Textos complementares para a disciplina Álgebra Linear Avançada I

Claudia Correa

Sumário

1 Estruturas algébricas

No presente texto, vamos discutir informalmente o conceito de estruturas algébricas.

Uma *estrutura algébrica* consiste de um conjunto e de operações definidas nesse conjunto. Um exemplo de uma estrutura algébrica é um espaço vetorial sobre $\mathbb{R}$. Um espaço vetorial sobre $\mathbb{R}$ consiste de um conjunto V, munido de duas operações:

$$+ : V \times V \longrightarrow V \quad \text{e} \quad \cdot : \mathbb{R} \times V \longrightarrow V,$$

e exigimos que essas operações satisfaçam algumas propriedades. Note que para se especificar um espaço vetorial sobre $\mathbb{R}$ não basta especificar o conjunto de vetores, temos que especificar também as operações. Por exemplo, vimos em aula duas estruturas diferentes de $\mathbb{R}$-espaço vetorial no conjunto $\mathbb{R}^2$.

Um aspecto interessante é que podemos colocar uma estrutura algébrica num conjunto Y a partir de uma estrutura algébrica num outro conjunto X e uma função bijetora $\varphi : X \longrightarrow Y$. A idéia consiste em transferir as operações de X para Y através da bijeção φ. Por exemplo, suponha que X esteja munido de uma operação $* : X \times X \longrightarrow X$, definimos a operação $\circ : Y \times Y \longrightarrow Y$, fazendo:

$$y_1 \circ y_2 = \varphi\big(\varphi^{-1}(y_1) * \varphi^{-1}(y_2)\big), \tag{1}$$

para todos y_1 e y_2 pertencentes a Y. Observe que de (1) segue que:

$$\varphi(x_1 * x_2) = \varphi(x_1) \circ \varphi(x_2), \tag{2}$$

para todos os elementos x_1 e x_2 de X. O interessante dessa definição é que se a operação $*$ em X satifaz uma determinada propriedade algébrica, então a operação $\circ$ definida em (1) também satisfaz essa propriedade. Por exemplo, se $*$ é comutativa, então a operação $\circ$ em Y também é comutativa. De fato, fixados y_1 e y_2 em Y, temos que:

$$y_1 \circ y_2 = \varphi\big(\varphi^{-1}(y_1) * \varphi^{-1}(y_2)\big) = \varphi\big(\varphi^{-1}(y_2) * \varphi^{-1}(y_1)\big) = y_2 \circ y_1.$$

Exemplo de uma aplicação dessas idéias.

Sabemos que o conjunto dos números inteiros $\mathbb{Z}$ não é um corpo, se munido das operações usuais. Mas, podemos nos perguntar se existem operações em $\mathbb{Z}$ que fazem desse conjunto um corpo. A resposta para essa pergunta é afirmativa. Para mostrar isso, vamos usar o seguinte lema.

Lema 1.1. *Existe uma função bijetora entre os conjuntos $\mathbb{Q}$ e $\mathbb{Z}$.*

Eu não vou provar o Lema 1.1 aqui. Para aqueles que não conhecem esse resultado, peço que acreditem nele. Em algum outro curso, vocês verão a prova desse resultado (acredito que em algum curso de teoria dos conjuntos).

Fixe uma bijeção $\varphi : \mathbb{Q} \longrightarrow \mathbb{Z}$. Usando essa bijeção, definimos as operações em $\mathbb{Z}$ de forma análoga ao feito em (1). Mais precisamente, defina:

$$n \oplus m = \varphi\big(\varphi^{-1}(n) + \varphi^{-1}(m)\big) \quad \text{e}$$

$$n \odot m = \varphi\big(\varphi^{-1}(n) \cdot \varphi^{-1}(m)\big),$$

para todos n e m inteiros, onde $+$ e $\cdot$ denotam as operações usuais de $\mathbb{Q}$.

Exercício 1.2. *Mostre que* $(\mathbb{Z}, \oplus, \odot)$ *é um corpo.*

2 Existência de bases em espaços vetoriais

O objetivo do presente texto é apresentar a prova de que todo espaço vetorial admite uma base. Note que em sala de aula, vimos que se um espaço vetorial admite um conjunto finito de geradores, então ele possui uma base. Assim, a seguinte pergunta se coloca naturalmente:

Pergunta 2.1. *Seja V um espaço vetorial e suponha que V não possua um subconjunto finito de geradores. Existe uma base para V?*

A resposta para essa pergunta é afirmativa. No que segue, nos dedicaremos a mostrar o teorema abaixo.

Teorema 2.2. *Todo espaço vetorial admite uma base.*

Por definição, temos que uma base de um espaço vetorial é um subconjunto desse espaço que é LI e que gera todo o espaço. A idéia da prova do Teorema 2.2 é mostrar que num espaço vetorial, existe um subconjunto LI maximal e depois, mostrar que se um conjunto LI é maximal, então ele é um conjunto de geradores do espaço. A dificuldade é provar que existe um tal conjunto LI maximal. A existência desse conjunto é garantida pelo Lema de Zorn. Para enunciarmos o Lema de Zorn, necessitamos de alguns conceitos, que introduzo abaixo.

Definição 2.3. *Seja um conjunto X. Uma ordem parcial em X é uma relação binária $\preceq$ em X satisfazendo as seguintes propriedades:*

1. *Reflexividade, i.e., dado x em X vale que $x \preceq x$;*
2. *Antisimetria, i.e., dados x e y em X, se $x \preceq y$ e $y \preceq x$, então $x = y$.*
3. *Transitividade, i.e., dados x, y e z em X se $x \preceq y$ e $y \preceq z$, então $x \preceq z$;*

Uma ordem parcial $\preceq$ é dita total se dados dois elementos x e y de X vale que $x \preceq y$ ou $y \preceq x$.

Exercício 2.4. *Dado um conjunto A, considere a coleção de todos os subconjuntos de A, i.e., defina:*

$$\wp(A) = \{X : X \subset A\}.$$

Defina em $\wp(A)$ a seguinte relação:

$$X \preceq Y \quad \text{se, e somente se,} \quad X \subset Y,$$

para todos X e Y elementos de $\wp(A)$. Mostre que $\preceq$ é uma ordem parcial em $\wp(A)$. Essa ordem é total?

