Álgebra Linear
Douglas Smigly

MAT5730

2^{o} semestre de 2019

Conteúdo

Informações da Disciplina

Informações Básicas

Essas são as notas de aula de Álgebra Linear(MAT5730), as aulas acontecem na sala B-134 às terças 10h e às quintas 8h.

Informações do Professor

O professor é o Ivan Shestakov, sua sala é a 290-A e o seu e-mail é shestak@ime.usp.br

Bibliografia

[1] Flávio Coelho and Mary Lilian Lourenço. *Um Curso de Álgebra Linear*. Edusp, 2001.

[2] Werner H. Greub. *Multilinear Algebra*. Springer, 1978.

[3] Werner H. Greub. *Linear Algebra*. Springer, 1981.

[4] Kenneth Hoffman and Ray Kunze. *Linear Algebra*. Prentice Hall, 1971.

[5] Steven Roman. *Advanced Linear Algebra*. Springer, 2005.

Avaliação

A nota final da disciplina será a média aritimética de P1, P2, e P3. Todos os alunos poderão fazer a prova sub para substituir a menor das suas notas (Sub aberta). As datas das provas são as seguintes:

Prova	**Data**
P1	10-09
P2	15-10
P3	12-11
SUB	19-11

Outras Informações

(i) Teremos listas, que não contarão para a nota

(ii) As listas serão publicadas em

(iii) Não haverá monitoria

Capítulo 1

Espaços vetoriais

1.1 Definições Iniciais

Definição 1.1. Um **grupo abeliano** é um conjunto X munido do seguinte:

- $+ : \mathrm{X} \times \mathrm{X} \to \mathrm{X}$,
- $0 \in \mathrm{X}$,
- $- : \mathrm{X} \to \mathrm{X}$,

satisfazendo as seguintes propriedades:

- Para $\mathrm{x}, \mathrm{y}, \mathrm{z} \in \mathrm{X}$ então $(\mathrm{x} + \mathrm{y}) + \mathrm{z} = \mathrm{x} + (\mathrm{y} + \mathrm{z})$,
- Para $\mathrm{x}, \mathrm{y} \in \mathrm{X}$ então $\mathrm{x} + \mathrm{y} = \mathrm{y} + \mathrm{x}$,
- Para $\mathrm{x} \in \mathrm{X}$ então $\mathrm{x} + 0 = \mathrm{x}$,
- Para $\mathrm{x} \in \mathrm{X}$ então $\mathrm{x} + (-\mathrm{x}) = 0$.

Definição 1.2. Um **corpo** é um grupo abeliano $(\mathrm{K}, +, 0, -)$ munido do seguinte:

- $\cdot : \mathrm{K} \times \mathrm{K} \to \mathrm{K}$,
- $1 \in \mathrm{K}$,
- $\cdot^{-1} : \mathrm{K} \setminus \{0\} \to \mathrm{K}$,

satisfazendo as seguintes propriedades:

- Para $\mathrm{x}, \mathrm{y}, \mathrm{z} \in \mathrm{K}$ então $(\mathrm{x} \cdot \mathrm{y}) \cdot \mathrm{z} = \mathrm{x} \cdot (\mathrm{y} \cdot \mathrm{z})$,
- Para $\mathrm{x}, \mathrm{y} \in \mathrm{K}$ então $\mathrm{x} \cdot \mathrm{y} = \mathrm{y} \cdot \mathrm{x}$,
- Para $\mathrm{x} \in \mathrm{K}$ então $\mathrm{x} \cdot 1 = \mathrm{x}$,
- Para $\mathrm{x} \in \mathrm{K} \setminus \{0\}$ então $\mathrm{x} \cdot \mathrm{x}^{-1} = 1$,
- Para $\mathrm{x}, \mathrm{y}, \mathrm{z} \in \mathrm{K}$ então $\mathrm{x} \cdot (\mathrm{y} + \mathrm{z}) = (\mathrm{x} \cdot \mathrm{y}) + (\mathrm{x} \cdot \mathrm{z})$.

Definição 1.3. Dado K um corpo, um **espaço vetorial sobre** K é um grupo abeliano $(\mathrm{V}, +, 0, -)$ munido do seguinte:

- $\cdot : \mathrm{K} \times \mathrm{V} \to \mathrm{V}$,

satisfazendo as seguintes propriedades:

- Para $\mathrm{a}, \mathrm{b} \in \mathrm{K}$ e $\mathrm{x} \in \mathrm{V}$ então $(\mathrm{a} \cdot \mathrm{b}) \cdot \mathrm{x} = \mathrm{a} \cdot (\mathrm{b} \cdot \mathrm{x})$,
- Para $\mathrm{x} \in \mathrm{V}$ então $\mathrm{x} \cdot 1 = \mathrm{x}$,
- Para $\mathrm{a} \in \mathrm{K}$ e $\mathrm{x}, \mathrm{y} \in \mathrm{V}$ então $\mathrm{a} \cdot (\mathrm{x} + \mathrm{y}) = (\mathrm{a} \cdot \mathrm{x}) + (\mathrm{a} \cdot \mathrm{y})$,
- Para $\mathrm{a}, \mathrm{b} \in \mathrm{K}$ e $\mathrm{x} \in \mathrm{V}$ então $(\mathrm{a} + \mathrm{b}) \cdot \mathrm{x} = (\mathrm{a} \cdot \mathrm{x}) + (\mathrm{b} \cdot \mathrm{x})$.

1.2 Base e Dimensão

Durante o restante deste capítulo, sempre adotaremos K como sendo um corpo qualquer.

Definição 1.4. Seja V um espaço vetorial sobre um corpo K. Seja I um conjunto e $\mathrm{v} : \mathrm{I} \to \mathrm{V}$ uma função. Uma **combinação linear** de v é um elemento $\mathrm{u} \in \mathrm{V}$ tal que existam um conjunto finito $\mathrm{J} \subseteq \mathrm{I}$ e uma função $\alpha : \mathrm{J} \to \mathrm{K}$ tais que:

$$\mathrm{u} = \sum_{\mathrm{i} \in \mathrm{J}} \alpha_{\mathrm{i}} \mathrm{v}_{\mathrm{i}}.$$

Dizemos que v **gera** V se e só se todo elemento de V é combinação linear de v.

Definição 1.5. Seja V um espaço vetorial sobre um corpo K. Dizemos que um conjunto $\mathrm{S} \subseteq \mathrm{V}$ **gera** V se e só se a função $\mathrm{v} : \mathrm{S} \to \mathrm{V}$ dada por $\forall \mathrm{s} \in \mathrm{S} : \mathrm{v}_{\mathrm{s}} = \mathrm{s}$ gera V.

Proposição 1.6. Seja V um espaço vetorial sobre um corpo K e sejam I um conjunto e $\mathrm{v} : \mathrm{I} \to \mathrm{V}$ uma função. Então v gera V se e somente se a imagem $\mathrm{S} = \{\mathrm{v}_{\mathrm{i}} : \mathrm{i} \in \mathrm{I}\}$ gera V.

Demonstração. Temos o seguinte:

- Se v gera V, então para $\mathrm{x} \in \mathrm{V}$ existem um conjunto finito $\mathrm{J} \subseteq \mathrm{I}$ e uma função $\alpha : \mathrm{J} \to \mathrm{K}$ tais que:

  $$\mathrm{x} = \sum_{\mathrm{i} \in \mathrm{J}} \alpha_{\mathrm{i}} \mathrm{v}_{\mathrm{i}},$$

  aí seja $\mathrm{T} = \mathrm{v}[\mathrm{J}]$, e seja:

  $$\forall \mathrm{s} \in \mathrm{T} : \mathrm{J}_{\mathrm{s}} = \{\mathrm{i} \in \mathrm{J} : \mathrm{v}_{\mathrm{i}} = \mathrm{s}\};$$

  e seja $\beta : \mathrm{T} \to \mathrm{K}$ a função dada por:

  $$\forall \mathrm{s} \in \mathrm{T} : \beta_{\mathrm{s}} = \sum_{\mathrm{i} \in \mathrm{J}_{\mathrm{s}}} \alpha_{\mathrm{i}},$$

  então T é finito, aí temos:

  $$\mathrm{x} = \sum_{\mathrm{i} \in \mathrm{J}} \alpha_{\mathrm{i}} \mathrm{v}_{\mathrm{i}} = \sum_{\mathrm{s} \in \mathrm{T}} \sum_{\mathrm{i} \in \mathrm{J}_{\mathrm{s}}} \alpha_{\mathrm{i}} \mathrm{v}_{\mathrm{i}} = \sum_{\mathrm{s} \in \mathrm{T}} \sum_{\mathrm{i} \in \mathrm{J}_{\mathrm{s}}} \alpha_{\mathrm{i}} \mathrm{s} = \sum_{\mathrm{s} \in \mathrm{T}} \beta_{\mathrm{s}} \mathrm{s};$$

  logo S gera V.

- Se S gera V, então para $\mathrm{x} \in \mathrm{V}$ existem um conjunto finito $\mathrm{T} \subseteq \mathrm{S}$ e uma função $\beta : \mathrm{T} \to \mathrm{K}$ tais que:

  $$\mathrm{x} = \sum_{\mathrm{s} \in \mathrm{T}} \beta_{\mathrm{s}} \mathrm{s},$$

  aí existe uma função $\mathrm{i} : \mathrm{T} \to \mathrm{I}$ tal que:

  $$\forall \mathrm{s} \in \mathrm{T} : \mathrm{v}_{\mathrm{i}_{\mathrm{s}}} = \mathrm{s},$$

  aí seja $\mathrm{J} = \mathrm{Im}(\mathrm{i})$, então J é finito e i é uma bijeção de T a J e sua inversa é $\mathrm{u} = \mathrm{v} \restriction \mathrm{J}$, aí seja $\alpha = \beta \circ \mathrm{u}$, então:

  $$\mathrm{x} = \sum_{\mathrm{s} \in \mathrm{T}} \beta_{\mathrm{s}} \mathrm{s} = \sum_{\mathrm{j} \in \mathrm{J}} \beta_{\mathrm{u}_{\mathrm{j}}} \mathrm{u}_{\mathrm{j}} = \sum_{\mathrm{j} \in \mathrm{J}} \alpha_{\mathrm{j}} \mathrm{u}_{\mathrm{j}} = \sum_{\mathrm{j} \in \mathrm{J}} \alpha_{\mathrm{j}} \mathrm{v}_{\mathrm{j}};$$

  logo v gera V. $\square$

Definição 1.7. Seja V um espaço vetorial sobre um corpo K e seja I um conjunto e seja $v : I \to V$ uma função. Dizemos que v é **linearmente independente** se e só se para todo conjunto finito $J \subseteq I$ e toda função $\alpha : J \to K$, então temos a implicação:

$$\sum_{i \in J} \alpha_i v_i = 0 \quad \Rightarrow \quad \forall i \in J : \alpha_i = 0.$$

Dizemos que v é **linearmente dependente** se e só se v não é linearmente independente.

Definição 1.8. Seja V um espaço vetorial sobre um corpo K e seja $S \subseteq V$ um conjunto. Dizemos que S é **linearmente independente** se e só se a função $v : S \to V$ dada por $\forall s \in S : v_s = s$ é linearmente independente. Dizemos que S é **linearmente dependente** se e só se não é linearmente independente.

Exemplo 1.9. Se V é um espaço vetorial sobre um corpo K e $u \in V$ é um elemento não nulo, então a função $v : \{0, 1\} \to V$ dada por $v_0 = u$ e $v_1 = u$ é linearmente dependente, mas o conjunto $\{v_0, v_1\} = \{u\}$ é linearmente independente.

Definição 1.10. Seja V um espaço vetorial sobre um corpo K e seja I um conjunto. Uma **base de V ordenada por** I é uma função $b : I \to V$ tal que:

(i) b é linearmente independente.

(ii) b gera V.

Definição 1.11. Seja V um espaço vetorial sobre um corpo K. Uma **base** de V é um conjunto $B \subseteq V$ tal que:

(i) B é linearmente independente.

(ii) B gera V.

Teorema 1.12. Seja V um espaço vetorial e sejam $I \subseteq V$ linearmente independente e $S \subseteq V$ gerador de V tais que $I \subseteq S$. Então existe uma base B de V tal que

$$I \subseteq B \subseteq S.$$

Demonstração. Consideremos o conjunto:

$$\mathcal{M} := \{M \subseteq S \mid M \text{ é linearmente independente e } I \subseteq M\}$$

Então $(\mathcal{M}, \subseteq)$ é um conjunto parcialmente ordenado indutivo (ou seja, todo subconjunto totalmente ordenado possui uma cota superior). De fato, $I \in \mathcal{M}$, o que nos mostra que $\mathcal{M} \neq \emptyset$, e para subconjunto totalmente ordenado não vazio $\mathcal{C} \subseteq \mathcal{M}$ então $\bigcup \mathcal{C} \in \mathcal{M}$.

Logo, pelo Lema de Zorn, $\mathcal{M}$ possui um elemento maximal B. Vamos provar que esse elemento maximal é de fato uma base para V.

(i) B é linearmente independente: segue da definição de $\mathcal{M}$.

(ii) B gera V: Suponha por absurdo que B não gera V. Então existe $v \in S$ que não é combinação linear de elementos de B, aí $B \cup \{v\}$ é linearmente independente e $I \subseteq B \cup \{v\} \subseteq S$. Então $B \cup \{v\} \in \mathcal{M}$, uma contradição, pois B já é um elemento maximal de $\mathcal{M}$ e obviamente $B \subseteq B \cup \{v\}$. Logo B gera V. Portanto, B é uma base de V e $I \subseteq B \subseteq S$. □

O resultado acima mostra que todo espaço vetorial tem base, bastando para isso tomar $I = \emptyset$ e $S = V$.

Corolário 1.13. Seja V um espaço vetorial sobre um corpo K, seja $I \subseteq V$ um conjunto linearmente independente e seja $S \subseteq V$ um conjunto que gere V. Então

(i) O espaço V tem uma base;

(ii) Existe uma base B de V tal que $I \subseteq B$;

(iii) Existe uma base B de V tal que $B \subseteq S$.

Lema 1.14. Seja V um espaço vetorial sobre um corpo K. Sejam $(v_i)_{i=1}^n$ uma sequência linearmente independente e $(u_j)_{j=1}^m$ uma sequência que gera V. Então $n \leq m$.

Sublema 1.15. Seja V um espaço vetorial sobre um corpo K. Uma sequência $(v_i)_{i=1}^m$ é linearmente dependente se e somente se existem i e uma sequência $(\alpha_j)_{j=1}^{i-1}$ tais que

$$v_i = \sum_{j=1}^{i-1} \alpha_j v_j.$$

Demonstração do Sublema. Se $(v_i)_{i=1}^m$ é linearmente dependente, então existe uma sequência $(\alpha_i)_{i=1}^m$ não identicamente nula tal que:

$$\sum_{i=1}^{m} \alpha_i v_i = 0.$$

Seja i o maior índice tal que $\alpha_i \neq 0$. Então segue que

$$\begin{aligned} & \alpha_1 v_1 + \ldots + \alpha_i v_i = 0 \\ \iff & \alpha_1 v_1 + \ldots + \alpha_{i-1} v_{i-1} = -\alpha_i v_i \\ \iff & v_i = -\sum_{j=1}^{i-1} \frac{\alpha_j}{\alpha_i} v_j. \end{aligned}$$

□

Demonstração do Lema. Primeiro, listamos os dois conjuntos de vetores: o conjunto gerador seguido do conjunto linearmente independente:

$$u_1, \ldots, u_m; v_1, \ldots, v_n$$

Então movemos o primeiro vetor v_1 para a esquerda da primeira lista:

$$v_1, u_1, \ldots, u_m; v_2, \ldots, v_n$$

Como $u_1, \ldots, u_m$ gera V, v_1 é combinação linear dos u_i's. Isso implica que podemos remover um dos s_i's, que indexando se necessário pode ser u_1, da primeira lista, e ainda temos um conjunto gerador:

$$v_1, u_2, \ldots, u_m; v_2, \ldots, v_n$$

Note que o primeiro conjunto dos vetores ainda gera V e o segundo conjunto ainda é linearmente independente.

Agora repetimos o processo, movendo v_2 da segunda lista para a primeira lista:

$$v_1, v_2, u_2, \ldots, u_m; v_3, \ldots, v_n$$

Como antes, os vetores na primeira lista são linearmente dependentes, já que eles geravam V antes da inclusão de v_2. Entretanto, como os v_i's são linearmente independentes, qualquer combinação linear não trivial dos vetores na primeira lista que valha 0 deve envolver pelo menos um dos u_i's. Portanto, podemos remover este vetor, que novamente reindexando se necessário pode ser u_2 e ainda temos um conjunto gerador:

$$v_1, v_2, u_3, \ldots, u_m; v_3, \ldots, v_n$$

Mais uma vez, o primeiro conjunto dos vetores gera V e o segundo conjunto é linearmente independente.

Agora, if $m < n$, então este processo eventualmente esgotará os u_i's e nos levará à lista

$$v_1, v_2, \ldots, v_m; v_{m+1}, \ldots, v_n$$

em que $v_1, v_2, \ldots, v_m$ geram V, o que claramente não é possível pois v_n não é combinação linear dos $v_1, v_2, \ldots, v_m$. Portanto $n \leq m$. □

Observação 1.16. Com o lema, também podemos mostrar que, se existe um conjunto gerador finito, então podemos mostrar que todo conjunto linearmente independente é finito.

De fato, se existirem uma sequência geradora $(u_j)_{j=1}^m$ e um conjunto linearmente independente infinito S, então podemos pegar $m + 1$ vetores distintos e assim formar uma sequência linearmente independente $(v_i)_{i=1}^{m+1}$, contradizendo o lema 1.14.

