T)^{r_i}(\alpha) = \overrightarrow{0}$. Note que $f_jg_j = qp_i^{r_i}$.

Mas, $I = E_1 + ... + E_k$, então, $\alpha = I(\alpha) = E_1\alpha + ... + E_i\alpha + ... + E_k\alpha \Rightarrow\Rightarrow \alpha = E_i\alpha$.

Portanto, por (i) e (ii) temos que $Im(E_i) = Ker(p_i(T)^{r_i})$.

Logo, $V = W_1 \bigoplus ... \bigoplus W_k$ onde $W_i = Ker(p_i(T)^{r_i}), i = 1, ..., k$.

(b) Seja $\alpha \in W_i$, então $p_i(T)^{r_i}\alpha = \overrightarrow{0} \Rightarrow p_i(T)^{r_i}T\alpha = Tp_i(T)^{r_i}\alpha = \overrightarrow{0} \Rightarrow T\alpha \in Ker(p_i(T)^{r_i}) = W_i$.

Logo, os W_i são invariantes sob T.

(c) Temos que $W_i = Ker(p_i(T)^{r_i})$, então,

$p_i(T)^{r_i}\alpha = \overrightarrow{0}, \forall\alpha \in W_i \Rightarrow p_i(T_i)^{r_i}\alpha = \overrightarrow{0}$.

Falta mostrar que $p_i^{r_i}$ é o polinômio mínimo de T_i.

Considere $g \in K[x]$ tal que $g(T_i) = \overrightarrow{0}$. Precisamos mostrar que $p_i^{r_i}$ divide g.

Observe que:

$g(T_i)f_i(T_i) = \overrightarrow{0} \Rightarrow g(T_i)f_i(T_i)(\alpha) = \overrightarrow{0}, \forall\alpha \in W_i$.

Portanto, gf_i é divisível pelo polinômio mínimo p de T.

Logo, $gf_i = qp, q \in K[x]$. Então,

$gf_i = qp = qf_ip_i^{r_i} \Rightarrow (g - qp_i^{r_i})f_i = \overrightarrow{0} \Rightarrow g = qp_i^{r_i} \Rightarrow p_i^{r_i}|g.$

5 Conclusão

A demonstração do Teorema da Decomposição Primária foi realizada utilizando, principalmente, os conceitos de subespaço invariante, projeção e polinômio mínimo que é o polinômio mônico de menor grau gerador do ideal dos polinômios que anulam o operador linear T sobre o espaço vetorial V de dimensão finita sobre o corpo K. A demonstração não é dificil de entender desde que todas as definições e teoremas que auxiliam no seu encadeamento lógico estejam claros para o leitor, por isso que é preciso esclarecer todos os pontos importantes antes de qualquer demonstração matemática, caso contrário, restarão lacunas que dificilmente um leitor em contato pela primeira vez com qualquer teorema complexo consegue superar.

Referências

[1] COSTA, A. I. S. *Uma demonstração do Teorema Fundamental da Álgebra*. 2016. 76 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal de São Carlos, São Carlos, 2016.

[2] GONÇALVES, A. *Introdução à Álgebra*. 6. ed. Rio de Janeiro: SBM, 2017.

[3] HOFFMAN, K.; KUNZE, R. *Álgebra Linear*. Trad. WATANABE, R. 2. ed. Rio de Janeiro: LTC, 1979.