Definição 2.5. *Sejam X um conjunto e $\preceq$ uma ordem parcial em X.*

(a) Um subconjunto Y de X é dito uma cadeia se a restrição da ordem $\preceq$ a Y é uma ordem total em Y.

(b) Uma cota superior em X de um subconjunto Y de X é um elemento x de X com a seguinte propriedade:

$$y \preceq x, \quad \text{para todo } y \in Y.$$

A definição de cota inferior se faz de forma análoga.

(c) Um elemento x de X é dito maximal em X se :

$$x \preceq y \Rightarrow y = x, \quad \text{para todo } y \in X.$$

A definição de elemento minimal é feita de forma análoga.

Exercício 2.6. *Seja A um conjunto e considere $\wp(A)$ munido da ordem parcial definida no Exercício 2.4. Mostre que se $\mathfrak{D}$ é um subconjunto de $\wp(A)$, então a união $\bigcup \mathfrak{D}$ é uma cota superior de $\mathfrak{D}$ em $\wp(A)$.*

Finalmente, temos em mãos tudo que precisamos para entender o enunciado do Lema de Zorn.

Lema de Zorn. Sejam $\mathfrak{C}$ um conjunto e $\preceq$ uma ordem parcial em $\mathfrak{C}$. Suponha que $\mathfrak{C}$ seja não vazio e que toda cadeia de elementos de $\mathfrak{C}$ possua uma cota superior em $\mathfrak{C}$. Então, $\mathfrak{C}$ possui um elemento maximal[1].

Agora, vamos usar o Lema de Zorn para provar o Teorema 2.2. A prova desse teorema seguirá facilmente dos dois próximos lemas.

Lema 2.7. *Seja V um espaço vetorial sobre um corpo K. Então, existe um subconjunto S de V que é maximal dentre os LI, i.e., S é um subconjunto LI de V e S não está contido propriamente em nenhum subconjunto LI de V.*

Demonstração. Denote por $\mathfrak{C}$ a coleção de todos os subconjuntos LI de V. Defina em $\mathfrak{C}$ a seguinte relação binária:

$$A \preceq B \text{ se, e somente se, } A \subset B,$$

para todos A e B pertencentes a $\mathfrak{C}$.

Exercício 2.8. *Mostre que a relação definida acima é uma ordem parcial em $\mathfrak{C}$.*

[1] Não vou provar aqui o Lema de Zorn. Em algum outro curso, vocês provavelmente discutirão esse resultado.

Note que $\mathfrak{C}$ não é vazio. Por exemplo, o conjunto vazio pertence a $\mathfrak{C}$. Agora, considere $\mathfrak{D}$ uma cadeia de elementos de $\mathfrak{C}$ e vamos mostrar que $\mathfrak{D}$ possui uma cota superior em $\mathfrak{C}$. De acordo com o Exercício 2.6, temos que $\bigcup \mathfrak{D}$ é uma cota superior de $\mathfrak{D}$ em $\wp(V)$. No entanto, à princípio, não sabemos se $\bigcup \mathfrak{D}$ pertence a $\mathfrak{C}$.

Exercício 2.9. *Mostre que $\bigcup \mathfrak{D}$ é um subconjunto LI de V e portanto, pertence a $\mathfrak{C}$.*

Dessa forma, o Lema de Zorn garante a existência de um elemento maximal em $\mathfrak{C}$. □

Lema 2.10. *Sejam V um espaço vetorial sobre um corpo K e S um subconjunto de V. Se S é um conjunto LI maximal de V, então S é um conjunto de geradores de V.*

Demonstração. Dado $v \in V$, devemos mostrar que v pertence ao subespaço gerado por S. Suponha, por absurdo, que v não pertença ao subespaço gerado por S. Do Exercício 2.11 abaixo segue que $S \cup \{v\}$ é um conjunto LI.

Exercício 2.11. *Sejam S um subconjunto LI de um espaço vetorial V e v um vetor desse espaço. Mostre que se v não pertence ao subespaço gerado por S, então o conjunto $S \cup \{v\}$ é LI.*

Claramente, vale que $S \subset S \cup \{v\}$. Como v não pertence a S, temos que S está contido propriamente em $S \cup \{v\}$. Mas, isso não pode acontecer devido à maximalidade de S. Essa contradição mostra que v pertence ao subespaço gerado por S. □

Prova do Teorema 2.2. Seja V um espaço vetorial sobre um corpo K. Seja S o subconjunto LI maximal de V dado pela Lema 2.7. De acordo com o Lema 2.10, temos que S é um conjunto de geradores de V. Portanto, S é um conjunto LI que gera V. Assim, S é uma base de V. □

Observação 2.12. *Em aula, vimos que se um espaço vetorial tem dimensão finita, i.e., admite uma base finita, então todas as bases desse espaço têm o mesmo número de elementos. Na verdade, o mesmo vale para espaços que não possuem dimensão finita. Não veremos isso nesse curso, pois acredito que vocês ainda não têm todas as ferramentas para o estudo desse resultado.*

3 Unicidade da base pré-dual

O objetivo do presente texto é apresentar a prova do seguinte teorema.