Vamos relembrar o que fizemos até aqui com um exemplo:

Exemplo 1.17. Considere $V = \mathbb{R}^4$ um $\mathbb{R}$-espaço vetorial. Sejam os vetores:

$$\begin{aligned} v_1 &= (1, 0, 0, 0) \\ v_2 &= (0, 1, 0, -1) \\ v_3 &= (0, 0, 1, -1) \\ v_4 &= (1, -1, 0, 0) \\ v_5 &= (1, 2, 1, 0) \end{aligned}$$

Considere $I = \{v_1, v_2\}$ e $S = \{v_1, v_2, v_3, v_4, v_5\}$. Observe que I é LI; de fato,

$$\alpha_1 v_1 + \alpha_2 v_2 = 0 \Rightarrow \alpha_1(1, 0, 0, 0) + \alpha_2(0, 1, 0, -1) = 0 \Rightarrow \begin{cases} \alpha_1 &= 0 \\ \alpha_2 &= 0 \\ -\alpha_2 &= 0 \end{cases} \Rightarrow \alpha_1 = \alpha_2 = 0$$

Ademais, tomando $v = (x, y, z, w) \in \mathbb{R}^4$, temos que

$$(x - z + w + y)v_1 + (z - w - \varepsilon)v_2 + (z - \varepsilon)v_3 + (z - w - y + \varepsilon)v_4 + \varepsilon_5 = v,$$

para todo $\varepsilon \in \mathbb{R}$. Logo, S gera V.

Então, existe uma base B de $\mathbb{R}^4$ tal que

$$\{v_1, v_2\} \subseteq B \subseteq \{v_1, v_2, v_3, v_4, v_5\}$$

De fato, esta base é $B = \{v_1, v_2, v_3, v_4\}$, pois percebe-se que

$$v_5 = \frac{5}{2}v_1 + \frac{1}{2}v_2 - \frac{1}{2}v_3 - \frac{3}{2}v_4$$

Para trabalhar com a cardinalidade das bases, utilizaremos alguns fatos conhecidos, enunciados na próxima proposição:

Proposição 1.18. Se λ e μ são cardinais, então:

- Se $\lambda \leq \mu$ e $\mu \leq \lambda$, então $\lambda = \mu$. (Teorema de Cantor-Bernstein)
- Se λ e μ são infinitos, então
$$\lambda + \mu = \lambda\mu = \max\{\lambda, \mu\}.$$

Teorema 1.19. Seja V um espaço vetorial, então duas bases quaisquer têm o mesmo cardinal.

Demonstração. Sejam B e C bases de V.

- Se B ou C são finitos, então pela observação 1.16 podemos inferir que B e C são ambos finitos e assim aplicar o lema 1.14.
- Se B e C são infinitos. Para $u \in C$ existem um conjunto finito $I_u \subseteq B$ e uma função $\alpha_u : I_u \to K$ tais que $u = \sum_{i \in I_u} (\alpha_u)_i i$. Seja $I \subseteq \bigcup_{u \in C} \subseteq B$. Então I gera V, assim $I = C$. Desse modo:

  $$|B| = |I| = \left| \bigcup_{u \in C} I_u \right| \leq \sum_{u \in C} |I_u| \leq \aleph_0 \cdot |C| = |C|,$$

  assim $|B| \leq |C|$. Analogamente $|C| \leq |B|$. Portanto $|B| = |C|$.

□

Definição 1.20. Dizemos que a **dimensão** de um espaço vetorial é a cardinalidade de sua base.

1.3 Subespaços

Definição 1.21. Seja V um espaço vetorial sobre um corpo K. Um **subespaço** de V é um conjunto $W \subseteq V$ tal que:

- $0 \in W$,
- Para $x, y \in W$ então $x + y \in W$,
- Para $a \in K$ e $x \in W$ então $ax \in W$.

Proposição 1.22. Seja V um espaço vetorial e seja $\mathcal{W}$ um conjunto de subespaços. Então $\bigcap \mathcal{W}$ é um subespaço de V.

Definição 1.23. Se S é subconjunto de V, definimos:

$$\langle S \rangle = \left\{ \sum_{v \in I} \alpha_v v \mid I \subseteq S \text{ e } I \text{ é finito e } \alpha \in K^I \right\}$$

e chamamos de **subespaço gerado** por S.

Proposição 1.24. Se S é subconjunto de V, então:

$$\langle S \rangle = \bigcap \{ W \mid W \text{ é subespaço de } V \text{ e } S \subseteq W \}.$$

Demonstração. Seja:

$$T = \bigcap \{ W \mid W \text{ é subespaço de } V \text{ e } S \subseteq W \}.$$

Para $x \in \langle S \rangle$, então existem um conjunto finito $I \subseteq S$ e uma função $\alpha : I \to V$ tal que:

$$x = \sum_{v \in I} \alpha_v v,$$

aí para todo subespaço W tal que $S \subseteq W$, então para todo $v \in I$ temos $v \in S$, aí $v \in W$; aí por indução finita temos $x \in W$; logo $x \in T$. Portanto $\langle S \rangle \subseteq T$.

Além disso, temos o seguinte:

- $\emptyset \subseteq S$ e $\emptyset$ é finito e $\emptyset \in K^{\emptyset}$ e:

  $$0 = \sum_{v \in \emptyset} \emptyset_v v,$$

  aí $0 \in \langle S \rangle$.

- Para $\mathrm{x}, \mathrm{y} \in \langle \mathrm{S} \rangle$, então existem conjuntos finitos $\mathrm{I}, \mathrm{J} \subseteq \mathrm{S}$ e funções $\alpha \in \mathrm{K}^{\mathrm{I}}$ e $\beta \in \mathrm{K}^{\mathrm{J}}$ tais que:

$$\mathrm{x} = \sum_{\mathrm{u} \in \mathrm{I}} \alpha_{\mathrm{u}} \mathrm{u}, \quad \mathrm{y} = \sum_{\mathrm{v} \in \mathrm{J}} \beta_{\mathrm{v}} \mathrm{v},$$

  aí sendo $\mathrm{L} = \mathrm{I} \cup \mathrm{J}$ então $\mathrm{L} \subseteq \mathrm{S}$ e L é finito, e também sendo $\tilde{\alpha}, \tilde{\beta} : \mathrm{L} \to \mathrm{K}$ dadas por:

$$\tilde{\alpha}_{\mathrm{l}} = \begin{cases} \alpha_{\mathrm{l}} & \text{se } \mathrm{l} \in \mathrm{I} \\ 0 & \text{se } \mathrm{l} \notin \mathrm{I} \end{cases}, \quad \tilde{\beta}_{\mathrm{l}} = \begin{cases} \beta_{\mathrm{l}} & \text{se } \mathrm{l} \in \mathrm{J} \\ 0 & \text{se } \mathrm{l} \notin \mathrm{J} \end{cases},$$

  e sendo $\gamma : \mathrm{L} \to \mathrm{K}$ dada por $\gamma_{\mathrm{l}} = \tilde{\alpha}_{\mathrm{l}} + \tilde{\beta}_{\mathrm{l}}$, então:

$$\mathrm{x} + \mathrm{y} = \sum_{\mathrm{l} \in \mathrm{L}} \gamma_{\mathrm{l}} \mathrm{l},$$

  aí $\mathrm{x} + \mathrm{y} \in \langle \mathrm{S} \rangle$.

- Para $\mathrm{a} \in \mathrm{K}$ e $\mathrm{x} \in \langle \mathrm{S} \rangle$, então existem conjunto finito $\mathrm{I} \subseteq \mathrm{S}$ e $\alpha \in \mathrm{K}^{\mathrm{I}}$ tais que:

$$\mathrm{x} = \sum_{\mathrm{v} \in \mathrm{I}} \alpha_{\mathrm{v}} \mathrm{v},$$

  aí sendo $\beta : \mathrm{I} \to \mathrm{K}$ dada por $\beta_{\mathrm{v}} = \mathrm{a}\alpha_{\mathrm{v}}$, então:

$$\mathrm{ax} = \sum_{\mathrm{v} \in \mathrm{I}} \beta_{\mathrm{v}} \mathrm{v},$$

  aí $\mathrm{ax} \in \langle \mathrm{S} \rangle$.

- Para $\mathrm{s} \in \mathrm{S}$, então $\{\mathrm{s}\} \subseteq \mathrm{S}$ e $\{\mathrm{s}\}$ é finito, e considerando a função $\alpha : \{\mathrm{s}\} \to \mathrm{K}$ dada por $\alpha_{\mathrm{s}} = 1$, então:

$$\mathrm{s} = \sum_{\mathrm{v} \in \{\mathrm{s}\}} \alpha_{\mathrm{v}} \mathrm{v},$$

  aí $\mathrm{S} \subseteq \langle \mathrm{S} \rangle$.

Logo $\langle \mathrm{S} \rangle$ é um subespaço de V tal que $\mathrm{S} \subseteq \langle \mathrm{S} \rangle$, aí $\mathrm{T} \subseteq \langle \mathrm{S} \rangle$. □

A intersecção de subsespaços sempre é um subespaço, mas o mesmo não acontece com a união de subespaços.

Proposição 1.25. Se A e B são subespaços de V tais que $\mathrm{A} \nsubseteq \mathrm{B}$ e $\mathrm{B} \nsubseteq \mathrm{A}$, então $\mathrm{A} \cup \mathrm{B}$ não é subespaço de V.

Demonstração. Nesse caso, existe $\mathrm{a} \in \mathrm{A}$ tal que $\mathrm{a} \notin \mathrm{B}$ e existe $\mathrm{b} \in \mathrm{B}$ tal que $\mathrm{b} \notin \mathrm{A}$. Seja $\mathrm{c} = \mathrm{a} + \mathrm{b}$. Então:

- Se $\mathrm{c} \in \mathrm{A}$, $\mathrm{b} = \mathrm{c} - \mathrm{a} \in \mathrm{A}$, o que é impossível.

- Se $\mathrm{c} \in \mathrm{B}$, $\mathrm{a} = \mathrm{c} - \mathrm{b} \in \mathrm{b}$, o que é impossível.

Logo, concluímos que $\mathrm{c} \notin \mathrm{A} \cup \mathrm{B}$, absurdo. □

Portanto concluímos que $\mathrm{A} \cup \mathrm{B}$ é um subespaço se e somente se $\mathrm{A} \subseteq \mathrm{B}$ ou $\mathrm{B} \subseteq \mathrm{A}$.

Observação 1.26. Seja $\mathrm{K} = \mathrm{F}_2 = \{0, 1\}$, e tome $\mathrm{V} = \mathrm{K}^2$. Então,

$$\mathrm{V} = \langle (0,1) \rangle \cup \langle (1,0) \rangle \cup \langle (1,1) \rangle$$

Na verdade, V só pode ser escrito como união de um número finito de subespaços próprios se K for um corpo finito, conforme a seguinte proposição.

Proposição 1.27. Um espaço vetorial V sobre um corpo infinito K não pode ser escrito como união de um número finito de subespaços próprios.

Demonstração. Suponhamos que $V = S_1 \cup \cdots \cup S_n$, em que podemos assumir que:

$$S_1 \not\subseteq S_2 \cup \cdots \cup S_n,$$

Seja $w \in S_1 \setminus (S_2 \cup \cdots \cup S_n)$ e seja $v \notin S_1$. Considere o conjunto infinito:

$$A = \{rw + v \mid r \in K\},$$

que é a "reta" passando por v e paralela a w. Queremos mostrar que cada S_i contém no máximo um vetor do conjunto infinito A, o que será uma contradição ao fato de que $V = S_1 \cup \cdots \cup S_n$. Isto provará o teorema.

Se $rw + v \in S_1$ para algum $r \neq 0$, então $w \in S_1$ implicará $v \in S_1$, contrário às hipóteses. Agora, suponha que $r_1 w + v \in S_1$ e $r_2 w + v \in S_1$, para algum $i \geq 2$, em que $r_1 \neq r_2$. Então:

$$(r_1 - r_2)w = (r_1 w + v) - (r_2 w + v) \in S_i,$$

aí $w \in S_i$, que também contradiz as hipóteses. □

Apesar de não podermos trabalhar com a união, podemos realizar a soma de subespaços, e esta sim é um subespaço:

Definição 1.28. Sejam $W_i \subseteq V$, $i \in I$, subespaços de V. Definimos:

$$\sum_{i \in I} W_i = \{w_{i_1} + \ldots + w_{i_k} \mid k \in \mathbb{N}, w_i \in W_i\}.$$

Pode-se mostrar que o conjunto:

$$\sum_{i \in I} W_i$$

é subespaço de V.

Definição 1.29. Uma soma:

$$\sum_{i \in I} W_i$$

é dita uma **soma direta** se para todo $i \in I$ tivermos:

$$W_i \cap \left(\sum_{j \neq i} W_j \right) = 0.$$

Teorema 1.30. Para subespaço A de V, então existe subespaço $B \subseteq V$ tal que $V = A \oplus B$.

Demonstração. Seja E uma base de A. Então existe uma base G de V tal que $E \subseteq G$, aí seja $F = G \setminus E$, e seja B o subespaço gerado por F. Então é fácil ver que $V = A \oplus B$. □

Teorema 1.31.

$$\dim(A + B) + \dim(A \cap B) = \dim(A) + \dim(B).$$

Demonstração. Seja E base de $A \cap B$. Então existe F tal que $B \cap F = \emptyset$ e $E \cup F$ seja base de A e existe G tal que $A \cap G = \emptyset$ e $E \cup G$ seja base de B. Então $E \cup F \cup G$ é base de $A + B$. Daí:

$$\dim(A + B) + \dim(A \cap B) = |E| + |F| + |G| + |E| = |E| + |F| + |E| + |G| = \dim(A) + \dim(B)$$

□

Exemplo 1.32. Considere novamente $V = \mathbb{R}^4$. Sejam

$$W_1 = \{(x, y, z, t) \in \mathbb{R}^4 | y + z + t = 0\},$$

$$W_2 = \{(x, y, z, t) \in \mathbb{R}^4 | x + y = 0 \text{ e } z - 2t = 0\}.$$

Então W_1 e W_2 são subespaços de V. Assim, $W_1 + W_2$ e $W_1 \cap W_2$ são subespaços de V. Vamos encontrar bases para eles.

Note que:

$$\begin{aligned} W_1 &= \{(x, y, z, t) \in \mathbb{R}^4 | y + z + t = 0\} \\ &= \{(x, y, z, -y - z) \in \mathbb{R}^4 | x, y, z \in \mathbb{R}\} \\ &= \{(x, 0, 0, 0) + (0, y, 0 - y) + (0, 0, z, -z) : x, y, z \in \mathbb{R}\} \\ &= \langle (1, 0, 0, 0), (0, 1, 0 - 1), (0, 0, 1, -1) \rangle \end{aligned}$$

Verifica-se também que $(1, 0, 0, 0), (0, 1, 0 - 1), (0, 0, 1, -1)$ são linearmente independentes. Logo, $B_1 = \{(1, 0, 0, 0), (0, 1, 0 - 1), (0, 0, 1, -1)\}$ é base para W_1.

Analogamente, mostra-se que $B_2 = \{(1, -1, 0, 0), (0, 0, 2, 1)\}$ é base para W_2.

Agora, para determinar uma base de $W_1 + W_2$, podemos escalonar a matriz

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 2 & 1 \end{pmatrix} \to \cdots \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Portanto, o conjunto

$$\mathcal{B} = \{(1, 0, 0, 0), (0, 1, 0, -1), (0, 0, 1, -1), (1, -1, 0, 0)\}$$

é base de $W_1 + W_2$.

Para determinar uma base de $W_1 \cap W_2$, basta resolver o sistema

$$\begin{cases} y + z + t = 0 \\ x + y = 0 \\ z - 2t = 0 \end{cases}$$

Assim, $W_1 \cap W_2 = \langle (3, -3, 2, 1) \rangle$.

Observe que

$$\dim(W_1 \cap W_2) + \dim(W_1 + W_2) = 1 + 4 = 5 = 3 + 2 = \dim(W_1) + \dim(W_2).$$

Como $\dim(W_1 + W_2) = 4$, temos que $W_1 + W_2 = V = \mathbb{R}^4$.

Observe também que, como $\dim(W_1 \cap W_2) = 1$, a soma $W_1 + W_2$ não é direta.

1.4 Coordenadas

Definição 1.33. Seja V um espaço vetorial de dimensão finita. Seja B uma base de V. Então para $v \in V$ existe um único $\alpha : B \to K$ tal que

$$v = \sum_{b \in B} \alpha_b b,$$

e chamamos esse α de $[v]_B$.

Capítulo 2

Transformações Lineares

2.1 Definições

Definição 2.1. Sejam U e V espaços vetoriais sobre um corpo K. Uma **transformação linear** é uma função $T : U \to V$ tal que

$$T(\alpha u + \beta v) = \alpha T(u) + \beta T(v)$$

para quaisquer $\alpha, \beta \in K$ e $u, v \in V$. Além disso, denotamos o conjunto das transformações lineares de U a V por $\mathcal{L}(U, V)$.

Teorema 2.2. Sejam U e V espaços vetoriais sobre K, seja B uma base de U e $f : B \to V$ uma função. Então existe uma única transformação linear $T \in \mathcal{L}(U, V)$ tal que $\forall b \in B : T(b) = f(b)$.

Definição 2.3. Seja $T \in \mathcal{L}(U, V)$. Definimos $\mathrm{Ker}(T) = \{u \in U : T(u) = 0\}$. Definimos $\mathrm{Rank}(T) = \dim(\mathrm{Im}(T))$.

Proposição 2.4. Seja $T \in \mathcal{L}(U, V)$. Então:

- $\mathrm{Ker}(T)$ é um subespaço de U.
- $\mathrm{Im}(T)$ é um subespaço de V.
- T é injetora se e só se $\mathrm{Ker}(T) = 0$.
- Se T é bijetora, então $T^{-1} \in \mathcal{L}(V, U)$.

Teorema 2.5. Seja $\mathcal{L}(U, V)$, seja B uma base de $\mathrm{Ker}(T)$, e seja C um conjunto tal que $T[C]$ seja base de $\mathrm{Im}(T)$. Então $B \cup C$ é base V.