Teorema 3.1. *Seja V um espaço vetorial de dimensão finita sobre um corpo K. Se B_1 e B_2 são duas bases ordenadas de V tais que $B_1^* = B_2^*$, então $B_1 = B_2$.*

Demonstração. Escreva $B_1 = (v_i)_{i=1}^n$, $B_2 = (u_i)_{i=1}^n$ e

$$C = B_1^* = B_2^* = (\alpha_i)_{i=1}^n.$$

Suponha, por absurdo, que B_1 e B_2 são distintas, o que implica que existe $j \in \{1, ...n\}$ tal que $v_j \neq u_j$. Do Exercício 2 da Lista sobre funcionais lineares e espaços duais segue que existe $\alpha \in V^*$ tal que $\alpha(v_j) \neq \alpha(u_j)$. Como C é base de V^*, existem únicos escalares $\lambda_1, ..., \lambda_n$ no corpo tais que:

$$\alpha = \sum_{i=1}^{n} \lambda_i \cdot \alpha_i.$$

Aplicando α em v_j, obtemos:

$$\alpha(v_j) = \sum_{i=1}^{n} \lambda_i \cdot \alpha_i(v_j) = \lambda_j, \tag{3}$$

pois C é a base dual de B_1. Por outro lado, aplicando α em u_j, obtemos:

$$\alpha(u_j) = \sum_{i=1}^{n} \lambda_i \cdot \alpha_i(u_j) = \lambda_j, \tag{4}$$

pois C é a base dual de B_2. De (3) e (4) segue que $\alpha(v_j) = \alpha(u_j)$. Essa contradição estabelece nosso resultado. □

4 Isomorfismo transposto

O objetivo do presente texto é apresentar uma prova do seguinta teorema.

Teorema 4.1. *Sejam V e W espaços vetoriais sobre um corpo K e considere $T : V \longrightarrow W$ uma transformação linear. As seguintes afirmações são equivalentes:*

1. *T é bijetora.*
2. *T^* é bijetora.*

Em aula, provamos o seguinte resultado.

Lema 4.2. *Sejam V e W espaços vetoriais sobre um corpo K e considere $T : V \longrightarrow W$ uma transformação linear. As seguintes afirmações são equivalentes:*

1. *T é sobrejetora.*
2. *T^* é injetora.*

Dessa forma, para estabelecer o Teorema 4.1, basta mostrarmos que T é injetora se, e somente se, T^* é sobrejetora.

Inicialmente, vamos mostrar que se T é injetora, então T^* é sobrejetora, o que será feito no Lema 4.5 abaixo. Para provar o Lema 4.5, precisaremos do seguinte lema.

Lema 4.3. *Sejam V e W espaços vetoriais sobre um corpo K e U um subespaço de V. Se $T : U \longrightarrow W$ é uma transformação linear, então existe uma transformação linear $\tilde{T} : V \longrightarrow W$ tal que:*

$$\tilde{T}(u) = T(u), \quad \forall u \in U.$$

Demonstração. De acordo com o Teorema 1 da Resolução dos exercícios bônus da lista sobre bases e somas de subespaços, temos que todo subespaço de um espaço vetorial é complementado. Seja $P : V \longrightarrow V$ uma projeção com $ImP = U$. Defina $\tilde{T} : V \longrightarrow W$ como $\tilde{T} = T \circ P$. É claro que $\tilde{T}$ é linear e que $\tilde{T}(u) = T(u)$, para todo $u \in U$. □

Definição 4.4. *Sejam X e Z conjuntos e Y um subconjunto de X. Dada uma função $f : Y \longrightarrow Z$, uma extensão de f a X é uma função $\tilde{f} : X \longrightarrow Z$ tal que:*

$$\tilde{f}(y) = f(y), \quad \forall y \in Y.$$

Tendo em mente a Definição 4.4, o Lema 4.3 nos diz que toda transformação linear definida num subespaço de um espaço vetorial admite uma extensão linear para o espaço todo.

Lema 4.5. *Sejam V e W espaços vetoriais sobre um corpo K e considere $T : V \longrightarrow W$ uma transformação linear. Se T é injetora, então T^* é sobrejetora.*

Demonstração. Devemos mostrar que dado $\alpha \in V^*$, existe $\gamma \in W^*$ tal que $T^*(\gamma) = \alpha$. Note que:

$$T : V \longrightarrow ImT$$

é um isomorfismo. Portanto, temos que $T^{-1} : ImT \longrightarrow V$ está bem definida e é uma transformação linear. Fixado $\alpha \in V^*$, defina $\beta : ImT \longrightarrow K$ como $\beta = \alpha \circ T^{-1}$. É claro que β é linear, já que é uma composição de duas transformações lineares. Do Lema 4.3 segue que existe uma extensão linear $\tilde{\beta} : W \longrightarrow K$ de β. Note que:

$$T^*(\tilde{\beta})(v) = \tilde{\beta}\big(T(v)\big) = \beta(T(v)) = \alpha(v), \quad \forall v \in V.$$

Portanto, temos que $T^*(\tilde{\beta}) = \alpha$. Isso estabelece a sobrejetividade de T^*. □

Agora, vamos mostrar que se T^* é sobrejetora, então T é injetora. Note que o Lema 4.2 garante que se T^* é sobrejetora, então T^{**} é injetora. Logo, nossa estratégia para estabelecer esse resultado será relacionar a T com a T^{**} e mostrar que a injetividade de T^{**} implica a injetividade de T. Recordemos a seguinte definição.

Definição 4.6. *Seja V um espaço vetorial sobre um corpo K. Definimos $Aval : V \longrightarrow V^{**}$ como $Aval(v) = aval_v$, para todo v pertencente a V, onde:*

$$aval_v(\alpha) = \alpha(v), \quad \forall \alpha \in V^*.$$

Em sala de aula, vimos que *Aval* é uma transformação linear e que se a dimensão de V é finita, então *Aval* é um isomorfismo. No entanto, não usamos a finitude da dimensão de V para concluir a injetividade de *Aval*. Dessa forma, em dimensão infinita, $Aval : V \longrightarrow V^{**}$ é uma transformação linear e injetora. O que implica que a função:

$$Aval : V \longrightarrow Im(Aval) \subset V^{**}$$

é um isomorfismo. Em outras palavras, *Aval* é um isomorfismo entre V e um subespaço de V^{**}. No próximo lema, vamos entender a relação entre T e T^{**}.