Demonstração. Para $v \in V$ então $T(v) \in \mathrm{Im}(T)$, então existem um conjunto finito $F \subseteq C$ e $\alpha : F \to K$ tais que:

$$T(v) = \sum_{w \in F} \alpha_w T(w),$$

assim:

$$T\left(v - \sum_{w \in F} \alpha_w w\right) = 0,$$

aí:

$$v - \sum_{w \in F} \alpha_w w \in \mathrm{Ker}(T),$$

assim existem um conjunto finito $E \subseteq B$ e função $\beta : B \to K$ tais que:

$$v - \sum_{w \in F} \alpha_w w = \sum_{u \in E} \beta_u u,$$

aí:

$$\mathrm{v} = \sum_{\mathrm{u} \in \mathrm{E}} \beta_{\mathrm{u}} \mathrm{u} + \sum_{\mathrm{w} \in \mathrm{F}} \alpha_{\mathrm{w}} \mathrm{w}.$$

Por outro lado, para subconjunto finito $\mathrm{E} \subseteq \mathrm{B} \cup \mathrm{C}$ e função $\alpha : \mathrm{E} \to \mathrm{K}$ tais que:

$$\sum_{\mathrm{e} \in \mathrm{E}} \alpha_{\mathrm{e}} \mathrm{e} = 0,$$

então:

$$\sum_{\mathrm{e} \in \mathrm{E} \cap \mathrm{C}} \alpha_{\mathrm{e}} \mathrm{T}(\mathrm{e}) = 0,$$

aí:

$$\forall \mathrm{e} \in \mathrm{E} \cap \mathrm{C} : \alpha_{\mathrm{e}} = 0,$$

aí:

$$\sum_{\mathrm{e} \in \mathrm{E} \setminus \mathrm{C}} \alpha_{\mathrm{e}} \mathrm{e} = 0,$$

aí:

$$\forall \mathrm{e} \in \mathrm{E} \setminus \mathrm{C} : \alpha_{\mathrm{e}} = 0,$$

portanto:

$$\forall \mathrm{e} \in \mathrm{E} : \alpha_{\mathrm{e}} = 0.$$

□

Teorema 2.6 (Teorema do Núcleo-Imagem)**.** Seja $\mathrm{T} \in \mathcal{L}(\mathrm{U}, \mathrm{V})$. Então

$$\mathrm{U} = \mathrm{Ker}(\mathrm{T}) \oplus \mathrm{Im}(\mathrm{T})$$

Corolário 2.7.

$$\dim \mathrm{V} = \dim(\mathrm{Ker}(\mathrm{T})) + \dim(\mathrm{Im}(\mathrm{T})).$$

Definição 2.8. Se $\mathrm{T} \in \mathcal{L}(\mathrm{U}, \mathrm{V})$ é bijetora, dizemos que T é um **isomorfismo** de U a V.

Proposição 2.9. $\mathrm{T} \in \mathcal{L}(\mathrm{U}, \mathrm{V})$ é isomorfismo se e somente se T^{-1} também o é.

Proposição 2.10. Dois espaços vetoriais U e V são isomorfos se e somente se quaisquer duas bases B de U e C de V possuem a mesma cardinalidade.

Teorema 2.11. Para espaços vetoriais U e V, então U é isomorfo a V se e só se $\dim(\mathrm{U}) = \dim(\mathrm{V})$.

2.2 Espaço Dual

Definição 2.12. Seja V um espaço vetorial sobre K. Denotamos $\mathrm{V}^* = \mathcal{L}(\mathrm{V}, \mathrm{K})$. O espaço V^* chama-se o **espaço dual** de V. Os elementos de V chamam-se **funcionais lineares**.

Se $\dim(\mathrm{V}) = \mathrm{n}$, então $\dim(\mathrm{V}^*) = \mathrm{n} \cdot 1 = \mathrm{n}$, aí V e V^* são isomorfos.

Teorema 2.13. Seja V um espaço vetorial com $\dim(\mathrm{V}) = \mathrm{n}$ e $\mathrm{B} = (\mathrm{v}_{\mathrm{i}})_{\mathrm{i}=1}^{\mathrm{n}}$ uma base de V. Então existe uma base $\mathrm{B}^* = (\mathrm{f}_{\mathrm{i}})_{\mathrm{i}=1}^{\mathrm{n}}$ de V^* tal que $\mathrm{f}_{\mathrm{i}}(\mathrm{v}_{\mathrm{j}}) = \delta_{\mathrm{i},\mathrm{j}}$ para quaisquer i, j. Além disso:

$$\forall \mathrm{v} \in \mathrm{V} : \mathrm{v} = \sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{f}_{\mathrm{i}}(\mathrm{v}) \mathrm{v}_{\mathrm{i}}$$

e:

$$\forall \mathrm{f} \in \mathrm{V}^* : \mathrm{f} = \sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{f}(\mathrm{v}_{\mathrm{i}}) \mathrm{f}_{\mathrm{i}}.$$

Demonstração. Para $i = 1, \dots, n$, existe uma única função linear $f_i : V \to K$ tal que:

$$f_i(v_j) = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$$

Sejam $\alpha_1, \dots, \alpha_n \in K$ tais que:

$$\sum_{i=1}^{n} \alpha_i f_i = 0.$$

Para $j = 1, \dots, n$, aplicando este funcional para o vetor $v_j \in B$, então:

$$0 = 0(v_j) = \sum_{i=1}^{n} \alpha_i f_i(v_j) = \alpha_j,$$

ou seja, $\alpha_j = 0$. Portanto B^* é linearmente independente.

Além disso, para $v \in V$ existem $\alpha_1, \dots, \alpha_n \in K$ tais que:

$$v = \sum_{i=1}^{n} \alpha_i v_i,$$

aí para $i = 1, \dots, n$ temos:

$$f_i(v) = \alpha_i f_i(v_i) = \alpha_i;$$

logo:

$$f(v) = \sum_{i=1}^{n} \alpha_i f(v_i) = \sum_{i=1}^{n} f(v_i) f_i(v).$$ □

Definição 2.14. A base B^* chama-se a **base dual** da base B.

Podemos estender o estudo do espaço dual para espaços vetoriais quaisquer.

Definição 2.15. Seja B uma base de V, então para cada $a \in B$ definimos a transformação linear $f_a \in V^*$ por $f_a(b) = \delta_{a,b}$.

Nesse caso, podemos adaptar facilmente o argumento na demonstração do teorema 2.13 para mostrar que $(f_a)_{a \in B}$ é linearmente independente em V^* e para todo $v \in V$ existe um conjunto finito $F \subseteq B$ tal que:

$$v = \sum_{b \in F} f_b(v) b.$$

2.3 Espaço Bidual

Definição 2.16. Seja V um espaço vetorial sobre K. O espaço $V^{**} = (V^*)^*$ chama-se o **espaço bidual** do espaço V.

Definição 2.17. Para $v \in V$, definamos $\varphi_v : V^* \to K$ assim:

$$\forall f \in V^* : \varphi_v(f) = f(v).$$

Então $\varphi_v \in V^{**}$.

Proposição 2.18. $\varphi \in \mathcal{L}(V, V^{**})$ e φ é injetora.

Demonstração. Seja B uma base de V. Para $\mathrm{v} \in \mathrm{Ker}(\varphi)$, então $\varphi_{\mathrm{v}} = 0$, aí temos $\forall \mathrm{b} \in \mathrm{B} : \mathrm{f_b}(\mathrm{v}) = \varphi_{\mathrm{v}}(\mathrm{f_b}) = 0$, aí existe um conjunto finito $\mathrm{F} \subseteq \mathrm{B}$ tal que:

$$\mathrm{v} = \sum_{\mathrm{b} \in \mathrm{F}} \mathrm{f_b}(\mathrm{v})\mathrm{b},$$

aí $\mathrm{v} = 0$. □

Corolário 2.19. Se $\dim(\mathrm{V})$ é finita, então $\varphi : \mathrm{V} \to \mathrm{V}^{**}$ é um isomorfismo.

Demonstração.

$$\dim(\mathrm{V}) = \dim(\mathrm{V}^*) = \dim(\mathrm{V}^{**}).$$ □

Observação 2.20. Nesse caso φ é um isomorfismo natural, ou seja, não depende da escolha de uma base.

Corolário 2.21. Se $\dim(\mathrm{V})$ é finita, então toda base de V^* é a base dual para uma base de V.

Demonstração. Seja $\mathrm{C} = (\mathrm{f_i})_{\mathrm{i}=1}^{\mathrm{n}}$ uma base de V^*. Consideremos a base dual $\mathrm{C}^* = (\mathrm{g_i})_{\mathrm{i}=1}^{\mathrm{n}}$ de V^{**}. Mas φ é sobrejetora, então existem $\mathrm{v}_1, \ldots, \mathrm{v_n} \in \mathrm{V}$ tais que para todo i tenhamos $\mathrm{g_i} = \varphi_{\mathrm{v_i}}$, assim:

$$\mathrm{f_i}(\mathrm{v_j}) = \varphi_{\mathrm{v_j}}(\mathrm{f_i}) = \mathrm{g_j}(\mathrm{f_i}) = \delta_{\mathrm{j,i}} = \delta_{\mathrm{i,j}},$$

logo $\mathrm{C} = (\mathrm{f_i})_{\mathrm{i}=1}^{\mathrm{n}}$ é base dual da base $(\mathrm{v_i})_{\mathrm{i}=1}^{\mathrm{n}}$ de V. □

2.4 Anuladores

Definição 2.22. Seja V um espaço vetorial e seja $\mathrm{S} \subseteq \mathrm{V}$ um subconjunto. Então definimos:

$$\mathrm{S}^0 = \{\mathrm{f} \in \mathrm{V}^* \mid \forall \mathrm{s} \in \mathrm{S} : \mathrm{f}(\mathrm{s}) = 0\}.$$

O conjunto S^0 chama-se o **anulador** de S.

Proposição 2.23. S^0 é um subespaço de V.

Teorema 2.24. Seja V um espaço de dimensão finita e $\mathrm{W} \subseteq \mathrm{V}$ um subespaço. Então:

$$\dim(\mathrm{V}) = \dim(\mathrm{W}) + \dim(\mathrm{V}^0).$$

Demonstração. Seja $\dim(\mathrm{V}) = \mathrm{n}$ e $\dim(\mathrm{W}) = \mathrm{m}$. Escolhemos uma base $(\mathrm{v}_1, \ldots, \mathrm{v_m})$ de W e completemo-la até uma base $(\mathrm{v}_1, \ldots, \mathrm{v_m}, \mathrm{v_{m+1}}, \ldots \mathrm{v_n})$ de V. Consideremos a base dual $(\mathrm{f}_1, \ldots, \mathrm{f_n})$ de V^*. Mostraremos que $(\mathrm{f_{m+1}}, \ldots, \mathrm{f_n})$ é uma base de W^0. É claro que para todo $\mathrm{i} = \mathrm{m}+1, \ldots, \mathrm{n}$ temos $\mathrm{f_i} \in \mathrm{W}^0$. Seja $\mathrm{f} \in \mathrm{W}^0$, então:

$$\mathrm{f} = \sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{f}(\mathrm{v_i})\mathrm{f_i} = \sum_{\mathrm{i}=\mathrm{m}+1}^{\mathrm{n}} \mathrm{f}(\mathrm{v_i})\mathrm{f_i}.$$ □

Teorema 2.25. Se $\dim(\mathrm{V})$ é finita e $\mathrm{V} = \mathrm{U} \oplus \mathrm{W}$, então $\mathrm{V}^* = \mathrm{U}^0 \oplus \mathrm{W}^0$ e $\mathrm{U}^0 \cong \mathrm{W}^*$ e $\mathrm{W}_0 \cong \mathrm{U}^*$.

Demonstração. Seja $\mathrm{B} = \mathrm{B_U} \cup \mathrm{B_W}$ base de V, em que $\mathrm{B_U}$ é base de U e $\mathrm{B_W}$ é base de W. Então a base dual é $\mathrm{B}^* = \mathrm{B_U^*} \cup \mathrm{B_V^*}$, e pelo teorema anterior temos $\langle \mathrm{B_U^*} \rangle = \mathrm{W}^0$ e $\langle \mathrm{B_V^*} \rangle = \mathrm{U}^0$. □

2.5 Transpostas

Definição 2.26. Sejam U e V espaços vetoriais sobre K, e $T \in \mathcal{L}(U, V)$. Então definimos a **transposta** de T como a função:

$$\begin{aligned} T^t : V^t &\rightarrow U^t \\ f &\mapsto T^t(f) = f \circ T \end{aligned}$$

Proposição 2.27. Se dim(U) é finita e $T \in \mathcal{L}(U, V)$, então:

a) $\mathrm{Ker}(T^t) = (\mathrm{Im}(T))^0$.

b) $\mathrm{Rank}(T^t) = \mathrm{Rank}(T)$.

c) $\mathrm{Im}(T^t) = (\mathrm{Ker}(T))^0$.

Demonstração. Temos o seguinte:

a) Temos:

$$\begin{aligned} \mathrm{Ker}(T^t) &= \{f \in V^* \mid T^t(f) = 0\} \\ &= \{f \in V^* \mid f \circ T = 0\} \\ &= \{f \in V^* \mid \forall u \in U : f(T(u)) = 0\} \\ &= \{f \in V^* \mid f[\mathrm{Im}(T)] = 0\} \\ &= (\mathrm{Im}(T))^0. \end{aligned}$$

b) Temos $\mathrm{Rank}(T^t) = \dim(\mathrm{Im}(T^t))$ e $\mathrm{Rank}(T) = \dim(\mathrm{Im}(T))$. Além disso:

$$\dim(V^*) = \dim(\mathrm{Im}(T^t)) + \dim(\mathrm{Ker}(T^t))$$

$$\dim(V^*) = \dim(\mathrm{Im}(T)) + \dim(\mathrm{Im}(T))^0$$

mas $\dim(V^*) = \dim(V)$ e $\dim(\mathrm{Ker}(T^t)) + \dim(\mathrm{Im}(T))^0$.

c) Temos $\mathrm{Im}(T^t) \subseteq (\mathrm{Ker}(T))^0$. Seja $\varphi \in \mathrm{Im}(T^t)$, então existe $g \in V^*$ tal que $\varphi = T^t(g)$, aí para todo $u \in U$ nós temos $\varphi(u) = T^t(g)(u) = g(T(u))$. Se $u \in \mathrm{Ker}(T)$ então $T(u) = 0$, aí $\varphi(u) = 0$; logo $\varphi \in (\mathrm{Ker}(T))^0$. Além disso:

$$\dim(U) = \dim(\mathrm{Ker}(T)) + \dim(\mathrm{Ker}(T))^0$$

$$\dim(U) = \dim(\mathrm{Ker}(T)) + \dim(\mathrm{Im}(T))$$

aí $\dim(\mathrm{Ker}(T))^0 = \dim(\mathrm{Im}(T))$, aí $(\mathrm{Ker}(T))^0 = \mathrm{Im}(T)$. □

Teorema 2.28. Sejam U e V espaços vetoriais de dimensão finita com bases B e C e bases duais B^* e C^*. Se $T \in \mathcal{L}(U, V)$, então:

$$[T]^t_{B,C} = [T^t]_{C^*,B^*}$$

Corolário 2.29. Se $A \in M_{m,n}(K)$, então:

$$\mathrm{RowRank}(A) = \mathrm{ColumnRank}(A).$$

Demonstração. Consideremos $T : K^n \rightarrow K^m$ dada por $T(v) = Av$. Sejam B e C as bases canônicas de K^n e K^m, então $[T]_{B,C} = A$. Temos:

$$\begin{aligned} \mathrm{Rank}(T) &= \mathrm{ColumnRank}(A) \\ \mathrm{Rank}(T^t) &= \mathrm{ColumnRank}(A^t) = \mathrm{RowRank}(A). \end{aligned}$$

□

2.6 Espaços Quocientes

Definição 2.30. Seja V um espaço, $\mathrm{W} \subseteq \mathrm{V}$ um subespaço. Para $\mathrm{u}, \mathrm{v} \in \mathrm{V}$, digamos que $\mathrm{u} \sim \mathrm{v}$ se e só se $\mathrm{u} - \mathrm{v} \in \mathrm{W}$. Então $\sim$ é uma relação de equivalência, ou seja:

- Reflexiva, ou seja, $\mathrm{v} \sim \mathrm{v}$ sempre.
- Simétrica, ou seja, se $\mathrm{v} \sim \mathrm{u}$ então $\mathrm{u} \sim \mathrm{v}$.
- Transitiva, ou seja, se $\mathrm{v} \sim \mathrm{u}$ e $\mathrm{u} \sim \mathrm{w}$, então $\mathrm{v} \sim \mathrm{w}$.

Seja V/W o conjunto das classes de equivalência relativamente a $\sim$. Para $\mathrm{v} \in \mathrm{V}$ seja $\overline{\mathrm{v}}$ a classe de equivalência de v.

- Definamos em V/W uma estrutura de espaço vetorial. Para $\overline{\mathrm{v}}, \overline{\mathrm{w}} \in \mathrm{V}/\mathrm{W}$ definamos $\overline{\mathrm{v}} + \overline{\mathrm{w}} = \overline{\mathrm{v} + \mathrm{w}}$.
- Para $\alpha \in \mathrm{K}$ e $\overline{\mathrm{v}} \in \mathrm{V}$ definamos $\alpha \cdot \overline{\mathrm{v}} = \overline{\alpha \mathrm{v}}$. Então V/W é um espaço vetorial chamado **espaço quociente**.

Observação 2.31. As operações estão “bem definidas” pois:

- Se $\overline{\mathrm{v}} = \overline{\mathrm{v}'}$ e $\overline{\mathrm{u}} = \overline{\mathrm{u}'}$, então $\mathrm{v} \sim \mathrm{v}'$ e $\mathrm{u} \sim \mathrm{u}'$, aí $\mathrm{v} - \mathrm{v}', \mathrm{u} - \mathrm{u}' \in \mathrm{W}$, aí $(\mathrm{v} + \mathrm{u}) - (\mathrm{v}' + \mathrm{u}') = (\mathrm{v} - \mathrm{v}') + (\mathrm{u} - \mathrm{u}') \in \mathrm{W}$, aí $\overline{\mathrm{v} + \mathrm{u}} = \overline{\mathrm{v}' + \mathrm{u}'}$, aí $\overline{\mathrm{v}} + \overline{\mathrm{u}} = \overline{\mathrm{v}'} + \overline{\mathrm{u}'}$.
- Analogamente para a outra propriedade.

Também verificaremos algumas propriedades, deixando o resto ao leitor.

- Temos a comutatividade da adição, pois $\overline{\mathrm{u}} + \overline{\mathrm{v}} = \overline{\mathrm{v}} + \overline{\mathrm{u}}$ equivale a $\overline{\mathrm{u} + \mathrm{v}} = \overline{\mathrm{v} + \mathrm{u}}$, que é verdade pois $\mathrm{u} + \mathrm{v} = \mathrm{v} + \mathrm{u}$.
- O que é o $\overline{0}$ de V/W? Temos $\overline{0} = \mathrm{W}$, e também para todo $\mathrm{w} \in \mathrm{W}$ temos $\mathrm{w} \sim 0$, aí $\overline{\mathrm{w}} = \overline{0} = \mathrm{W}$.