Lema 4.7. *Sejam V e W espaços vetoriais sobre um corpo K. Denote por $Aval^V : V \longrightarrow V^{**}$ e por $Aval^W : W \longrightarrow W^{**}$ os operadores de avaliação de V e W, respectivamente. Mais precisamente:*

$$Aval^V(v)(\alpha) = \alpha(v), \ \forall v \in V \ \ e \ \ \forall \alpha \in V^*$$

e

$$Aval^W(w)(\beta) = \beta(w), \ \forall w \in W \ \ e \ \ \forall \beta \in W^*.$$

Se $T : V \longrightarrow W$ é uma transformação linear, então vale que:

$$\big(Aval^W\big)^{-1} \circ T^{**} \circ Aval^V = T.$$

Em outras palavras, o diagrama abaixo é comutativo:

$$\begin{array}{ccc} V^{**} & \xrightarrow{T^{**}} & W^{**} \\ {\scriptstyle Aval^V}\uparrow & & \uparrow{\scriptstyle Aval^W} \\ V & \xrightarrow{T} & W \end{array}$$

Demonstração. Fixado v em V, temos que $T^{**} \circ Aval^V(v) \in W^{**}$. Fixe $\beta \in W^*$ e calculemos:

$$T^{**} \circ Aval^V(v)(\beta) = T^{**}\big(Aval^V(v)\big)(\beta) = T^{**}(aval_v)(\beta)$$

$$= aval_v\big(T^*(\beta)\big) = T^*(\beta)(v) = \beta\big(T(v)\big) = Aval^W\big(T(v)\big)(\beta).$$

Isso mostra que $T^{**} \circ Aval^V(v)(\beta) = \big(Aval^W \circ T(v)\big)(\beta)$, para todo $\beta \in W^*$ e portanto, temos que $T^{**} \circ Aval^V(v) = Aval^W \circ T(v)$, para todo $v \in V$. Donde segue que:

$$T^{**} \circ Aval^V = Aval^W \circ T. \tag{5}$$

Finalmente, compondo à esquerda os dois lados da igualdade (5) com $\big(Aval^W\big)^{-1}$, obtemos nosso resultado. □

Note que se identificarmos V e W com $Aval^V[V]$ e $Aval^W[W]$, respectivamente, temos que T^{**} é uma extensão de T.

A única ferramenta que ainda nos falta para concluir nosso resultado é dada pelo exercício abaixo.

Exercício 4.8. *Sejam X e Z conjuntos, Y um subconjunto de X e $f : Y \longrightarrow Z$ uma função. Se uma extensão $\tilde{f} : X \longrightarrow Z$ de f é injetora, então f é injetora.*

Lema 4.9. *Sejam V e W espaços vetoriais sobre um corpo K e considere $T : V \longrightarrow W$ uma transformação linear. Se $T^* : W^* \longrightarrow V^*$ é sobrejetora, então T é injetora.*

Demonstração. Como T^* é sobrejetora, o Lema 4.2 garante que T^{**} é injetora. Do Lema 4.7 segue que T^{**} pode ser vista como uma extensão de T. O resultado segue do Exercício 4.8. □

Os Lemas 4.5 e 4.9 e concluem a prova do Teorema 4.1. Temos o seguinte corolário do Teorema 4.1.

Corolário 4.10. *Sejam V e W espaços vetoriais sobre um corpo K e considere $T : V \longrightarrow W$ uma transformação linear. As seguintes afirmações são equivalentes:*

1. *T é isomorfismo.*
2. *T^* é isomorfismo*

□

5 Relações de equivalência e conjunto quociente

Iniciamos nossa revisão sobre realções de equivalência com uma estorinha. Suponham que vocês se formaram no graduação e desejem fazer uma festança para celebrar. Como vocês são muito populares, vocês tem muita gente para convidar. Por ser uma ocasião tão importante, vocês querem enviar convites para as casas dos seus amigos e familiares. Mas, daria muito trabalho enviar um convite para cada pessoa. Como resolver esse problema? Ou seja, como enviar convite para todos os seus amigos sem mandar um convite para cada pessoa? Bem, eu mandaria um convite para cada residência em que more pelo menos um de meus convidados. Assim, se dois dos meus convidados moram na mesma residência, os dois receberão o mesmo convite. Podemos pensar que se X denota o conjunto de todos os meus convidados, estamos definido a seguinte relação binária em X:

Convidado A e Convidado B estão relacionadas $\Leftrightarrow$ A e B moram na mesma casa.

Note que essa relaçao satisfaz algumas propriedades interessantes, a saber:

- Cada convidado está relacionado consigo mesmo;
- Se o Convidado A está relacionado com o Convidado B, então o Convidado B está relacionado com o Convidado A;
- Se o Convidado A está relacionado com o Convidado B e o Convidado B está relacionado com o Convidado C, então o Convidado A está relacionado com o Convidado C.

Relações binárias que satisfazem essas propriedades são chamadas de relações de equivalência.

Definição 5.1. *Uma* relação de equivalência *num conjunto X é uma relação binária $\sim$ em X satisfazendo as seguintes condições:*

(a) para todo $x \in X$, $x \sim x$ (reflexividade);

(b) para todos $x, y \in X$, se $x \sim y$ então $y \sim x$ (simetria);

(c) para todos $x, y, z \in X$, se $x \sim y$ e $y \sim z$ então $x \sim z$ (transitividade).

Se $\sim$ é uma relação de equivalência em X, então a classe de equivalência *de um elemento $x \in X$ (com respeito à relação de equivalência $\sim$) é o subconjunto $[x]$ de X definido por:*

$$[x] = \big\{y \in X : x \sim y\big\}.$$

Exemplo 5.2. *Na relação de equivalência da nossa estória, a classe de equivalência de um de nossos convidados é o conjunto de todos os convidados que moram na mesma casa que ele.*

Note que a relação de igualdade é uma relação de equivalência. Na verdade, relações de equivalência são generalizações da relação de igualdade. Dois elementos distintos de um conjunto são identificados com respeito a alguma propriedade. Por exemplo, digamos que meus amigos Júlia e Léo morem na mesma casa. Claramente, eles são distintos, no entanto do ponto de vista dos convites, eles são tratados como um só.