Também temos o seguinte:

- Se $\mathrm{W} = \mathrm{V}$, então $\mathrm{V}/\mathrm{V} = \{\overline{0}\}$.
- Se $\mathrm{W} = \{0\}$, então $\mathrm{V}/\{0\} \cong \mathrm{V}$.

Proposição 2.32. Consideremos a aplicação:

$$\pi : \mathrm{V} \to \mathrm{V}/\mathrm{W}, \qquad \mathrm{v} \mapsto \overline{\mathrm{v}}.$$

Então $\pi \in \mathcal{L}(\mathrm{V}, \mathrm{V}/\mathrm{W})$, com $\mathrm{Ker}(\pi) = \mathrm{W}$.

Notação 2.33. π chama-se a **projeção canônica** de V para V/W.

Demonstração. Temos o seguinte:

- $\pi(\mathrm{v} + \mathrm{u}) = \overline{\mathrm{v} + \mathrm{u}} = \overline{\mathrm{v}} + \overline{\mathrm{u}} = \pi(\mathrm{v}) + \pi(\mathrm{u})$.
- $\pi(\alpha \mathrm{v}) = \overline{\alpha \mathrm{v}} = \alpha \overline{\mathrm{v}} = \alpha \pi(\mathrm{v})$.

Além disso, se $\mathrm{w} \in \mathrm{W}$ então $\pi(\mathrm{w}) = \overline{\mathrm{w}} = \mathrm{W}$ □

Proposição 2.34. Seja $\mathrm{T} \in \mathcal{L}(\mathrm{U}, \mathrm{V})$ e $\mathrm{W} \subseteq \mathrm{U}$ tal que $\mathrm{W} \subseteq \mathrm{Ker}(\mathrm{T})$. Então existe um único $\overline{\mathrm{T}} \in \mathcal{L}(\mathrm{U}/\mathrm{W}, \mathrm{V})$ tal que para todo $\mathrm{u} \in \mathrm{U}$ tenhamos:

$$\overline{\mathrm{T}}(\overline{\mathrm{u}}) = \mathrm{T}(\mathrm{u}).$$

Demonstração. Temos o seguinte:

1) Mostraremos que $\overline{T}$ está "bem definida". Se $\overline{u} = \overline{v}$, então $u - v \in W \subseteq \mathrm{Ker}(T)$, aí $T(u - v) = 0$, aí $T(u) = T(v)$.

2) Mostraremos que $\overline{T}$ é uma transformação linear.

- $\overline{T}(\overline{u} + \overline{v}) = \overline{T}(\overline{u + v}) = T(u + v) = T(u) + T(v) = \overline{T}(\overline{u}) + \overline{T}(\overline{v})$.
- $\overline{T}(\alpha\overline{v}) = \overline{T}(\overline{\alpha v}) = T(\alpha v) = \alpha T(v) = \alpha\overline{T}(\overline{v})$.

Agora, para todo $T' \in \mathcal{L}(U/W, V)$ tal que para todo $u \in U$ tenhamos:

$$T'(\overline{u}) = T(u),$$

então para todo $v \in U/W$ existe um $u \in U$ tal que $v = \overline{u}$, aí:

$$T'(v) = T'(\overline{u}) = T(u) = \overline{T}(\overline{u}) = \overline{T}(v);$$

logo $T' = \overline{T}$. □

Teorema 2.35. Sejam U e V espaços vetoriais sobre K, e seja $T \in \mathcal{L}(U, V)$. Então $U/\mathrm{Ker}(T) \cong \mathrm{Im}(T)$.

Demonstração. Pela proposição anterior, existe uma única $\overline{T} : U/\mathrm{Ker}(T) \to V$ tal que para todo $u \in U$ tenhamos:

$$\overline{T}(\overline{u}) = T(u).$$

Observemos que $\mathrm{Im}(\overline{T}) = \mathrm{Im}(T) = \{T(u) \mid u \in U\}$.

Além disso, para $\overline{u} \in \mathrm{Ker}(\overline{T})$, então $T(u) = \overline{T}(\overline{u}) = 0$, aí $u \in \mathrm{Ker}(T)$, aí $\overline{u} = \overline{0}$, de modo que $\overline{T}$ é injetora. □

Teorema 2.36. Seja W subespaço de V. Então todos os complementos de W em V são isomorfos ao V/W.

Demonstração. Seja $V = W \oplus U$. Consideremos a projeção canônica:

$$\pi : V \to V/W.$$

Seja $\overline{\pi} = \pi \restriction U$. Então $\mathrm{Ker}(\overline{\pi}) = U \cap \mathrm{Ker}(\pi) = U \cap W = \{0\}$. Logo $\overline{\pi}$ é injetora.

Para $\overline{v} \in V/W$, seja $v = w + u$, com $w \in W$ e $u \in U$. Então $\pi(v) = \pi(w) + \pi(u) = \pi(u) = \overline{\pi}(u)$, aí $\overline{v} = \overline{\pi}(u)$, assim $\overline{\pi}$ é sobre V/W. □

Corolário 2.37. Seja $W \subseteq V$ um subespaço. Então $\dim V = \dim W + \dim V/W$.

Demonstração. Seja $V = W \oplus U$, então $\dim V = \dim W + \dim U$, mas $U \cong V/W$, aí $\dim U = \dim V/W$. □

Observação 2.38. Existem espaços vetoriais W e U e W' e U' tais que $W \oplus U \cong W' \oplus U'$ e $W \cong W'$, mas $U \not\cong U'$. De fato podemos tomar:

$$W = \bigoplus_{i=0}^{\infty} Ke_{2i}, \quad U = \bigoplus_{i=0}^{\infty} Ke_{2i+1}, \quad W' = \bigoplus_{i=0}^{\infty} Ke_i, \quad U' = \{0\}.$$

Capítulo 3

Determinantes

3.1 Formas Multilineares

Definição 3.1. Seja V um espaço vetorial e $V^r = V \times \cdots \times V$. Uma **forma** r**-linear** sobre V é uma função $F : V^r \to K$ que é linear em cada argumento, ou seja, para cada $i = 1, \dots, r$ temos:

$$F(v_1, \dots, \alpha v_i + \beta v_i', \dots, v_r) = \alpha F(v_1, \dots, v_i, \dots, v_r) + \beta F(v_1, \dots, v_i', \dots, v_r).$$

Denotamos por $L_r(V)$ o conjunto das formas r-lineares sobre V.

Exemplo 3.2. Seja $V = K^2$ e:

$$F((x_1, y_1), (x_2, y_2), (x_3, y_3)) = x_1 y_2 x_3 - x_1 x_2 x_3.$$

Então F é uma forma 3-linear.

Definição 3.3. Uma forma $F \in L_r(V)$ chama-se **alternada** se e só se para $(v_1, \dots, v_r) \in V^r$ e $i < j$ tais que $v_i = v_j$ então $F(v_1, \dots, v_r) = 0$. Denotamos por $A_r(V)$ o conjunto das formas r-lineares alternadas.

Definição 3.4. Uma forma F é chamada **antissimétrica** se para $v \in V^r$ e para $i < j$ temos:

$$F(v_1, \dots, v_i, \dots, v_j, \dots, v_r) = -F(v_1, \dots, v_j, \dots, v_i, \dots, v_r).$$

Proposição 3.5. Toda forma alternada é antissimétrica.

Demonstração. Seja $F \in A_r(V)$. Sejam $v \in V^r$ e $i < j$, então:

$$\begin{aligned} 0 &= F(v_1, \dots, v_i + v_j, \dots, v_i + v_j, \dots, v_r) \\ &= F(v_1, \dots, v_i, \dots, v_i, \dots, v_r) + F(v_1, \dots, v_i, \dots, v_j, \dots, v_r) \\ &+ F(v_1, \dots, v_j, \dots, v_i, \dots, v_r) + F(v_1, \dots, v_j, \dots, v_j, \dots, v_r) \\ &= F(v_1, \dots, v_i, \dots, v_j, \dots, v_r) + F(v_1, \dots, v_j, \dots, v_i, \dots, v_r) \end{aligned}$$

□

Proposição 3.6. Se a característica do corpo é $\neq 2$, então toda forma antissimétrica é reflexiva.

Demonstração. Para F antissimétrica e $v \in V^r$ e $i < j$, se $v_i = v_j$, sendo $v = v_i$, então:

$$F(v_1, \dots, v, \dots, v, \dots, v_1) = -F(v_1, \dots, v, \dots, v, \dots, v_r),$$

aí:

$$2F(v_1, \dots, v, \dots, v, \dots, v_r) = 0,$$

aí:

$$F(v_1, \dots, v, \dots, v, \dots, v_r) = 0.$$

□

Definição 3.7. Seja $F \in L_r(V)$ e $\sigma \in S_r$ uma permutação. Para $(v_1, \dots, v_r) \in V^r$ definimos:

$$(\sigma F)(v_1, \dots, v_r) = F\left(v_{\sigma(1)}, \dots, v_{\sigma(r)}\right).$$

É fácil ver que $\sigma F \in L_r(V)$.

Observação 3.8. Para $F \in L_r(V)$, então F é antissimétrica se e somente se para toda transposição $\tau \in S_r$ tivermos $\tau F = -F$.

Proposição 3.9. Seja $F \in L_r(V)$ uma forma antissimétrica. Então para $\sigma \in S_r$, temos:

$$\sigma F = (\operatorname{sgn} \sigma) F.$$

Demonstração. Para $\sigma \in S_r$, então σ pode ser escrita como um produto de transposições:

$$\sigma = \tau_1 \dots \tau_k,$$

aí σ é par se e só se k é par. Portanto:

$$\sigma F = (\tau_1 \dots \tau_k) F = (-1)^k F = (\operatorname{sgn} \sigma) F,$$

pois $\operatorname{sgn} \sigma = (-1)^k$. □

Proposição 3.10. Toda forma r-linear determina uma forma r-linear alternada da seguinte maneira:

$$F \mapsto \varphi(F) = \sum_{\sigma \in S_r} (\operatorname{sgn} \sigma)(\sigma F).$$

Demonstração. Seja $v_i = v_j = v$ com $i < j$. Precisamos provar que $\varphi(F)(v) = 0$. Seja τ a transposição (i, j), então $S_r = A_r \cup A_r \tau$ e $A_r \cap A_r \tau = \emptyset$. Então temos o seguinte:

$$\begin{aligned}
\varphi(F)(v) &= \textstyle\sum_{\sigma \in S_r} (\operatorname{sgn} \sigma)(\sigma F(v)) \\
&= \textstyle\sum_{\sigma \in A_r} (\sigma F(v)) - \sum_{\sigma \in A_r} (\sigma \tau F(v)) \\
&= \textstyle\sum_{\sigma \in A_r} (\sigma F(v)) - \sum_{\sigma \in A_r} (\sigma F(v)) \\
&= 0.
\end{aligned}$$

□

Observação 3.11. Se $F \in A_r(V)$ e $v \in V^r$ é linearmente dependente, então:

$$F(v) = 0.$$

Lema 3.12. Seja $\dim V = n$ e $F \in A_n(V)$. Seja $(e_1, \dots, e_n)$ uma base de V, então F é completamente determinada pelo valor $F(e)$.

Demonstração. Seja $(v_1, \dots, v_n) \in V^n$. Então existe $(\alpha_{i,j}) \in M_n(K)$ tal que:

$$v_i = \sum_{j=1}^{n} \alpha_{i,j} e_j.$$

Assim:

$$\begin{aligned}
F(v_1, \dots, v_n) &= F\left(\sum_{j_1=1}^{n} \alpha_{1,j_1} e_{j_1}, \dots, \sum_{j_n=1}^{n} \alpha_{n,j_n} e_{j_n}\right) \\
&= \sum_{j_1, \dots, j_n = 1}^{n} \alpha_{1,j_1} \dots \alpha_{n,j_n} F\left(e_{j_1}, \dots, e_{j_n}\right) \\
&= \sum_{\sigma \in S_n} \alpha_{1,\sigma_1} \dots \alpha_{n,\sigma_n} F\left(e_{\sigma_1}, \dots, e_{\sigma_n}\right) \\
&= \left(\sum_{\sigma \in S_n} \alpha_{1,\sigma_1} \dots \alpha_{n,\sigma_n} \operatorname{sgn} \sigma\right) F(e_1, \dots, e_n).
\end{aligned}$$

□

Note então que o valor

$$\sum_{\sigma \in S_n} \alpha_{1,\sigma_1} \ldots \alpha_{n,\sigma_n} \operatorname{sgn} \sigma$$

determina F para qualquer $v \in V^n$. Chamaremos este valor de **determinante** de F.

Exemplo 3.13.

3.2 Determinantes

Seja K um corpo e consideremos o anel das matrizes $M_n(K)$. Identificaremos os elementos de $M_n(K)$ com os elementos de $(K^n)^n$ assim:

$$\begin{pmatrix} a_{1,1} & & a_{1,n} \\ & \ddots & \\ a_{n,1} & & a_{n,n} \end{pmatrix} \longleftrightarrow \left((a_{1,1}, \ldots, a_{1,n}), \ldots, (a_{n,1}, \ldots, a_{n,n})\right).$$

Portanto, uma função n-linear aqui é uma função n-linear nas linhas da matriz.

Definição 3.14. Uma função $\det : M_n(K) \to K$ é dita uma função **determinante** se e só se det é n-linear alternada e $\det(I) = 1$.

Pelo que vimos, existe e é única a função determinante: É a forma n-linear alternada que vale 1 na base canônica de K^n.

Logo, se $A = (a_{i,j}) \in M_n(K)$, então:

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma_1} \ldots a_{n,\sigma_n}.$$

Exemplo 3.15. Para $n = 2$, temos $S_2 = \{I, (1, 2)\}$, e assim, sendo:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix},$$

então temos:

$$\det(A) = a_{1,1}a_{2,2} - a_{1,2}a_{2,1}.$$

Exemplo 3.16. Agora, se $n = 3$, então $S_3 = \{I, (1, 2, 3), (1, 3, 2), (1, 2), (1, 3), (2, 3)\}$, e assim, sendo:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix},$$

então temos:

$$\det(A) = a_{1,1}a_{2,2}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} - a_{1,2}a_{2,1}a_{3,3} - a_{1,3}a_{2,2}a_{3,1} - a_{1,1}a_{2,3}a_{3,2}.$$

Proposição 3.17. Temos as seguintes propriedades:

1) Para todo $A \in M_n(K)$ temos $\det(A) = \det\left(A^t\right)$.

2) Para $A, B \in M_n(K)$ vale $\det(AB) = \det(A)\det(B)$.

3) Para $A \in M_n(K)$, então A é inversível se e só se $\det(A) \neq 0$. Neste caso, temos $\det\left(A^{-1}\right) = (\det(A))^{-1}$.

Demonstração. Temos o seguinte:

1) Sendo $A = (a_{i,j}) \in M_n(K)$, então temos:

$$\begin{aligned} \det(A) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \quad a_{1,\sigma_1} \dots a_{n,\sigma_n} \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \quad a_{\sigma_1^{-1},1} \dots a_{\sigma_n^{-1},n} \\ &= \sum_{\tau \in S_n} \operatorname{sgn}(\tau^{-1}) \quad a_{\tau_1,1} \dots a_{\tau_n,n} \\ &= \sum_{\tau \in S_n} \operatorname{sgn}(\tau) \quad a^t_{1,\tau_1} \dots, a^t_{n,\tau_n} \\ &= \det\left(A^t\right). \end{aligned}$$

2) Seja $F_A : M_n(K) \to K$ tal que $\forall X \in M_n(K) : F_A(X) = \det(AX)$. Então a função F_A é uma função n-linear alternada sobre as colunas, mas também $F_A(I) = \det(A)$, aí $F_A(B) = \det(A)\det(B)$, assim $\det(AB) = \det(A)\det(B)$

3) Se A é inversível, então existe a inversa A^{-1}, assim:

$$1 = \det(I) = \det\left(AA^{-1}\right) = \det(A)\det(A)^{-1},$$

aí $\det(A) \neq 0$ e $\det\left(A^{-1}\right) = (\det(A))^{-1}$. Por outro lado, se $\det(A) \neq 0$, então $\det\left(A^t\right) \neq 0$, aí as colunas de A são linearmente independentes, aí consideremos $T : K^n \to K^n$ tal que $[T]_{can} = A$, então T é inversível, assim $A = [T]_{can}$ é inversível.

□

Assim lembremo-nos do seguinte: a função det é uma função n-linear e alternada nas linhas (ou nas colunas) da matriz, logo:

1) Trocar duas linhas (ou colunas) da matriz muda o sinal do determinante.

2) Somar a uma linha (ou coluna) uma combinação linear das demais linhas (colunas) não altera o valor do determinante.

3) Ao multiplicar uma linha (ou coluna) por um escalar, o determinante fica multiplicado por esse escalar.

Proposição 3.18. Temos o seguinte:

1) O determinante de uma matriz triangular é o produto dos elementos da diagonal da matriz.

2) Se:

$$A = \begin{pmatrix} B & 0 \\ C & D \end{pmatrix}$$

em que $B \in M_r(K)$ e $D \in M_{n-r}(K)$ e $C \in M_{n-r,r}(K)$ e $0 \in M_{r,n-r}(K)$, então:

$$\det(A) = \det(B)\det(D).$$

Demonstração. Temos o seguinte:

1) Seja $A = (a_{i,j}) \in M_n(K)$ uma matriz triangular inferior, então para $i < j$ temos $a_{i,j} = 0$, mas a única permutação $\sigma \in S_n$ tal que para todo $i = 1, \dots, n$ tenhamos $i \geq \sigma_i$ é a permutação identidade I, assim temos:

$$\begin{aligned} \det(A) &= \textstyle\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma_1} \dots a_{n,\sigma_n} \\ &= \operatorname{sgn}(I) a_{1,I_1} \dots a_{n,I_n} \\ &= a_{1,1} \dots a_{n,n}. \end{aligned}$$

2) Seja $F : M_r(K) \to K$ tal que:

$$F(X) = \det \begin{pmatrix} X & 0 \\ C & D \end{pmatrix}.$$

Então F é r-linear alternada nas linhas de X, assim $F(X) = F(I)\det(X)$.

Agora consideremos $G : M_{n-r}(K) \to K$ tal que:

$$G(Y) = \det \begin{pmatrix} I & 0 \\ C & Y \end{pmatrix}$$

Então G é $(n-r)$-linear alternada nas colunas de Y, logo $G(Y) = G(I)\det(Y)$. Mas:

$$G(I) = \det \begin{pmatrix} I & 0 \\ C & I \end{pmatrix} = 1,$$

assim $G(Y) = \det(Y)$, aí $F(I) = G(D) = \det(D)$, assim $F(X) = F(I)\det(X) = \det(X)\det(D)$, aí acaba.

□

Agora temos a **regra de Laplace**:

Teorema 3.19. Dada $A = (a_{i,j}) \in M_n(K)$, indicaremos por $M_{i,j}$ a matriz quadrada de tamanho $n-1$ obtida a partir de A eliminando a linha i e a coluna j.
Para cada $i = 1, \dots, n$, então vale:

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{i,j} \det\left(M_{i,j}\right).$$

Para cada $j = 1, \dots, n$, então vale:

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{i,j} \det\left(M_{i,j}\right).$$

Demonstração. Provaremos a primeira afirmação pois a segunda é análoga. □

AULA DE 19 DE AGOSTO (COLOCAREI ASSIM QUE CONSEGUIR)

FICOU FALTANDO A PROVA DA REGRA DE LAPLACE E A PARTE DE MATRIZES SOBRE ANEIS COMUTATIVOS

Bláa blá blá

Capítulo 4

Formas Canônicas

4.1 Autovalores e Autovetores

Definição 4.1. Seja V um espaço vetorial sobre um corpo K e seja $T \in \mathcal{L}(V)$.

- Para $\lambda \in K$, dizemos que λ é um **autovalor** de T se existe um $v \neq 0$ tal que $T(v) = \lambda v$.
- Para $\lambda \in K$, um **autovetor** associado a λ é um $v \in V$ tal que $T(v) = \lambda v$.
- Para $\lambda \in K$, chamamos de **autoespaço** associado a λ o conjunto $V_T(\lambda)$ dos autovetores associados a λ.

Exemplo 4.2. Seja $V = \mathbb{C}^1(\mathbb{R})$ e considere o operador linear $T \in \mathcal{L}(V)$ tal que $T(v) = v'$ para cada $v \in V$. Considere $v = e^{\lambda x}$ com $\lambda \in K$. Então $T(v) = \lambda e^{\lambda x} = \lambda v$. Ou seja v é um autovetor associado a λ.

Definição 4.3. Seja V um espaço vetorial sobre um corpo K e seja $T \in \mathcal{L}(V)$. O **spectrum** do operador T é o conjunto:

$$\mathrm{Spec}(T) := \{\lambda \in K : \lambda \text{ é autovalor de } T\}.$$

No contexto da definição anterior, considere $\lambda \in \mathrm{Spec}(T)$. Então

$$\begin{aligned} v \in V_T(\lambda) &\iff T(v) = \lambda v \\ &\iff (T - \lambda I)(v) = 0 \\ &\iff v \in \mathrm{Ker}(T - \lambda I). \end{aligned}$$

Ainda no mesmo contexto, vamos assumir agora que $\dim(V) = n < \infty$. Então temos que

$$\lambda \in \mathrm{Spec}(T) \implies \mathrm{Ker}(T - \lambda I) \neq \{0\} \implies \det(T - \lambda I) = 0.$$

Reciprocamente, se $\det(T - \lambda I) = 0$ então $V_T(\lambda) = \mathrm{Ker}(T - \lambda I) \neq \{0\}$.

Definição 4.4. Seja V um espaço vetorial sobre um corpo K e seja $T \in \mathcal{L}(V)$. O **polinômio característico** de T é o polinômio:

$$p_T(t) := \det(tI - T).$$

Note que $\lambda \in \mathrm{Spec}(T)$ se e só se λ é raiz de $p_T(\lambda)$. Além disso, note que se B e B′ são bases V, então $p_T(\lambda) = p_{[T]_B}(\lambda)$. De fato, se P é a matriz de mudança da base B para a base B′, então

$$[\lambda I - T]_{B'} = P^{-1}[\lambda I - T]_B P$$

Isso implica que

$$\det([\lambda I - T]_{B'}) = \det(P^{-1})\det([\lambda I - T]_B)\det(P).$$

Ou seja,

$$\det([\lambda I - T]_{B'}) = \det([\lambda I - T]_B).$$

Exemplo 4.5. Seja $T \in \mathcal{L}(\mathbb{R}^2)$ tal que

$$[T]_{can} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Isto é, $T(x, y) = (-y, x)$ para cada $(x, y) \in \mathbb{R}^2$. Então

$$\begin{aligned} p_T(x) &= \det \begin{pmatrix} x & 1 \\ -1 & x \end{pmatrix} \\ &= x^2 + 1. \end{aligned}$$

Dessa forma, $\mathrm{Spec}(T) = \varnothing$ pois $p_T(x)$ não possui raízes em $K = \mathbb{R}$.

Exemplo 4.6. Seja $T \in \mathcal{L}(\mathbb{R}^3)$ tal que

$$[T]_{can} = \begin{pmatrix} 3 & 1 & -1 \\ 2 & 2 & -1 \\ 2 & 2 & 0 \end{pmatrix}.$$

Então:

$$\begin{aligned} p_T(x) &= \det \begin{pmatrix} x-3 & -1 & 1 \\ -2 & x-2 & 1 \\ -2 & -2 & x \end{pmatrix} \\ &= (x-1)^2(x-2). \end{aligned}$$

Isso implica que $\mathrm{Spec}(T) = \{1, 2\}$. Além disso, temos que

$$V_T(1) = \mathrm{Ker}(T - I) = \mathrm{Ker} \begin{pmatrix} 2 & 1 & -1 \\ 2 & 1 & -1 \\ 2 & 2 & -1 \end{pmatrix} = \langle (1, 0, 2) \rangle.$$

e ainda

$$V_T(2) = \mathrm{Ker}(T - 2I) = \mathrm{Ker} \begin{pmatrix} 1 & 1 & -1 \\ 2 & 0 & -1 \\ 2 & 2 & -2 \end{pmatrix} = \langle (1, 1, 2) \rangle$$

Exemplo 4.7. Seja $T \in \mathcal{L}(\mathbb{R}^3)$ tal que

$$[T]_{can} = \begin{pmatrix} 1 & 2 & -1 \\ -2 & -3 & -1 \\ 2 & 2 & -2 \end{pmatrix}.$$

Neste caso temos que

$$\begin{aligned} p_T(x) &= \det \begin{pmatrix} x-1 & -2 & 1 \\ 2 & x+3 & 1 \\ -2 & -2 & x+2 \end{pmatrix} \\ &= (x+1)^2(x+2). \end{aligned}$$

Isso implica que $\mathrm{Spec}(T) = \{-1, -2\}$ e ainda

$$V_T(-1) = \langle (1, 0, 2), (0, 1, 2) \rangle$$

e

$$V_T(-2) = \langle(1,-1,1)\rangle.$$

Uma vez que os autovetores acima são L.I, eles formam uma base B de $\mathbb{R}^3$ e

$$[T]_B = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

é uma matriz diagonal.

Teorema 4.8. Seja V um espaço vetorial sobre um corpo K tal que $\dim(V) = n < \infty$ e seja $T \in \mathcal{L}(V)$, e sejam $\lambda_1, \ldots, \lambda_k$ os autovalores distintos, e para $i = 1, \ldots, k$ seja $n_k = \dim V_T(\lambda_i)$. São equivalentes:

1. T é diagonalizável.

2. $p_T(t) = (t - \lambda_1)^{n_1} \ldots (t - \lambda_k)^{n_k}$.

3. $n_1 + \ldots + n_k = n$.

Lema 4.9. Sejam $\lambda_1, \ldots, \lambda_k \in K$ distintos. Então:

1. Se $v_i \in V_T(\lambda_i)$ para cada $i = 1, \ldots, k$ e $v_1 + \ldots + v_k = 0$, então $v_1 = \ldots = v_k = 0$.

2. Se $B_i \subseteq V_T(\lambda_i)$ é L.I para cada $i = 1, \ldots, k$, então $B_1 \cup \cdots \cup B_k$ é L.I.

Demonstração do Lema.

1. Vamos provar essa afirmação por indução em k. Primeiro note que o resultado é trivial quando $k = 1$. Agora seja $k \in \mathbb{N}$ e assuma que o resultado vale para cada natural $i < k$. Sejam $v_1, \ldots, v_k$ tais que $v_i \in V_T(\lambda_i)$ para cada $i = 1, \ldots, k$ e $v_1 + \ldots + v_k = 0$. Então:

$$0 = \lambda_1 0 = \lambda_1(v_1 + v_2 + \ldots + v_k) = \lambda_1 v_1 + \lambda_1 v_2 + \ldots + \lambda_1 v_k. \tag{4.1}$$

Além disso, é claro que:

$$0 = T(0) = T(v_1 + v_2 + \ldots + v_k) = \lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_k v_k. \tag{4.2}$$

Subtraindo a Equação 4.1 de 4.2, obtemos:

$$(\lambda_2 - \lambda_1)v_2 + \ldots + (\lambda_k - \lambda_1)v_k = 0. \tag{4.3}$$

Agora notamos que cada termo $(\lambda_i - \lambda_1)v_i$ no lado esquerdo é um autovetor de T associado a λ_i e aplicamos a hipótese de indução para concluir que $v_2 = \ldots = v_k = 0$. Finalmente, como sabemos que $v_1 + \ldots + v_k = 0$ e $v_2 = \ldots = v_k = 0$, obtemos que $v_1 = 0$ também, o que conclui nossa prova.

2. Seja $S \subseteq B_1 \cup \cdots \cup B_k$ finito e seja $\alpha\colon S \to \mathbb{R}$ tal que:

$$\sum_{v \in S} \alpha_v v = 0.$$

Note que $V_T(\lambda_i) \cap V_T(\lambda_j) = \{0\}$ sempre que e $i \neq j$ e então podemos escrever

$$\sum_{v \in S} \alpha_v v = \sum_{v \in S_1} \alpha_v v + \ldots + \sum_{v \in S_k} \alpha_v v,$$

onde $S_i \subseteq B_i$ é finito para cada $i = 1, \ldots, k$. Utilizando o fato de que:

$$\sum_{v \in S_i} \alpha_v v \in V_T(\lambda_i)$$

para cada $i = 1, \ldots, k$ e aplicando o item anterior, obtemos que

$$\sum_{v \in S_1} \alpha_v v = \ldots = \sum_{v \in S_k} \alpha_v v = 0.$$

Finalmente como como $S_i \subseteq B_i$ para cada $i = 1, \ldots, k$ e B_i é sempre L.I por hipótese segue que a restrição de α a cada S_i é identicamente nula. Como $S = S_1 \cup \cdots \cup S_k$, segue que α é indenticamente nula. □

Demonstração. Temos o seguinte:

- (i)⇒(ii): Seja B uma base tal que:

$$[T]_B = \begin{pmatrix} \lambda_1 I_{m_1} & & \\ & \ddots & \\ & & \lambda_k I_{m_k} \end{pmatrix},$$

em que $m_1, \ldots, m_k$ são inteiros positivos. Então o polinômio característico de T é:

$$p_T(t) = (t - \lambda_1)^{m_1} \ldots (t - \lambda_k)^{m_k}.$$

Além disso, para $i = 1, \ldots, k$, então a matriz de $T - \lambda_i I$ é igual a:

$$\begin{pmatrix} (\lambda_1 - \lambda_i) I_{m_1} & & & & \\ & \ddots & & & \\ & & 0_{m_i} & & \\ & & & \ddots & \\ & & & & (\lambda_k - \lambda_i) I_{m_k} \end{pmatrix},$$

aí é fácil ver que:

$$n_i = \dim V_T(\lambda_i) = \dim \operatorname{Ker}(T - \lambda_i I) = m_i,$$

ou seja, $n_i = m_i$; assim:

$$p_T(t) = (t - \lambda_1)^{n_1} \ldots (t - \lambda_k)^{n_k}.$$

- (ii)⇒(iii): O polinômio característico de T tem grau n, aí:

$$n_1 + \ldots + n_k = \deg(p_T(t)) = n.$$

- (iii)⇒(i): Para cada $i = 1, \ldots, k$ considere uma base B_i de $V_T(\lambda_i)$. Seja $B = B_1 \cup \cdots \cup B_k$. Pelo Lema 4.9, temos que B é L.I. Como $|B| = n$ segue que B é uma base de V. Além disso, B é uma base de autovetores de T. Logo, T é diagonalizável.

□

4.2 Polinômio Minimal

Definição 4.10. Seja V um espaço sobre K, $\dim V = n < \infty$, $T \in \mathcal{L}(V)$. Definamos por recursão $T^0 = I$ e $T^{k+1} = T^k \circ T$. Se $p(t) \in K[t]$, $p(t) = a_0 + a_1 t + \cdots + a_m t^m$, então está bem definido o operador $p(T) = a_0 \cdot I + a_1 \cdot I + \cdots + a_m \cdot T^m \in \mathcal{L}(V)$.

Lembremo-nos de que, se $\dim(U) = m$ e $\dim(V) = n$, então $\dim \mathcal{L}(U, V) = mn$. Assim, se V é um espaço vetorial tal que $\dim(V) = n < \infty$, então $\dim \mathcal{L}(V) = n^2$, de modo que existe $m \leq n^2 + 1$ tal que os operadores $I, T, T^2, \ldots, T^m$ sejam linearmente dependentes. Seja m o menor deles. Então existem $a_0, \ldots, a_{m-1} \in K$ tais que:

$$T^m + a_{m-1} T^{m-1} + \cdots + a_1 T + a_0 I = 0.$$

Seja:

$$m_T(t) = t^m + a_{m-1} t^{m-1} + \cdots + a_1 t + a_0,$$

então $m_T(T) = 0$, e $m_T(t)$ é um polinômio mônico de grau mínimo tal que $m_T(T) = 0$.

Definição 4.11. Um polinômio mônico de grau mínimo tal que $m_T(t) \in K[t]$ tal que $m_T(t) = 0$ chama-se um **polinômio minimal** do operador T.

Lema 4.12. Seja $f(t) \in K[t]$ tal que $f(T) = 0$. Então $m(t) \mid f(t)$.

Demonstração. Dividimos $f(t)$ por $m(t)$ (com resto):

$$f(t) = m_T(t) \cdot q(t) + r(t), \qquad \deg(r(t)) < \deg(m_T(t)) \text{ ou } r(t) = 0.$$

Como $f(T) = 0$ e $m_T(t) = 0$, então $r(T) = 0$, aí $r(t) = 0$. □

Corolário 4.13. O polinômio $m_T(t)$ é único.

Se V é um espaço vetorial e $T \in \mathcal{L}(V)$, então V tem uma estrutura de $K[t]$ módulo à esquerda: Se $f(t) \in K[t]$, para $v \in V$ definimos:

$$f(t) \cdot v = f(T)(v).$$

Além disso, se considerarmos:

$$\begin{aligned} \varphi : K[t] &\to \operatorname{End}(V) \\ f(t) &\mapsto f(T), \end{aligned}$$

então φ é um homomorfismo de K-álgebras e portanto $\operatorname{Ker}(\varphi)$ é um ideal de $K[t]$.

Teorema 4.14. Os polinômios $p_T(t)$ e $m_T(t)$ têm as mesmas raízes em K (a menos de multiplicidade). Em outras palavras, $m_T(\lambda) = 0 \Leftrightarrow \lambda \in \operatorname{Spec}(T)$.

Demonstração. Se $m_T(\lambda) = 0$, então $m_T(t) = (t - \lambda) q(t)$. Por minimalidade de $m_T(t)$, $q(T) \neq 0$, então existe $w \in V$ tal que $q(T)(w) \neq 0$, aí seja $v = q(T)(w)$, então $v \neq 0$ e:

$$\begin{aligned} (T - \lambda I)(v) &= (T - \lambda I) q(T)(w) \\ &= m_T(t)(w) = 0, \end{aligned}$$

aí $T(v) = \lambda v$, aí $\lambda \in \operatorname{Spec}(T)$.

Por outro lado, se $\lambda \in \operatorname{Spec}(T)$, seja $v \in V$ tal que $v \neq 0$ e $T(v) = \lambda v$, então:

$$T(T(v)) = \lambda^2 v, \ldots, T^m(v) = \lambda^m v, \ldots,$$

aí para $f(t) \in K[t]$ temos $f(T)(v) = f(\lambda) \cdot v$, aí $0 = m_T(T)(v) = m_T(\lambda) \cdot v$, aí $m_T(\lambda) = 0$. □

Corolário 4.15. Se T é diagonalizável e $\operatorname{Spec}(T) = \{\lambda_1, \ldots, \lambda_r\}$, então:

$$m_T(t) = (t - \lambda_1) \ldots (t - \lambda_r).$$

Demonstração. Já sabemos que:

$$m_T(t) = (t - \lambda_1)^{k_1} \dots (t - \lambda_r)^{k_r} q(t)$$

em que $q(t)$ não tem raízes em K. Seja

$$f(t) = (t - \lambda_1 I) \dots (t - \lambda_r I).$$

Seja $v \in V$, então $v = v_1 + \cdots + v_r$ para alguns $v_i \in V_T(\lambda_i)$, aí temos $(T - \lambda_i I)(v_i) = 0$, aí $f(T)(v_i) = 0$; logo $f(T)(v) = 0$. Portanto $f(T) = 0$, aí $m_T \mid f$, aí $m_T = f$. □

4.3 Subespaços Invariantes

Definição 4.16. Seja $T \in \mathcal{L}(V)$. Um subespaço $W \subseteq V$ chama-se T-**invariante** se $T(W) \subseteq W$.

Observação 4.17. Um subespaço é T-invariante se e só se é um $K[t]$-submódulo.

Exemplo 4.18. Seja $V = \mathbb{C}(\mathbb{R})$ e considere o operador $D \colon f \to f'$. Então o subespaço

$$P_n := \{f(t) \in \mathbb{R}[t] : \deg(f) \leq n\}$$

é D-invariante.