Exercício 5.3. *Seja S a esfera de $\mathbb{R}^n$, i.e.,*

$$S = \{x \in \mathbb{R}^n \text{ tal que } \|x\| = 1\}.$$

Defina a seguinte relação binária em S:

$$x \sim y \text{ se, e somente se, } x = y \text{ ou } x = -y$$

1. *Mostre que essa é uma relação de equivalência em S.*
2. *Descreva as classes de equivalência de $\sim$.*

Exercício 5.4. *Defina a seguinte relação binária em $\mathbb{R}^n$:*

$$x \sim y \text{ se, e somente se, } \|x\| = \|y\|.$$

1. *Mostre que essa é uma relação de equivalência em $\mathbb{R}^n$.*
2. *Descreva as classes de equivalência de $\sim$.*

Definição 5.5. *Seja X um conjunto. Dadas R_1 e R_2 relações binárias em X, dizemos que R_1 é menor que R_2 se $R_1 \subset R_2$.*

Exercício 5.6. *Seja X um conjunto.*

1. *Existe uma menor relação de equivalência em X? Caso sim, descreva essa relação de equivalência e entenda o conjunto quociente de X por essa relação.*

2. *Existe uma maior relação de equivalência em X. Caso sim, descreva essa relação de equivalência e entenda o conjunto quociente de X por essa relação.*

3. *Dada uma relação binária em X, existe uma relação de* **equivalência** *em X que contenha a relação dada? Caso sim, existe a menor relação de equivalência que contenha a relação dada? Caso sim, descreva um método para a construção dessa menor relação de equivalência.*

Note que a relação de igualdade é uma relação de equivalência. Na verdade, relações de equivalência são generalizações da relação de igualdade. Dois elementos distintos de um conjunto são identificados com respeito a alguma propriedade. Por exemplo, digamos que meus amigos Júlia e Léo morem na mesma casa. Claramente, eles são distintos, no entanto do ponto de vista dos convites, eles são tratados como um só.

Definição 5.7. *Se $\sim$ é uma relação de equivalência num conjunto X, então o* conjunto quociente *$X/\sim$ é o conjunto de todas as classes de equivalência determinadas por $\sim$, ou seja:*

$$X/\sim = \big\{[x] : x \in X\big\}.$$

Em outras palavras, o conjunto quociente de X por uma relação de equivalência é o conjunto obtido colapsando todos os elementos de cada classe de equivalência num único ponto.

Exemplo 5.8. *Como discutido anteriormente, na nossa estória cada classe de equivalência da relação é o conjunto de todos os convidados que moram na mesma casa. O conjunto quociente é a coleção dessas classes de equivalência. Note que se Y denota o conjunto de todos os convites que vamos enviar, então existe uma correspondência bijetora entre Y e o conjunto quociente. Também podemos pensar nesse conjunto quociente como a coleção de todas as casas em que mora algum de nossos convidados.*

Definição 5.9. *Uma* partição *de um conjunto X é uma coleção $\mathcal{A}$ de subconjuntos não vazios de X tal que:*

(a) $X = \bigcup_{A\in\mathcal{A}} A$ *(isto é, para todo $x \in X$, existe $A \in \mathcal{A}$ com $x \in A$);*

(b) para todos $A, B \in \mathcal{A}$, se $A \neq B$ então $A \cap B = \emptyset$.

Exercício 5.10. *Dados um conjunto X e uma relação de equivalência $\sim$ em X, mostre que o conjunto:*

$$\{C \subset X : C \text{ é classe de equivalência de } \sim\}$$

é uma partição de X. Essa partição é chamada de partição gerada por $\sim$.

Na verdade, temos que cada partição de X também gera uma relação de equivalência em X.

Exercício 5.11. *Dados um conjunto X e uma partição P de X, mostre que a seguinte relação binária é uma relação de equivalência em X:*

$$x \sim y \Leftrightarrow \exists A \in P \text{ tal que } x, y \in A.$$

Essa relação é chamada de relação de equivalência gerada por P. Mostre também que a partição gerada por $\sim$ coincide com P.

Exercício 5.12. *Sejam X um conjunto, $\sim$ uma relação de equivalência em X e denote por P a partição gerada por $\sim$. Mostre que a relação de equivalência gerada por P coincide com $\sim$.*

Note que segue dos Exercícios 5.11 e 5.12 que existe uma bijeção entre o conjunto das partições de um conjunto e o conjunto das relações de equivalência nesse conjunto.

No próximo exercício, apresentamos um exemplo de relação de equivalência. Embora, esse tipo de relação de equivalência pareça particular, na verdade ele engloba todas as relações de equivalência, como veremos na Observação 5.16.

Exercício 5.13. *Sejam X e Y conjuntos e $f : X \to Y$ uma função. Mostre que a relação binária $\sim$ em X definida por:*

$$x \sim z \iff f(x) = f(z)$$

é uma relação de equivalência. Essa relação de equivalência é chamada de relação de equivalência determinada por f.

Exercício 5.14. *Se $f : X \to Y$ é uma função e $\sim$ é a relação de equivalência determinada por f, mostre que o conjunto quociente $X/\sim$ é dado por:*

$$X/\sim = \left\{f^{-1}(y) : y \in \mathrm{Im}(f)\right\},$$

isto é, $X/\sim$ é a coleção dos conjuntos de nível de f.

Definição 5.15. *Se $\sim$ é uma relação de equivalência num conjunto X, então a função $q : X \to X/\sim$ definida por:*

$$q(x) = [x], \quad x \in X,$$

é chamada a aplicação quociente *associada à relação de equivalência $\sim$. A aplicação quociente é obviamente sobrejetora.*

Observação 5.16. *Note que a relação de equivalência determinada pela aplicação quociente $q : X \to X/\sim$ é precisamente a relação de equivalência $\sim$, já que:*

$$q(x) = q(y) \iff [x] = [y] \iff x \sim y,$$

para todos $x, y \in X$. Segue então que toda relação de equivalência é determinada por uma função. No entanto, funções diferentes podem definir a mesma relação de equivalência (veja o Exercício 5.21).

Os próximos exercícios tratam do assunto de definição de funções por passagem ao quociente.