Proposição 4.19. Seja V um espaço vetorial de dimensão finita sobre um corpo K, seja $T \in \mathcal{L}(V)$ e seja W um subespaço T-invariante de V. Seja B_1 uma base de W e seja B uma base de V tal que $B_1 \subseteq B$. Então $B_2 = \{\overline{b} : b \in B \setminus B_1\}$ é uma base de V/W e, sendo $\overline{T} \in L(V/W)$ o operador induzido, temos:

$$[T]_B = \begin{pmatrix} [T\restriction_W]_{B_1} & * \\ 0 & [\overline{T}]_{B_2} \end{pmatrix},$$

Demonstração. Seja $\dim(V) = n$ e $T \in \mathcal{L}(V)$, e seja $W \subseteq V$ um subespaço T-invariante. Escolhemos uma base $B_1 = \{v_1, \dots, v_m\}$ de W e completemos uma base $B = \{v_1, \dots, v_m, v_{m+1}, \dots, v_n\}$ do espaço V. Qual é a matriz $[T]_B$?

Vamos começar notando que T é W-invariante e então:

$$\begin{aligned} T(v_1) &= \sum_{i=1}^{m} \alpha_{1,i} v_i \\ T(v_2) &= \sum_{i=1}^{m} \alpha_{2,i} v_i \\ &\vdots \\ T(v_m) &= \sum_{i=1}^{m} \alpha_{m,i} v_i \\ T(v_{m+1}) &= \sum_{i=1}^{n} \alpha_{m+1,i} v_i \\ &\vdots \\ T(v_n) &= \sum_{i=1}^{n} \alpha_{n,i} v_i. \end{aligned}$$

Dessa forma segue que:

$$[T]_B = \begin{pmatrix} \alpha_{1,1} & \dots & \alpha_{1,m} & \alpha_{1,m+1} & \dots & \alpha_{1,n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \alpha_{m,1} & \dots & \alpha_{m,m} & \alpha_{m,m+1} & \dots & \alpha_{m,n} \\ 0 & \dots & 0 & \alpha_{m+1,m+1} & \dots & \alpha_{m+1,n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \alpha_{n,m+1} & \dots & \alpha_{n,n} \end{pmatrix}.$$

Isto é, a matriz de T na base B tem a forma:

$$[T]_B = \begin{pmatrix} X & * \\ 0 & Y \end{pmatrix},$$

onde $X \in M_m(K)$ e $Y \in M_{n-m}(K)$. Note que X é a matriz da restrição de T a W na base B_1. Além disso, temos o seguinte:

$$\begin{aligned} \bar{T}(\bar{v}_{m+1}) &= \sum_{i=m+1}^{n} \alpha_{m+1,i}\bar{v}_i \\ &\vdots \\ \bar{T}(\bar{v}_n) &= \sum_{i=m+1}^{n} \alpha_{n,i}\bar{v}_i. \end{aligned}$$

Portanto Y é a matriz da transformação $\bar{T}$ na base $\{\bar{v}_{m+1}, \ldots, \bar{v}_n\}$. □

Lema 4.20. Seja $\dim(V) = n$, $T \in \mathcal{L}(V)$ e $W \subseteq V$ um subespaço T-invariante. Então:

$$p_T(t) = p_{T\restriction_W}(t) \cdot p_{\bar{T}}(t)$$

em que $\bar{T}$ é o operador induzido em V/W.

Demonstração. Escolhamos B_1 e B como bases de W e V tais que $B_1 \subseteq B$, então, considerando $B_2 = \{\bar{b} : b \in B \setminus B_1\}$, a matriz de T na base B tem a forma:

$$Z = \begin{pmatrix} X & * \\ 0 & Y \end{pmatrix},$$

onde X é a matriz de $T\restriction_W$ em relação a B_1 e Y é a matriz de $\bar{T}$ em relação a B_2, assim:

$$\begin{aligned} p_T(t) &= p_Z(t) \\ &= \det(tI - Z) \\ &= \det\begin{pmatrix} tI_m - X & * \\ 0 & tI_{n-m} - Y \end{pmatrix} \\ &= \det(tI_m - X)\det(tI_{n-m} - Y) \\ &= p_X(t)p_Y(t) \\ &= p_{T\restriction_W}(t)p_{\bar{T}}(t) \end{aligned}$$ □

Observação 4.21. O mesmo não ocorre para polinômios minimais. De fato, seja $T = I_V$ e seja W um subespaço T-invariante (De fato, quando T é a identidade, todo subespaço de V é T-invariante), então $T_1 = I_W$ e $T_2 = I_{V/W}$ e aí $m_T(t) = m_{T_1}(t) = m_{T_2}(t) = t - 1$. Não obstante, ainda temos um resultado interessante para isso.

Lema 4.22. Seja $\dim(V) = n$, $T \in \mathcal{L}(V)$ e $W \subseteq V$ um subespaço T-invariante. Então:

$$m_{T\restriction_W}(t) \mid m_T(t), \quad m_{\bar{T}}(t) \mid m_T(t),$$

em que $\bar{T}$ é o operador induzido em V/W.

Demonstração. Escolhamos B_1 e B como bases de W e V tais que $B_1 \subseteq B$, então, considerando $B_2 = \{\bar{b} : b \in B \setminus B_1\}$, a matriz de T na base B tem a forma:

$$Z = \begin{pmatrix} X & * \\ 0 & Y \end{pmatrix},$$

onde X é a matriz de $T\restriction_W$ em relação a B_1 e Y é a matriz de $\bar{T}$ em relação a B_2, assim é fácil de mostrar por indução que para todo $k \geq 0$ então temos uma matriz da forma:

$$Z^k = \begin{pmatrix} X^k & * \\ 0 & Y^k \end{pmatrix},$$

assim temos uma matriz é da forma:

$$m_T(Z) = \begin{pmatrix} m_T(X) & * \\ 0 & m_T(Y) \end{pmatrix},$$

mas sabemos que $m_T(Z) = 0$, aí $m_T(X) = 0$ e $m_T(Y) = 0$, aí a conclusão segue. □

4.4 Subespaços Cíclicos

Definição 4.23. Seja V um espaço vetorial e $T \in \mathcal{L}(V)$. Para $v \in V$, definimos o **subespaço T-cíclico gerado por** v como o conjunto $Z(v, T)$ de todos os vetores da forma $p(T)(v)$ em que $p \in K[x]$. Dizemos que v é um **vetor cíclico** para T se e só se $Z(v, T) = V$.

Proposição 4.24. Seja V um espaço vetorial e seja $T \in \mathcal{L}(V)$. Para $v \in V$, então $Z(v, T)$ é o subespaço gerado pelo conjunto $\{T^n(v) : n \in \mathbb{N}\}$.

Definição 4.25. Dado $v \in V$, um polinômio mônico de grau mínimo $m_{T,v}(t) \in K[t]$ tal que $m_{T,v}(T)(v) = 0$ chama-se um **polinômio T-anulador** do vetor v.

Lema 4.26. Seja $f(t) \in K[t]$ tal que $f(T)(v) = 0$. Então $m_{T,v}(t) \mid f(t)$.

Demonstração. Dividimos $f(t)$ por $m_{T,v}(t)$ (com resto):

$$f(t) = m_{T,v}(t) \cdot q(t) + r(t), \qquad \deg(r(t)) < \deg(m_{T,v}(t)) \text{ ou } r(t) = 0.$$

Como $f(T)(v) = 0$ e $m_{T,v}(T)(v) = 0$, então $r(T)(v) = 0$, aí $r(t) = 0$. □

Corolário 4.27. O polinômio $m_{T,v}(t)$ é único.

Teorema 4.28. Seja V um espaço vetorial e $T \in \mathcal{L}(V)$. Seja $v \in V$ que possua um polinômio T-anulador, e consideremos o polinômio $m_{T,v}$. Então:

- O grau de $m_{T,v}$ é igual à dimensão de $Z(v, T)$.
- Se o grau de $m_{T,v}$ é k, então $v, T(v), \dots, T^{k-1}(v)$ formam uma base de $Z(v, T)$.
- Se $W = Z(v, T)$, então $m_{T\restriction_W} = m_{T,v}$.

O teorema seguinte mostra como subespaços cíclicos podem ser compostos e decompostos.

Teorema 4.29. Seja V um espaço vetorial e $T \in \mathcal{L}(V)$.

- (Compondo subespaços cíclicos) Se $u_1, \dots, u_n \in V$ tem T-anuladores mutuamente primos entre si, então o T-anulador de $u = u_1 + \cdots + u_n$ é:

  $$m_{T,u} = m_{T,u_1} \dots m_{T,u_n}$$

  e também:

  $$Z(u, T) = Z(u_1, T) \oplus \cdots \oplus Z(u_n, T).$$

- (Decompondo subespaços cíclicos) Se $m_{T,u} = f_1 \dots f_n$ com $f_1, \dots, f_n$ mutuamente primos entre si, então u tem a forma:

  $$u = u_1 + \cdots + u_n,$$

  em que $m_{T,u_i} = f_i$, e também:

  $$Z(u, T) = Z(u_1, T) \oplus \cdots \oplus Z(u_n, T).$$

4.5 Teorema de Cayley-Hamilton

Teorema 4.30 (Teorema da Cayley-Hamilton)**.** Seja V um espaço vetorial de dimensão finita sobre um corpo K, e seja $T \in \mathcal{L}(V)$. Então $p_T(T) = 0$, onde $p_T(t) \in K[t]$ é um polinômio característico de T.

Demonstração. Basta provar que $\forall v \in V : p_T(T)(v) = 0$. Seja $v \in V$. Consideremos:

$$m_{T,v}(t) = t^m + \alpha_{m-1}t^{m-1} + \cdots + \alpha_1 t + \alpha_0,$$

o polinômio mônico de menor grau tal que $m_{T,v}(T)(v) = 0$. Então $B_1 = \{v, T(v), \ldots, T^{m-1}(v)\}$ é linearmente independente. Seja W o subespaço gerado por ele. Note que W é T-invariante e ainda:

$$[T \restriction_W]_{B_1} = \begin{pmatrix} 0 & 0 & \ldots & 0 & -\alpha_0 \\ 1 & 0 & \ldots & 0 & -\alpha_1 \\ 0 & 1 & \ldots & 0 & -\alpha_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & -\alpha_{m-1} \end{pmatrix}$$

Então, pelo Exercício 18 da lista 1, segue que:

$$p_{T\restriction_W}(t) = t^m + \alpha_{m-1}t^{m-1} + \ldots + \alpha_1 t + \alpha_0.$$

Aplicando essa função a v segue:

$$p_{T\restriction_W}(T)(v) = m_{T,v}(T)(v) = 0.$$

Para concluir que $p_T(T)(v) = 0$, notamos que $p_T(t) = p_{T\restriction_W}(t) \cdot p_{\bar{T}}(t)$, em que $\bar{T}$ é o operador induzido em V/W. □

Corolário 4.31. Se $A \in M_n(K)$ então $p_A(A) = 0$, onde $p_A(t) = \det(tI - A)$.

Exemplo 4.32. Considere a matriz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Então temos que $p_A(t) = t^2 - (a + d)t + (ad - bc)$ e também

$$\begin{aligned} P_A(A) &= A^2 - (a + d)A + (ad - bc)I \\ &= \begin{pmatrix} a^2 + bc & ab + ad \\ ac + dc & bc + d^2 \end{pmatrix} - \begin{pmatrix} a^2 + ad & ab + bd \\ ac + dc & ad + d^2 \end{pmatrix} + \det(A)I \\ &= \begin{pmatrix} bc - ad & 0 \\ 0 & bc - ad \end{pmatrix} + \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} = 0. \end{aligned}$$

Teorema 4.33 (Teorema da Cayley-Hamilton ao Avesso)**.** Se V é espaço de dimensão finita e $T \in L(V)$, então todo polinômio irredutível que divide p_T também divide m_T.

Demonstração. Faremos a demonstração por indução na dimensão de V. Suponhamos o lema válido para $\dim(V) < n$. Seja V espaço vetorial tal que $\dim(V) = n$ e seja $T \in L(V)$ e seja p um polinômio irredutível que divide p_T. Se $V = 0$, é fácil. Senão, então tome um $v \neq 0$ qualquer. Consideremos:

$$m_{T,v}(t) = t^m + \alpha_{m-1}t^{m-1} + \cdots + \alpha_1 t + \alpha_0,$$

o polinômio mônico de menor grau tal que $m_{T,v}(T)(v) = 0$. Então $B_1 = \{v, T(v), \dots, T^{m-1}(v)\}$ é linearmente independente. Seja W o subespaço gerado por ele. Note que W é T-invariante e ainda:

$$[T\restriction_W]_{B_1} = \begin{pmatrix} 0 & 0 & \dots & 0 & -\alpha_0 \\ 1 & 0 & \dots & 0 & -\alpha_1 \\ 0 & 1 & \dots & 0 & -\alpha_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & -\alpha_{m-1} \end{pmatrix}$$

Então, pelo Exercício 18 da lista 1, segue que:

$$p_{T\restriction_W}(t) = t^m + \alpha_{m-1}t^{m-1} + \dots + \alpha_1 t + \alpha_0.$$

Além disso, vendo a definição de $m_{T,v}$, é fácil ver que:

$$m_{T\restriction_W}(t) = t^m + \alpha_{m-1}t^{m-1} + \dots + \alpha_1 t + \alpha_0.$$

Sendo $\overline{T} \in L(V/W)$ o operador induzido, temos $p_T = p_{T\restriction_W} p_{\overline{T}}$ e $m_{T\restriction_W} \mid m_T$ e $m_{\overline{T}} \mid m_T$. Assim, como $p \mid p_T$, então $p \mid p_{T\restriction_W}$ ou $p \mid p_{\overline{T}}$.

- Se $p \mid p_{T\restriction_W}$, como $p_{T\restriction_W} = m_{T\restriction_W}$, então $p \mid m_{T\restriction_W}$, aí $p \mid m_T$.
- Se $p \mid p_{\overline{T}}$, então, por hipótese de indução, temos $p \mid m_{\overline{T}}$, aí $p \mid m_T$. □

4.6 Decomposições Primárias

Teorema 4.34 (Decomposição Primária Geral)**.** Seja V um espaço vetorial sobre um corpo K tal que $\dim(V) = n < \infty$ e seja $T \in \mathcal{L}(V)$. Suponhamos que $f(T) = 0$ e também:

$$f = f_1 \dots f_r,$$

com $f_1, \dots, f_r$ mutuamente primos entre si. Para cada i seja $V_i = \text{Ker } f_i(T)$. Então:

- Cada V_i é T-invariante.
- $V = V_1 \oplus \dots \oplus V_r$.
- Cada projeção canônica $P_i : V \to V_i$ é um polinômio de T.

Lema 4.35 (Identidade de Bézout)**.** Se $\text{mdc}(f_1, \dots, f_r) = 1$ então existem $g_1, \dots, g_r \in K[t]$ tais que:

$$f_1 g_1 + \dots + f_r g_r = 1.$$

Demonstração do Teorema. Para cada i, então para $v \in V_i$ temos $f_i(T)(v) = 0$, aí $Tf_i(T)(v) = 0$, aí $f_i(T)T(v) = 0$, aí $T(v) \in V_i$; logo V_i é T-invariante. Agora para cada i seja:

$$h_i = \frac{f}{f_i}.$$

Então $\text{mdc}(h_1, \dots, h_r) = 1$, assim existem $g_1, \dots, g_r \in K[t]$ tais que:

$$h_1 g_1 + \dots + h_r g_r = 1,$$

aí:

$$h_1(T)g_1(T) + \dots + h_r(T)g_r(T) = I.$$

Para $v_1, \dots, v_r \in V$, se para todo i tivermos $v_i \in V_i$ e:

$$v_1 + \dots + v_r = 0,$$

então para cada i temos:

$$h_i(T)(v_1) + \cdots + h_i(T)(v_r) = 0,$$

mas para cada $j \neq i$ então $f_j \mid h_i$, aí $h_i(T)(v_j) = 0$; assim:

$$h_i(T)(v_i) = 0,$$

mas:

$$v_i = h_1(T)g_1(T)(v_i) + \cdots + h_r(T)g_r(T)(v_i),$$

e para cada $j \neq i$ temos $f_i \mid h_j$, aí $h_j(T)(v_i) = 0$; assim:

$$v_i = h_i(T)g_i(T)(v_i) = 0;$$

portanto:

$$v_1 = \cdots = v_r = 0.$$

Para todo $v \in V$ então:

$$v = h_1(T)g_1(T)(v) + \cdots + h_r(T)g_r(T)(v),$$

e para cada i temos:

$$f_i(T)h_i(T)g_i(T)(v) = f(T)g_i(T)(v) = 0,$$

aí:

$$h_i(T)g_i(T)(v) \in V_i;$$

logo:

$$V = V_1 \oplus \cdots \oplus V_r,$$

e, para cada i, a função $h_i(T)g_i(T)$ é a projeção canônica de V em V_i. □

Teorema 4.36 (Decomposição Primária para Minimais)**.** Seja V um espaço vetorial sobre um corpo K tal que $\dim(V) = n < \infty$ e seja $T \in \mathcal{L}(V)$, e seja:

$$m_T = p_1^{k_1} \dots p_r^{k_r},$$

com $p_1 \dots, p_r$ irredutíveis e mutuamente primos entre si. Para cada i seja $V_i = \operatorname{Ker} \, p_i(T)^{k_i}$. Então:

- Cada V_i é T-invariante.
- $V = V_1 \oplus \cdots \oplus V_r$.
- Cada projeção canônica $P_i : V \to V_i$ é um polinômio de T.
- Para cada i então $m_{T\restriction_{V_i}} = p_i^{k_i}$.