Exercício 5.17. *Sejam $f : X \to Y$ uma função, $\sim$ uma relação de equivalência em X e denote por $q : X \to X/\sim$ a aplicação quociente. Mostre que as seguintes afirmações são equivalentes:*

(a) existe uma função $\bar{f} : X/\sim \to Y$ tal que $\bar{f} \circ q = f$;

(b) a relação de equivalência $\sim$ está contida na relação de equivalência determinada por f, isto é, para todos $x, z \in X$, se $x \sim z$ então $f(x) = f(z)$;

(c) f é constante nas classes de equivalência determinadas por $\sim$, isto é, para qualquer $A \in X/\sim$, a função $f|_A$ é constante;

Mostre que se existe uma função $\bar{f} : X/\sim \to Y$ tal que $\bar{f} \circ q = f$, então ela é única. Dizemos que $\bar{f}$ é obtida de f por passagem ao quociente.

Exercício 5.18. *Sejam $f : X \to Y$ uma função, $\sim$ uma relação de equivalência em X e denote por $q : X \to X/\sim$ a aplicação quociente. Assuma que f passa ao quociente, isto é, que existe uma (única) função $\bar{f} : X/\sim \to Y$ tal que $\bar{f} \circ q = f$. Mostre que:*

(a) a função $\bar{f}$ é injetora se e somente se a relação de equivalência determinada por f coincide com $\sim$;

(b) as funções f e $\bar{f}$ possuem a mesma imagem.

Conclua que quando $\sim$ é a relação de equivalência determinada por f então $\bar{f}$ é uma bijeção entre $X/\sim$ e $\mathrm{Im}(f)$. Essa última afirmação é chamada de **Teorema do Isomorfismo** *no contexto de conjuntos.*

Os enunciados dos Exercícios 5.17 e 5.18 podem ser adaptados facilmente para a situação em que a aplicação q é uma aplicação sobrejetora qualquer, e não necessariamente a aplicação quociente determinada por uma relação de equivalência. Esse é o conteúdo dos Exercícios 5.19 e 5.20 a seguir.

Exercício 5.19. *Sejam $f : X \to Y$ uma função e $q : X \to Z$ uma função sobrejetora. Mostre que as seguintes afirmações são equivalentes:*

(a) existe uma função $\bar{f} : Z \to Y$ tal que $\bar{f} \circ q = f$;

(b) a relação de equivalência determinada por q está contida na relação de equivalência determinada por f, isto é, para todos $x, x' \in X$, se $q(x) = q(x')$ então $f(x) = f(x')$;

(c) f é constante nos conjuntos de nível de q, isto é, para todo $z \in Z$, temos que a função $f|_{q^{-1}(z)}$ é constante.

Mostre que se existe uma função $\bar{f} : Z \to U$ tal que $\bar{f} \circ q = f$, então ela é única[2]*. Dizemos que $\bar{f}$ é obtida de f* por passagem ao quociente *através da aplicação q.*

Exercício 5.20. *Sejam $f : X \to Y$ uma função e $q : X \to Z$ uma função sobrejetora. Assuma que f passa ao quociente através da aplicação q, isto é, que existe uma (única) função $\bar{f} : Z \to Y$ tal que $\bar{f} \circ q = f$. Mostre que:*

(a) a função $\bar{f}$ é injetora se e somente se a relação de equivalência determinada por f coincide com a relação de equivalência determinada por q;

(b) as funções f e $\bar{f}$ possuem a mesma imagem.

[2]Na verdade, a sobrejetividade de q é necessária apenas para a unicidade de $\bar{f}$. A equivalência entre (a), (b) e (c) vale mesmo que q não seja sobrejetora, exceto no caso degenerado em que X e Y são vazios, mas Z não é vazio.

Conclua que quando f e q determinam a mesma relação de equivalência então $\bar{f}$ é uma bijeção entre Z e $\mathrm{Im}(f)$.

Exercício 5.21. *Sejam $f : X \to U$, $g : X \to V$ funções sobrejetoras. Mostre que as seguintes afirmações são equivalentes:*

(a) existe uma função bijetora $\phi : V \to U$ tal que $\phi \circ g = f$;

(b) f e g determinam a mesma relação de equivalência em X.

(Sugestão: para mostrar que (b) implica (a), obtenha $\phi = \bar{f}$ passando f ao quociente através de $q = g$. Use o resultado dos Exercícios 5.19 e 5.20.)

6 Anel de polinômios

O objetivo do presente texto é estabelecer algumas propriedades de $K[X]$ que usaremos em nossos estudos. Ao longo de todo o texto, K denota um corpo e $K[X]$ denota o anel de polinômios com coeficientes em K.

Recordamos que, dados polinômios $p_1, \ldots, p_k \in K[X]$ não todos nulos, então o *máximo divisor comum* desses polinômios, denotado por $\mathrm{mdc}\big(p_1, \ldots, p_k\big)$, é o único polinômio mônico $p \in K[X]$ satisfazendo as seguintes condições:

(a) p é um divisor comum de $p_1, \ldots, p_k$, isto é:

$$p | p_i, \quad i = 1, \ldots, k;$$

(b) se $\tilde{p} \in K[X]$ é um divisor comum de $p_1, \ldots, p_k$, então $\tilde{p} | p$.

Vale o *Teorema de Bezout*: dados $p_1, \ldots, p_k \in K[X]$ não todos nulos, então existem $q_1, \ldots, q_k \in K[X]$ tais que:

$$\mathrm{mdc}\big(p_1, \ldots, p_k\big) = q_1 \cdot p_1 + \cdots + q_k \cdot p_k.$$

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

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

Proposição 6.1. *Sejam $p, q_1, q_2 \in K[X]$ e suponha que:*

$$\mathrm{mdc}\big(p, q_1\big) = 1.$$

Se p divide $q_1 \cdot q_2$, então p divide q_2.

Demonstração. Pelo Teorema de Bezout, existem $r, s \in K[X]$ tais que:

$$r \cdot p + s \cdot q_1 = 1;$$

multiplicando ambos os lados da igualdade por q_2, obtemos:

$$r \cdot p \cdot q_2 + s \cdot q_1 \cdot q_2 = q_2.$$

Do fato que p divide $r \cdot p \cdot q_2$ e $s \cdot q_1 \cdot q_2$ segue a conclusão. □

Definição 6.2. *Dizemos que um polinômio $p \in K[X]$ é* irredutível *(em $K[X]$) se* $\text{grau}(p) \geq 1$ *e se dados p_1 e p_2 em $K[X]$ tais que:*

$$p = p_1 \cdot p_2,$$

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

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

Exercício 6.3. *Sejam p e q em $K[X]$ com p irredutível. Mostre que se p não divide q, então* $\text{mdc}\,(p, q) = 1$.

O seguinte resultado é corolário imediato da Proposição 6.1 e do resultado do Exercício 6.3.

Corolário 6.4. *Sejam $p, q_1, q_2 \in K[X]$. Se p é irredutível e p divide o produto $q_1 \cdot q_2$, então ou p divide q_1 ou p divide q_2. Mais geralmente, se $p \in K[X]$ é irredutível e divide um produto $q_1 \cdot \cdots \cdot q_n$, com $q_i \in K[X]$, $i = 1, \ldots, n$, então p divide q_i, para algum $i = 1, \ldots, n$.* □

Definição 6.5. *Sejam $p \in K[X]$ um polinômio irredutível e $q \in K[X]$ um polinômio não nulo. A* multiplicidade *do fator irredutível p em q é o maior inteiro $k \geq 0$ tal que p^k divide q. (Convencionamos que $p^0 = 1$.)*

Obviamente, esse maior inteiro existe, já que se p^k divide q, então

$$k \cdot \text{grau}(p) \leq \text{grau}(q).$$

Além do mais, a multiplicidade do fator irredutível p em q é não nula se, e somente se, p divide q.

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

Exercício 6.6. *Sejam $p \in K[X]$ um polinômio irredutível, $q \in K[X]$ um polinômio não nulo e $k \geq 0$ um inteiro. Mostre que a multiplicidade do fator irredutível p em q é k se, e somente se, existe $r \in K[X]$ tal que $q = p^k \cdot r$ e tal que p não divide r.*

Exercício 6.7. *Seja $q \in K[X]$ um polinômio mônico e escreva:*

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

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

(a) $p \in \{p_1, \dots, p_k\}$ se, e somente se, $p|q$;

(b) se $p = p_i$, para algum $i = 1, \dots, k$, então a multiplicidade do fator irredutível p em q é exatamente o expoente n_i.

Sugestão para os itens (a) e (b): use o Corolário 6.4.

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

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

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

(c) $\{p_1, \dots, p_k\} = \{q_1, \dots, q_l\}$ (em particular $k = l$);

(d) se $p_i = q_j$, com $1 \leq i \leq k$, $1 \leq j \leq l$, então os expoentes n_i e m_j são iguais.

Lema 6.8. *Sejam $k \geq 1$ um inteiro e $p_1, \dots, p_k \in K[X]$ polinômios tais que:*

$$\mathrm{mdc}(p_i, p_j) = 1,$$

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

$$P_i = \prod_{\substack{j=1 \\ j \neq i}}^{k} p_j \in K[X].$$

Então, vale que $\mathrm{mdc}\big(P_1, \dots, P_k\big) = 1$.

Demonstração. Como todo polinômio de grau maior ou igual a 1 tem um divisor irredutível, é suficiente mostrar que $P_1, \ldots, P_k$ não possuem um divisor irredutível comum. Suponha por absurdo que exista um polinômio irredutível $p \in K[X]$ que seja divisor comum dos polinômios $P_1, \ldots, P_k$. Como p divide P_1, pelo Corolário 6.4, p divide p_i, para algum $i = 2, \ldots, k$. Mas p também divide P_i e, novamente do Corolário 6.4 segue que p divide p_j, para algum $j = 1, \ldots, k$, com $j \neq i$. Mas, isso contradiz o fato que o $\mathrm{mdc}(p_i, p_j) = 1$. □

7 Exemplos sobre formas canônicas

Exemplo 7.1. *Seja $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ uma transformação linear cuja matriz numa base ordenada B de $\mathbb{R}^3$ é dada por:*

$$[T]_B = \begin{bmatrix} 2 & 2 & -1 \\ 1 & 0 & 1 \\ 2 & -2 & 3 \end{bmatrix}.$$

O polinômio característico de T é definido como:

$$p_T(x) = det\big([T - x \cdot Id]_B\big) = det \begin{bmatrix} (2-x) & 2 & -1 \\ 1 & -x & 1 \\ 2 & -2 & (3-x) \end{bmatrix}.$$

Calculando o determinante acima, obtemos que:

$$p_T(x) = -(x-1) \cdot (x-2)^2.$$

Dessa forma, os únicos autovalores de T são 1 e 2. Além disso, $m_a(1) = 1$ e $m_a(2) = 2$.

Vamos determinar os autoespaços de T. Inicialmente, estudemos o autoespaço associado ao autovalor 1. Sabemos que, por definição, o autoespaço associado ao 1 é $Ker(T - Id)$. Portanto, um vetor v de $\mathbb{R}^3$ cujas coordenadas na base B são $[v]_B = (x, y, z)$ pertence ao autoespaço associado ao 1 se, e somente se:

$$\begin{bmatrix} 1 & 2 & -1 \\ 1 & -1 & 1 \\ 2 & -2 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = 0.$$

O que é equivalente a (x, y, z) satisfazer:

$$x + 2y - z = 0$$

$$x - y + z = 0$$

$$2x - 2y + 2z = 0.$$

Portanto, temos que

$$Ker(T - Id) = \big\{v \in \mathbb{R}^3 : [v]_B = (x, -2x, -3x), \ para \ \ x \in \mathbb{R}\big\}.$$

Assim, vale que $m_g(1) = 1$.