Demonstração. Por definição temos $m_T(T) = 0$. Logo, pelo teorema da decomposição primária geral, temos os três primeiros itens. Agora considere $T_i \coloneqq T \restriction_{V_i}$ para cada $i = 1, \dots, r$. Temos que $p_i(T_i)^{k_i} = 0$. Então segue que $m_{T_i} \mid p_i^{k_i}$, ou seja, $m_{T_i} = p_i^{m_i}$, onde $m_i \leq k_i$. Consideremos:

$$g = p_1^{k_1} \dots p_i^{m_i} \dots p_r^{k_r}.$$

Para $j \neq i$ e para $v \in V_j$, então $p_j^{k_j}(v) = 0$ e portanto $g(T)(v) = 0$. Se $v \in V_i$ então $p_i^{m_i}(T)(v) = 0$ e $g(T)(v) = 0$. Assim, como $V = V_1 \oplus \cdots \oplus V_r$, concluímos que $g(T) = 0$. Isso implica que $m_T \mid g$, aí $p_i^{k_i} \mid p_i^{m_i}$, aí $k_i \leq m_i$, assim $m_i = k_i$, aí $m_{T_i} = p_i^{k_i}$. □

Teorema 4.37 (Decomposição Primária para Característicos)**.** Seja V um espaço vetorial sobre um corpo K tal que $\dim(V) = n < \infty$ e seja $T \in \mathcal{L}(V)$, e seja:

$$p_T = p_1^{k_1} \dots p_r^{k_r},$$

com $p_1 \dots, p_r$ irredutíveis e mutuamente primos entre si. Para cada i seja $V_i = \operatorname{Ker} \, p_i(T)^{k_i}$. Então:

- Cada V_i é T-invariante.
- $V = V_1 \oplus \cdots \oplus V_r$.
- Cada projeção canônica $P_i : V \to V_i$ é um polinômio de T.
- Para cada i então $p_{T\restriction_{V_i}} = p_i^{k_i}$.

Demonstração. Pelo teorema de Cayley-Hamilton temos $p_T(T) = 0$. Portanto, pelo teorema da decomposição primária geral, temos os três primeiros itens. Agora considere $T_i := T\restriction_{V_i}$ para cada $i = 1, \ldots, r$. Temos que $p_i(T_i)^{k_i} = 0$. Então segue que $m_{T_i} \mid p_i^{k_i}$, aí, pelo teorema de Cayley-Hamilton ao avesso (Teorema 4.33), todo fator irredutível de p_{T_i} deve dividir m_{T_i}, logo ser igual a p_i. Assim $p_{T_i} = p_i^{l_i}$ para algum l_i. Entretanto, considerando bases B_i de V_i, e juntando numa base B de V, é fácil ver que $p_T = p_{T_1} \ldots p_{T_k}$, assim $p_T = p_1^{l_1} \ldots p_r^{l_r}$, aí pela fatoração única devemos ter $l_i = k_i$ para todo i, concluindo a demonstração. □

A decomposição primária para minimais também goza de uma propriedade muito importante para o estudo da álgebra linear.

Teorema 4.38 (Unicidade da Decomposição Primária para Minimais)**.** Seja V um espaço vetorial e seja $T \in \mathcal{L}(V)$. Suponhamos que:

$$V = U_1 \oplus \cdots \oplus U_m$$

em que U_i é um subespaço T-invariante tal que $m_{T\restriction_{U_i}} = p_i^{e_i}$ e $p_1, \ldots, p_m$ são polinômios mônicos irredutíveis distintos, e suponhamos que:

$$V = W_1 \oplus \cdots \oplus W_n$$

em que W_j é um subespaço T-invariante tal que $m_{T\restriction_{W_j}} = q_j^{f_j}$ e $q_1, \ldots, q_n$ são polinômios mônicos irredutíveis distintos. Então $m = n$ e, depois de uma reindexação adequada, $U_k = W_k$ para todo k. Portanto $p_k = q_k$ e $e_k = f_k$ para todo k.

Demonstração. Para todo i, então U_i contém um elemento u_i tal que $m_{T,u_i} = p_i^{e_i}$; assim, definindo a soma $u = u_1 + \cdots + u_m$, então $m_{T,u} = p_1^{e_1} \ldots p_m^{e_m}$. Logo $m_T = p_1^{e_1} \ldots p_m^{e_m}$. Analogamente temos $m_T = q_1^{f_1} \ldots q_n^{f_n}$.

Portanto, pela fatoração única em K[t], então $m = n$ e, depois de uma reindexação apropriada, temos $p_k = q_k$ e $e_k = f_k$ para todo k. Para todo k, temos:

$$U_k \subseteq \operatorname{Ker}\ p_k(T)^{e_k},$$

mas pela decomposição primária geral temos:

$$U_1 \oplus \cdots \oplus U_m = \left(\operatorname{Ker}\ p_1(T)^{e_1}\right) \oplus \cdots \oplus \left(\operatorname{Ker}\ p_m(T)^{e_m}\right),$$

aí para todo k temos $U_k = \operatorname{Ker}\ p_k(T)^{e_k}$. Analogamente temos $W_k = \operatorname{Ker}\ q_k(T)^{f_k}$ para todo k. □

4.7 Critérios de Diagonalização

Teorema 4.39. Um operador $T \in \mathcal{L}(V)$ é diagonalizável se, e somente se:

$$m_T(t) = (t - \lambda_1) \ldots (t - \lambda_r)$$

com $\lambda_i \neq \lambda_j$ sempre que $i \neq j$.

Demonstração. A ida já foi provada no corolário 4.15, então vamos mostrar apenas a volta. Pelo teorema da decomposição primária geral, sendo $V_i = \text{Ker } (T - \lambda_i I)$ para todo i, então cada V_i é T-invariante e $V = V_1 \oplus \ldots \oplus V_r$, aí para todo i temos $T \restriction_{V_i} = \lambda_i I$, aí $V_i \subseteq V_T(\lambda_i)$; logo T é diagonalizável. □

Considere $\{T_i : i \in I\} \subseteq \mathcal{L}(V)$. Em que condições os operadores T_i podem ser diagonalizados simultaneamente, ou seja, existe base B de V tal que para todo $i \in I$ a matriz $[T_i]_B$ seja diagonal?

Teorema 4.40. Um conjunto $\{T_i : i \in I\}$ pode ser diagonalizado simultaneamente se, e somente se cada T_i é diagonalizável e $T_i T_j = T_j T_i$ para todo $i, j \in I$.

Demonstração. Mostraremos por indução na dimensão. Suponhamos que o teorema é válido para espaços de dimensão menor que n. Seja V um espaço tal que $\dim(V) = n$ e seja $\mathcal{F}$ um conjunto de operadores que comutam um com outro. Se todo elemento de $\mathcal{F}$ é múltiplo da identidade, então acaba. Caso contrário, existe um $T \in \mathcal{F}$ que não é múltiplo da identidade. Sejam $c_1, \ldots, c_k$ os autovalores de T. Para i seja $W_i = \text{Ker}(T - c_i I)$. Então, como os elementos de $\mathcal{F}$ comutam um com outro, então W_i é invariante para todo elemento de $\mathcal{F}$. Para cada $U \in \mathcal{F}$, então m_U é produto de fatores lineares distintos, aí, como $m_{U \restriction_{W_i}} \mid m_U$, então $m_{U \restriction_{W_i}}$ é produto de fatores lineares distintos, aí $U \restriction_{W_i}$ é diagonalizável. Como $\dim(W_i) < n$, então existe uma base B_i tal que para todo $U \in \mathcal{F}$ a matriz $[U \restriction_{W_i}]_{B_i}$ seja diagonal. Portanto $B = B_1 \cup \cdots \cup B_k$ é a base que buscamos. □

4.8 Triangularização de Matrizes

4.9 Decomposições Cíclicas

O seguinte teorema mostra como podemos decompor um espaço vetorial anulável por uma potência de polinômio irredutível em subespaços cíclicos.

Teorema 4.41 (Decomposição Cíclica de Espaços Primários)**.** Seja V um espaço vetorial com *dimensão finita* e seja $T \in \mathcal{L}(V)$ tal que $m_T = p^e$, em que p é um polinômio irredutível. Então V é uma soma direta:

$$V = Z(v_1, T) \oplus \cdots \oplus Z(v_n, T)$$

de subespaços cíclicos com anuladores $m_{T,v_i} = p^{e_i}$, que podem ser arranjados em ordem decrescente:

$$e = e_1 \geq e_2 \geq \cdots \geq e_n.$$

Demonstração. Seja $v_1 \in V$ um vetor com anulador igual a polinômio minimal de T, ou seja:

$$m_{T,v_1} = m_T = p^e.$$

Tal elemento deve existir pois $m_{T,v} \mid m_T$ para todo $v \in V$ e se ninguém tiver anulador igual a $p(t)^e$, então $p(t)^{e-1}$ anulará V.

Se mostrarmos que $Z(v_1, T)$ possui complemento T-invariante, ou seja, $V = Z(v_1, T) \oplus S_1$ para algum subespaço T-invariante S_1, então, como S_1 tem dimensão finita sobre K, ao considerarmos $T \restriction_{S_1}$, podemos repetir o processo para obter:

$$V = Z(v_1, T) \oplus Z(v_2, T) \oplus S_2$$

em que $m_{T,v_i} = p^{e_i}$. Podemos continuar esta decomposição:

$$V = Z(v_1, T) \oplus Z(v_2, T) \oplus \cdots \oplus Z(v_n, T) \oplus S_n$$

enquanto $S_n \neq 0$. Mas a sequência ascendente de subespaços T-invariantes:

$$Z(v_1, T) \subseteq Z(v_1, T) \oplus Z(v_2, T) \subseteq \ldots$$

deve terminar pois a sequência das dimensões é estritamente crescente e V tem dimensão finita, assim existe um inteiro n tal que $S_n = 0$, fornecendo-nos a decomposição buscada.

Seja $v = v_1$. A soma direta de subespaços T-invariantes $V_1 = Z(v, T) \oplus 0$ claramente existe. Suponhamos que a soma direta de subespaços T-invariantes:

$$V_k = Z(v, T) \oplus W_k$$

exista. Afirmamos que, se $V_k \neq V$, então é possível encontrar um subespaço T-invariante W_{k+1} que contenha propriamente W_k e para o qual a soma direta $V_{k+1} = Z(v, T) \oplus W_{k+1}$ exista. Esta processo deve também terminar após um número finito de passos, fornecendo-nos uma decomposição em soma direta de subespaços T-invariantes:

$$V = Z(v, T) \oplus W$$

como desejado.

Se $V_k \neq V$, então seja $u \in V \setminus V_k$, aí o polinômio de menor grau r tal que $r(T)(u) \in V_k$ deve ser p^f para algum $f \leq e$. Além disso, como $u \notin V_k$, então $f > 0$. Assim existem $a(t) \in K[t]$ e $w \in W_k$ tais que:

$$p(T)^f(u) = a(T)(v) + w.$$

Logo:

$$0 = p(T)^e(u) = p(T)^{e-f}p(T)^f(u) = p(T)^{e-f}(a(T)(v) + w) = p(T)^{e-f}a(T)(v) + p(T)^{e-f}(w).$$

Como $Z(v, T) \cap W_k = 0$ então $p(T)^{e-f}a(T)(v) = 0$, aí $p^e \mid p^{e-f}a$, aí $p^f \mid a$, aí existe $\alpha(t) \in K[t]$ tal que $a = p^f\alpha$, assim:

$$p(T)^f(u) = a(T)(v) + w = p(T)^f\alpha(T)(v) + w,$$

aí:

$$p(T)^f(u - \alpha(T)(v)) \in W_k.$$

Assim seja:

$$W_{k+1} = W_k + Z\left(u - \alpha(T)(v), T\right).$$

Para $x \in Z(v, T) \cap W_{k+1}$, então existem $f(t) \in K[t]$ e $g(t) \in K[t]$ e $w \in W_k$ tais que:

$$x = f(T)(v) = w + g(T)(u - \alpha(T)(v)),$$

aí:

$$g(T)(u) = (f - g\alpha)(T)(v) - w \in V_k,$$

aí $p^f \mid g$, aí:

$$g(T)(u - \alpha(T)(v)) \in W_k,$$

aí:

$$x \in Z(v, T) \cap W_k,$$

aí $x = 0$. Logo a soma direta de subespaços T-invariantes:

$$V_{k+1} = Z(v, T) \oplus W_{k+1}$$

existe. □

A decomposição cíclica de espaços primários, assim como a decomposição primária para minimais, goza da propriedade da unicidade.

Teorema 4.42 (Unicidade da Decomposição Cíclica de Espaços Primários)**.** Seja V um espaço vetorial e seja $T \in \mathcal{L}(V)$. Suponhamos que V é uma soma direta:

$$V = Z(u_1, T) \oplus \cdots \oplus Z(u_m, T),$$

em que $m_{T,u_i} = p_i^{e_i}$ e também:

$$e_1 \geq e_2 \geq \cdots \geq e_m,$$

e também suponhamos que V é uma soma direta:

$$V = Z(v_1, T) \oplus \cdots \oplus Z(v_n, T),$$

em que $m_{T,v_j} = q_j^{f_j}$ e também:

$$f_1 \geq f_2 \geq \cdots \geq f_n.$$

Então $m = n$ e $p = q$ e $e_k = f_k$ para todo k.

Lema 4.43. Seja V um espaço vetorial e $T \in \mathcal{L}(V)$ e seja $p(t)$ um polinômio irredutível.

- Se $p(T) = 0$, então V é um espaço vetorial sobre o corpo $K[t]/p(t)K[t]$ com a multiplicação definida por:

  $$\bar{r}(v) = r(T)v$$

  para quaisquer $r(t) \in K[t]$ e $v \in V$.

- Para qualquer subespaço T-invariante W de V o conjunto:

  $$W \cap \mathrm{Ker}\ p(T) = \{v \in W : p(T)(v) = 0\}$$

  é um subespaço T-invariante de V e se $V = U \oplus W$, então:

  $$\mathrm{Ker}\ p(T) = \big(U \cap \mathrm{Ker}\ p(T)\big) \oplus \big(W \cap \mathrm{Ker}\ p(T)\big).$$

Demonstração do Teorema. Primeiro notemos que $m_T = p_1^{e_1}$ e $m_T = q_1^{f_1}$. Assim $p = q$ e $e_1 = f_1$. Agora mostraremos que $m = n$. De acordo com o lema anterior, sendo $W = \mathrm{Ker} p(T)$, então:

$$W = \big(W \cap Z(u_1, T)\big) \oplus \cdots \oplus \big(W \cap Z(u_m, T)\big)$$

e também:

$$W = \big(W \cap Z(v_1, T)\big) \oplus \cdots \oplus \big(W \cap Z(v_n, T)\big).$$

Como $p(T)[W] = 0$, então W é um espaço vetorial sobre o corpo $L = K[t]/p(t)K[t]$ e aí cada uma das duas decomposições expressa W como uma soma direta de subespaços de dimensão 1. Logo $m = \dim_L(W) = n$.

Finalmente mostraremos que os expoentes e_i e f_i são iguais usando indução em e_1. Se $e_1 = 1$, então $e_i = 1$ para todo i e como $f_1 = e_1$, temos também $f_i = 1$ para todo i. Suponhamos que o resultado seja válido para $e_1 \leq k - 1$ e seja $e_1 = k$. Escreva:

$$(e_1, \ldots, e_n) = (e_1, \ldots, e_s, 1, \ldots, 1), \quad e_s > 1$$

e

$$(f_1, \ldots, f_n) = (f_1, \ldots, f_t, 1, \ldots, 1), \quad f_t > 1.$$

Então:

$$p(T)[V] = p(T)[Z(u_1, T)] \oplus \cdots \oplus p(T)[Z(u_m, T)]$$

e

$$p(T)[V] = p(T)[Z(v_1, T)] \oplus \cdots \oplus p(T)[Z(v_n, T)],$$

mas $p(T)[Z(v_1, T)]$ é um subespaço cíclico anulável por $p(T)^{e_1 - 1}$, aí pela hipótese de indução temos:

$$s = t \quad \text{e} \quad e_1 = f_1, \ldots, e_s = f_s,$$

concluindo assim a demonstração da unicidade. □

Agora podemos juntar a decomposição primária para minimais e a decomposição cíclica para espaços primários e obter a decomposição cíclica em divisores elementares.

Teorema 4.44 (Decomposição Cíclica em Divisores Elementares)**.** Seja V um espaço vetorial de *dimensão finita* e seja $\mathrm{T} \in \mathcal{L}(\mathrm{V})$. Se o polinômio minimal é dado por:

$$\mathrm{m_T} = \mathrm{p_1^{e_1} \dots p_n^{e_n}},$$

em que os $\mathrm{p_i}$ são polinômios irredutíveis mônicos distintos sobre K, então V pode ser decomposto em uma soma direta:

$$\mathrm{V} = \mathrm{V_1} \oplus \mathrm{V_n},$$

em que:

$$\mathrm{V_i} = \mathrm{Ker}\ \ \mathrm{p_i(T)^{e_i}}$$

é um subespaço T-invariante tal que $\mathrm{m_{T\restriction V_i}} = \mathrm{p_i^{e_i}}$. Finalmente, cada subespaço T-invariante $\mathrm{V_i}$ pode ser escrito como uma soma direta de submódulos cíclicos, de modo que:

$$\mathrm{V} = \Big(\mathrm{Z(v_{1,1}, T)} \oplus \dots \oplus \mathrm{Z(v_{1,k_1}, T)}\Big) \oplus \Big(\mathrm{Z(v_{n,1}, T)} \oplus \dots \oplus \mathrm{Z(v_{n,k_n}, T)}\Big),$$

em que $\mathrm{m_{T,v_{i,j}}} = \mathrm{p_i^{e_{i,j}}}$ e os termos de cada decomposição cíclica podem ser arranjados de modo que para cada i tenhamos:

$$\mathrm{e_i} = \mathrm{e_{i,1}} \geq \mathrm{e_{i,2}} \geq \dots \geq \mathrm{e_{i,k_i}}.$$

Além disso, juntando os teoremas das unicidades da decomposição primária para minimais e da decomposição cíclica para espaços primários, então temos a unicidade da decomposição cíclica em divisores elementares.

Teorema 4.45 (Unicidade da Decomposição Cíclica em Divisores Elementares)**.** Seja V um espaço vetorial e seja $\mathrm{T} \in \mathcal{L}(\mathrm{V})$. Suponhamos que V possa ser escrito como uma soma direta:

$$\mathrm{V} = \Big(\mathrm{Z(u_{1,1}, T)} \oplus \dots \oplus \mathrm{Z(u_{1,k_1}, T)}\Big) \oplus \dots \oplus \Big(\mathrm{Z(u_{m,1}, T)} \oplus \dots \oplus \mathrm{Z(u_{m,k_m}, T)}\Big)$$

em que $\mathrm{m_{T,u_{i,j}}} = \mathrm{p_i^{e_{i,j}}}$ e:

$$\mathrm{e_{i,1}} \geq \mathrm{e_{i,2}} \geq \dots \geq \mathrm{e_{i,k_i}},$$

e suponhamos que V possa ser escrito como uma soma direta:

$$\mathrm{V} = \Big(\mathrm{Z(v_{1,1}, T)} \oplus \dots \oplus \mathrm{Z(v_{1,l_1}, T)}\Big) \oplus \dots \oplus \Big(\mathrm{Z(v_{n,1}, T)} \oplus \dots \oplus \mathrm{Z(v_{n,l_n}, T)}\Big)$$

em que $\mathrm{m_{T,v_{i,j}}} = \mathrm{q_i^{f_{i,j}}}$ e:

$$\mathrm{f_{i,1}} \geq \mathrm{f_{i,2}} \geq \dots \geq \mathrm{f_{i,l_i}}.$$

Então:

- O número de somandos é o mesmo em ambas as decomposições; de fato, $\mathrm{m} = \mathrm{n}$ e, depois de uma reindexação apropriada, $\mathrm{k_u} = \mathrm{l_u}$ para todo u.