Agora, estudemos o autoespaço associado ao 2. *Sabemos que o autoespaço associado ao* 2 *é dado por* $Ker(T-2\cdot Id)$. *Logo, temos que um vetor* v *de* $\mathbb{R}^3$ *com coordenadas* $[v]_B = (x, y, z)$ *pertence ao* $Ker(T-2\cdot Id)$ *se, e somente se:*

$$\begin{bmatrix} 0 & 2 & -1 \\ 1 & -2 & 1 \\ 2 & -2 & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = 0.$$

O que é equivalente a (x, y, z) *satisfazer:*

$$2y - z = 0$$

$$x - 2y + z = 0$$

$$2x - 2y + z = 0.$$

Portanto, temos que

$$Ker(T - 2Id) = \big\{v \in \mathbb{R}^3 : [v]_B = (0, y, 2y), \quad \textit{para } y \in \mathbb{R}\big\}.$$

Dessa forma, temos que $m_g(2) = 1$ *o que implica que* T *não é diagonalizável, já que:*

$$1 = m_g(2) < m_a(2) = 2.$$

Exemplo 7.2. *Considere* $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ *a mesma transformação linear do Exemplo 7.1 e vamos determinar o polinômio minimal de* T. *Como* $p_T(T) = 0$, *temos que* m_T *divide* p_T. *Assim, temos que existe* $q \in \mathbb{R}[X]$ *tal que:*

$$p_T(x) = q(x) \cdot m_T(x). \tag{6}$$

Além disso, sabemos que os polinômios minimal e característico possuem as mesmas raízes. O que implica que o polinômio $(x-1)\cdot(x-2)$ *divide* m_T. *Logo, tendo também* (6) *em mente, temos duas possibilidades para o polinômio minimal de* T*:*

$$m_T(x) = (x-1)\cdot(x-2) \quad \textit{ou} \quad m_T(x) = (x-1)\cdot(x-2)^2.$$

Como T *não é diagonalizável, temos que* m_T *não pode ser um produto de polinômios de grau distintos, o que nos leva a concluir que:*

$$m_T(x) = (x-1)\cdot(x-2)^2.$$

Exemplo 7.3. *Seja $T : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ a transformação linear cuja matriz na base ordenada canônica de $\mathbb{R}^2$ é:*

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in M_2(\mathbb{R}).$$

Sabemos que o polinômio característico de T é dado por:

$$p_T(x) = det(A - x \cdot I) = det \begin{bmatrix} -x & -1 \\ 1 & -x \end{bmatrix}.$$

Portanto, temos que $p_T(x) = x^2 + 1$. Como p_T não tem raízes em $\mathbb{R}$, temos que T não possui autovalores. O que implica que T não é diagonalizável.

Note que A também pode ser vista como uma matriz em $M_2(\mathbb{C})$ e portanto, podemos considerar $S : \mathbb{C}^2 \longrightarrow \mathbb{C}^2$ a única transformação linear cuja matriz na base canônica de $\mathbb{C}^2$ é A, onde $\mathbb{C}^2$ está vendo como $\mathbb{C}$-espaço vetorial. É claro que o polinômio característico de S é:

$$p_S(x) = x^2 + 1 \in \mathbb{C}[X].$$

Mas, p_S tem duas raízes em $\mathbb{C}$. Portanto:

$$p_S(x) = (x - i) \cdot (x + i).$$

Note que $m_a(i) = 1$ e $m_a(-i) = 1$, o que implica que $m_g(i) = 1$ e $m_g(-i) = 1$, já que:

$$1 \leq m_g(i) \leq m_a(i) = 1 \quad e$$

$$1 \leq m_g(-i) \leq m_a(-i) = 1.$$

Portanto, temos que S é diagonalizável, já que seu polinômio característico é um produto de fatores de grau 1 e as multiplicidades algébricas e geométricas de seus autovalores coincidem.

Em termos da matriz A, temos que A é semelhante sobre $\mathbb{C}$ a uma matriz diagonal e que A **não** *é semelhante sobre $\mathbb{R}$ a uma matriz diagonal.*

Exemplo 7.4. *Seja $T : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ a transformação linear do Exemplo 7.3. Vamos determinar o polinômio minimal de T. Como visto acima o polinômio característico de T é $p_T(x) = x^2 + 1$. Do fato que $p_T(T) = 0$ segue que m_T divide p_T. No entanto, como $x^2 + 1$ é um polinômio irredutível em $\mathbb{R}[X]$, temos que seus*

únicos divisores são polinômios de grau zero e múltiplos escalares dele mesmo. Portanto, como o minimal é mônico, temos duas possibilidades para o polinômio minimal de T:

$$m_T(x) = 1 \quad ou \quad m_T(x) = x^2 + 1.$$

O que nos leva a concluir que $m_T(x) = x^2 + 1$, já que m_T não pode ser o polinômio constante igual a 1.

Agora, seja $S : \mathbb{C}^2 \longrightarrow \mathbb{C}^2$ a transformação linear dada no Exemplo 7.3. Vimos que:

$$p_S(x) = x^2 + 1 = (x - i) \cdot (x + i).$$

Como o polinômio minimal divide o polinômio característico e ambos possuem as mesmas raízes, concluímos que:

$$m_S(x) = x^2 + 1 = (x - i) \cdot (x + i).$$

Exemplo 7.5. *Seja V um espaço vetorial real de dimensão finita e considere $T : V \longrightarrow V$ uma transformação linear. Suponha que T satisfaça:*

$$T^4 - 3 \cdot T^3 + 2 \cdot T^2 = 0 \quad e$$

que $KerT = KerT^2$. Vamos mostrar que T é diagonalizável.

Por hipótese, temos que o polinômio

$$p(x) = x^4 - 3 \cdot x^3 + 2 \cdot x^2 = x^2 \cdot (x^2 - 3 \cdot x + 2) = x^2 \cdot (x - 1) \cdot (x - 2)$$

anula T. Além disso, note que:

$$mdc\big(x^2, (x-1)\big) = mdc\big(x^2, (x-2)\big) = mdc\big((x-1), (x-2)\big) = 1.$$

Portanto, como visto em aula, temos que:

$$V = KerT^2 \bigoplus Ker(T - Id) \bigoplus Ker(T - 2 \cdot Id). \tag{7}$$

Da hipótese que $KerT^2 = KerT$ e da igualdade (7) segue que:

$$V = KerT \bigoplus Ker(T - Id) \bigoplus Ker(T - 2 \cdot Id),$$

o que implica que T é diagonalizável.