- Os subespaços primários são os mesmos; isto é, depois de uma reindexação apropriada, para todo i temos $\mathrm{p_i} = \mathrm{q_i}$ e:

$$\mathrm{Z(u_{i,1}, T)} \oplus \dots \oplus \mathrm{Z(u_{i,k_i}, T)} = \mathrm{Z(v_{i,1}, T)} \oplus \dots \oplus \mathrm{Z(v_{i,l_i}, T)}.$$

Definição 4.46. O multiconjunto dos polinômios $\mathrm{p_i^{e_{i,j}}}$ é unicamente determinado pela decomposição cíclica em divisores elementares, assim ele é chamado o multiconjunto dos **divisores elementares**.

A forma mais usual de se apresentar uma decomposição em subespaços cíclicos é a decomposição cíclica em fatores invariantes.

Teorema 4.47 (Decomposição Cíclica em Fatores Invariantes)**.** Seja V um espaço vetorial de *dimensão finita* e seja $T \in \mathcal{L}(V)$. Então V pode ser escrito como uma soma direta:

$$V = Z(v_1, T) \oplus \cdots \oplus Z(v_r, T)$$

em que $m_{T,v_i} = p_i$ e também:

$$p_r \mid p_{r-1} \mid \cdots \mid p_2 \mid p_1.$$

Por causa da unicidade da decomposição cíclica em divisores elementares, então temos a unicidade da decomposição cíclica em fatores invariantes

Teorema 4.48 (Unicidade da Decomposição Cíclica em Fatores Invariantes)**.** Seja V um espaço vetorial e seja $T \in \mathcal{L}(V)$. Suponhamos que V possa ser escrito como uma soma direta:

$$V = Z(u_1, T) \oplus \cdots \oplus Z(u_r, T)$$

em que $m_{T,u_i} = p_i$ e também:

$$p_r \mid p_{r-1} \mid \cdots \mid p_2 \mid p_1,$$

e que V possa ser escrito como uma soma direta:

$$V = Z(v_1, T) \oplus \cdots \oplus Z(v_s, T)$$

em que $m_{T,v_j} = q_j$ e também:

$$q_s \mid q_{s-1} \mid \cdots \mid q_2 \mid q_1.$$

Então $m = n$ e também $p_k = q_k$ para todo k.

Definição 4.49. A sequência dos polinômios p_i é unicamente determinado pela decomposição cíclica em fatores invariantes, assim ela é chamada a sequência dos **fatores invariantes**.

Capítulo 5

Espaços com Produto Interno

Neste capítulo, convencionaremos que K é $\mathbb{R}$ ou $\mathbb{C}$.

5.1 Definições e Exemplos

Definição 5.1. Um espaço vetorial V é dito um **espaço com produto interno** se estiver munida com uma função:

$$\begin{array}{rcl} \mathrm{V}\times\mathrm{V} & \to & \mathrm{K} \\ (\mathrm{u},\mathrm{v}) & \mapsto & \langle \mathrm{u},\mathrm{v}\rangle \end{array}$$

tal que:

- $\langle \alpha\mathrm{u}+\beta\mathrm{v},\mathrm{w}\rangle = \alpha\langle \mathrm{u},\mathrm{w}\rangle + \beta\langle \mathrm{v},\mathrm{w}\rangle$ para quaisquer $\alpha,\beta\in\mathrm{K}$ e $\mathrm{u},\mathrm{v},\mathrm{w}\in\mathrm{V}$.
- $\overline{\langle \mathrm{u},\mathrm{v}\rangle} = \langle \mathrm{v},\mathrm{u}\rangle$ para quaisquer $\mathrm{u},\mathrm{v}\in\mathrm{V}$.
- $\langle \mathrm{v},\mathrm{v}\rangle \geq 0$ para $\mathrm{v}\in\mathrm{V}$.
- $\langle \mathrm{v},\mathrm{v}\rangle = 0 \Rightarrow \mathrm{v}=0$ para $\mathrm{v}\in\mathrm{V}$.

Exemplo 5.2. O exemplo principal é $\mathrm{V}=\mathrm{K}^{\mathrm{n}}$, em que, tomando $\mathrm{u}=(\alpha_1,\ldots,\alpha_{\mathrm{n}})$ e $\mathrm{v}=(\beta_1,\ldots,\beta_{\mathrm{n}})$, definimos:

$$\langle \mathrm{u},\mathrm{v}\rangle = \alpha_1\overline{\beta_1}+\cdots+\alpha_{\mathrm{n}}\overline{\beta_{\mathrm{n}}}.$$

Exemplo 5.3. Podemos considerar $\mathrm{V}=\mathcal{M}_{\mathrm{n}}(\mathrm{K})\cong\mathrm{K}^{\mathrm{n}^2}$. Com base no exemplo anterior, definimos:

$$\langle \mathrm{A},\mathrm{B}\rangle = \sum_{\mathrm{i},\mathrm{j}} \mathrm{a}_{\mathrm{i},\mathrm{j}}\overline{\mathrm{b}_{\mathrm{i},\mathrm{j}}}.$$

Para toda $\mathrm{A}=(\mathrm{a}_{\mathrm{i},\mathrm{j}})\in\mathcal{M}_{\mathrm{n}}(\mathrm{K})$, definimos:

$$\mathrm{A}^* = (\overline{\mathrm{a}_{\mathrm{i},\mathrm{j}}}),$$

e

$$\mathrm{tr}(\mathrm{A}) = \mathrm{a}_{1,1}+\cdots+\mathrm{a}_{\mathrm{n},\mathrm{n}},$$

então podemos ver que:

$$\langle \mathrm{A},\mathrm{B}\rangle = \mathrm{tr}(\mathrm{AB}^*).$$

Exemplo 5.4. Podemos tomar $\mathrm{V}=\mathcal{C}[\mathrm{a},\mathrm{b}]$, o conjunto das funções contínuas de $[\mathrm{a},\mathrm{b}]$ em $\mathbb{C}$, e para $\mathrm{f},\mathrm{g}\in\mathrm{V}$ definirmos:

$$\langle \mathrm{f},\mathrm{g}\rangle = \int_{\mathrm{a}}^{\mathrm{b}} \mathrm{f}(\mathrm{t})\overline{\mathrm{g}(\mathrm{t})}\,\mathrm{dt}.$$

Exemplo 5.5. Seja $T \in \mathcal{L}(U, V)$ bijetora. Suponhamos que V tenha um produto interno. Se $u_1, u_2 \in U$, definimos:

$$\langle u_1, u_2 \rangle_U = \langle T(u_1), T(u_2) \rangle_V.$$

Suponhamos que U tenha uma base $B = (e_1, \dots, e_n)$. Então existe uma $T : U \to K^n$ tal que:

$$T(e_i) = (0, \dots, 1, \dots, 0),$$

em que a entrada i vale 1 e as outras valem 0. Sendo:

$$u = \alpha_1 e_1 + \cdots + \alpha_n e_n, \quad v = \beta_1 e_1 + \cdots + \beta_n e_n,$$

então:

$$\langle u, v \rangle_U = \langle T(u), T(v) \rangle_V = \sum_{i=1}^{n} \alpha_i \overline{\beta_i}.$$

Definição 5.6. Se $\dim(V) = n < \infty$ e $K = \mathbb{R}$, então chamamos V de **euclidiano**.
Se $\dim(V) = n < \infty$ e $K = \mathbb{C}$, então chamamos V de **unitário**.

Definição 5.7. Se V é um espaço com produto interno e V é um espaço completo em relação à norma $\|v\| = \sqrt{\langle v, v \rangle}$, então V se chama um **espaço de Hilbert**.

5.2 Matriz de Gramm

Definição 5.8. Seja V um espaço com produto interno. Sejam $v_1, \dots, v_k \in V$. Definimos:

$$G(v_1, \dots, v_n) = \begin{pmatrix} \langle v_1, v_1 \rangle & \dots & \langle v_1, v_n \rangle \\ \dots & \dots & \dots \\ \langle v_n, v_1 \rangle & \dots & \langle v_n, v_n \rangle \end{pmatrix}.$$

Nesse caso temos:

$$G(v_1, \dots, v_n)^* = G(v_1, \dots, v_n).$$

Toda matriz A que satisfaz $A^* = A$ é chamada **Hermitiana**.

Proposição 5.9. Seja $B = (e_1, \dots, e_n)$ uma base de V. Então $G(e_1, \dots, e_n)$ é inversível.

Demonstração. Primeiro observemos que para quaisquer $u, v \in V$, com:

$$[u]_B = (\alpha_1, \dots, \alpha_n), \quad [v]_B^* = (\beta_1, \dots, \beta_n)$$

então:

$$\langle u, v \rangle = [u]_B A [v]_B^*.$$

De fato:

$$\langle u, v \rangle = \sum_{i,j} \alpha_i \overline{\beta_j} \langle e_i, e_j \rangle,$$

aí:

$$\begin{aligned} [u]_B A [v]_B^* &= (\alpha_1, \dots, \alpha_n) \begin{pmatrix} \langle e_1, e_1 \rangle & \dots & \langle e_1, e_n \rangle \\ \dots & \dots & \dots \\ \langle e_n, e_1 \rangle & \dots & \langle e_n, e_n \rangle \end{pmatrix} \begin{pmatrix} \overline{\beta_1} \\ \vdots \\ \overline{\beta_n} \end{pmatrix} \\ &= \begin{pmatrix} \alpha_1 \langle e_1, e_1 \rangle + \cdots + \alpha_n \langle e_n, e_1 \rangle \\ \vdots \\ \alpha_1 \langle e_1, e_n \rangle + \cdots + \alpha_n \langle e_n, e_n \rangle \end{pmatrix} \begin{pmatrix} \overline{\beta_1} \\ \vdots \\ \overline{\beta_n} \end{pmatrix} \end{aligned}.$$

Se A não for inversível, então existe $u \neq 0$ tal que $[u]_B A = 0$. Neste caso, $\langle u, u \rangle = [u]_B A [u]_B^* = 0$, aí $u = 0$, contradição. $\square$

Se $B = (e_1, \ldots, e_n)$ é uma base de V e $A = G(e_1, \ldots, e_n)$ então para todo $v \in V$ temos:

$$[v]_B A [v]_B^* \geq 0$$

e a igualdade ocorre se e somente se $v = 0$.

Definição 5.10. Uma matriz Hermitiana A é dita:

- **Positiva semidefinitiva** se e só se para todo $x \in K^n$ temos $xAx^* \geq 0$.
- **Positiva definitiva** se e só se para todo $x \in K^n$ tal que $x \neq 0$ temos $xAx^* > 0$.

Proposição 5.11. Seja $A \in \mathcal{M}_n(K)$ uma matriz Hermitiana positiva definitiva. Seja V um espaço vetorial com base $B = (e_1, \ldots, e_n)$. Definamos, para $u, v \in V$, o seguinte:

$$\langle u, v \rangle = [u]_B A [v]_B^*.$$

Então $\langle u, v \rangle$ é um produto interno.

5.3 Espaços Normados

Definição 5.12. Um espaço vetorial V é dito um **espaço normado** se estiver munido com uma função:

$$\begin{array}{ccc} V & \to & \mathbb{R} \\ v & \mapsto & \|v\| \end{array}$$

que satisfaça as seguintes propriedades:

- $\|v\| \geq 0$ para $v \in V$.
- $\|v\| = 0 \Rightarrow v = 0$ para $v \in V$.
- $\|\alpha v\| = |\alpha| \|v\|$ para $\alpha \in K$ e $v \in V$.
- $\|u + v\| \leq \|u\| + \|v\|$ para $u, v \in V$.

Proposição 5.13 (Desigualdade de Cauchy-Bunyakovski-Schwarz)**.** Seja V um espaço com produto interno. Então para quaisquer $u, v \in V$ temos:

$$\big|\langle u, v \rangle\big| \leq \|u\| \cdot \|v\|.$$

Demonstração. Se $v = 0$, então é fácil. Se $v \neq 0$, então $\|v\| > 0$, aí para quaisquer $\alpha, \beta \in K$ temos:

$$\begin{array}{rcl} 0 & \leq & \langle \alpha u - \beta v, \alpha u - \beta v \rangle \\ & = & \alpha\overline{\alpha}\langle u, u \rangle + \beta\overline{\beta}\langle v, v \rangle - \alpha\overline{\beta}\langle u, v \rangle - \beta\overline{\alpha}\langle v, u \rangle \\ & = & |\alpha|^2 \|u\|^2 + |\beta|^2 \|v\|^2 - \left(\alpha\overline{\beta}\langle u, v \rangle + \overline{\alpha\overline{\beta}\langle u, v \rangle}\right). \end{array}$$

Em particular, fazendo $\alpha = \|v\|$ e $\beta = \langle u, v \rangle$, então:

$$\begin{array}{rl} & \|v\|^4 \|u\|^2 + \big|\langle u, v \rangle\big|^2 \|v\|^2 - 2\|v\|^2 \langle u, v \rangle^2 \geq 0 \\ \Rightarrow & \|v\|^2 \|u\|^2 - \big|\langle u, v \rangle\big|^2 \geq 0 \\ \Rightarrow & \big(\|v\| \|u\|\big)^2 \geq \big|\langle u, v \rangle\big|^2. \end{array}$$

□

Proposição 5.14. Seja V um espaço com produto interno e definamos $\|v\| = \sqrt{\langle v, v \rangle}$. Então $\|v\|$ é uma norma.

Demonstração. Provaremos apenas a última propriedade requerida para espaço normado, deixando as outras para o leitor. Sabemos que para $z \in \mathbb{C}$ então $z + \bar{z} \leq 2|z|$. De fato, sendo $z = a + bi$, então $|z| = \sqrt{a^2 + b^2} \geq a$, aí $z + \bar{z} = 2a \leq 2|z|$. Agora temos:

$$\begin{aligned} |u+v|^2 &= \langle u+v, u+v \rangle \\ &= \|u\|^2 + \|v\|^2 + \left(\langle u, v \rangle + \overline{\langle u, v \rangle}\right) \\ &\leq \|u\|^2 + \|v\|^2 + 2\left|\langle u, v \rangle\right| \\ &\leq \|u\|^2 + \|v\|^2 + 2\|u\| \cdot \|v\| \\ &= \left(\|u\| + \|v\|\right)^2. \end{aligned}$$

□

5.4 Ortogonalidade

Definição 5.15. Dois vetores $u, v \in V$ são ditos **ortogonais** se e só se $\langle u, v \rangle = 0$.

Uma família $(v_i)_{i \in I}$ de vetores é chamado **ortogonal** se e só se para quaisquer $i, j \in I$ tais que $i \neq j$ os vetores v_i e v_j forem ortogonais.

Uma família $(v_i)_{i \in I}$ de vetores é chamado **ortonormal** se e só se é ortogonal e para todo $i \in I$ temos $\|v_i\| = 1$.

Proposição 5.16. Se $(v_i)_{i \in I}$ é uma família ortogonal de vetores *não nulos*, então a família é L.I.

Demonstração. Para conjunto finito $J \subseteq I$ e para $\alpha : J \to I$, se:

$$\sum_{i \in J} \alpha_i v_i = 0,$$

então para $j \in J$ temos:

$$0 = \left\langle \sum_{i \in J} \alpha_i v_i, v_j \right\rangle = \sum_{i \in J} \alpha_i \langle v_i, v_j \rangle = \alpha_j \left\| v_j \right\|^2,$$

mas $v_j \neq 0$, aí $\left\| v_j \right\|^2 \neq 0$, aí $\alpha_j = 0$. □

Proposição 5.17 (Ortogonalização de Gramm-Schmidt)**.** Para toda sequência linearmente independente $(v_1, \ldots, v_k)$ de vetores, existe uma sequência ortogonal $(u_1, \ldots, u_k)$ tal que $\langle v_1, \ldots, v_k \rangle = \langle u_1, \ldots, u_k \rangle$.

Demonstração. Indução sobre k. □

Corolário 5.18. Todo espaço com produto interno de dimensão finita tem uma base ortonormal.

5.5 Funcionais Lineares

Proposição 5.19. Seja V um espaço com produto interno. Para $u \in V$, definimos $\varphi_u : V \to K$ assim:

$$\varphi_u(v) = \langle v, u \rangle.$$

Então φ_u é um funcional linear.

Teorema 5.20 (Teorema de Riesz)**.** Se $\dim(V) < \infty$, então para todo $f \in V^*$ existe $u \in V$ tal que $f = \varphi_u$.

Demonstração. Seja $f \in V^*$. Escolhemos uma base ortonormal $B = (e_1, \dots, e_n)$ em V e seja $\alpha_i = f(e_i) \in K$ para $i = 1, \dots, n$. Consideremos $u = \overline{\alpha_1} e_1 + \cdots + \overline{\alpha_n} e_n$. Então para $k = 1, \dots, n$ temos:

$$\begin{aligned} \varphi_u(e_k) = \langle e_k, u \rangle &= \langle e_k, \overline{\alpha_1} e_1 + \cdots + \overline{\alpha_n} e_n \rangle \\ &= \alpha_k \langle e_k, e_k \rangle = \alpha_k = f(e_k), \end{aligned}$$

ou seja, $\varphi_u(e_k) = f(e_k)$; logo $\varphi_u = f$. □

Observação 5.21. O teorema de Riesz não é válido para espaços com produto interno de dimensão finita. De fato, se $V = \mathcal{C}[a, b]$, então seja $x_0 \in [a, b]$ e seja $\varphi \in V^*$ dada por:

$$\varphi(f) = f(x_0).$$

Índice