álgebra linear

versão 130

3 de setembro de 2015

jerônimo c. pellegrini

Sumário

Apresentação

Este texto foi elaborado como um primeiro curso de Álgebra Linear, desenvolvendo conceitos básicos na primeira parte e avançando para outros tópicos e aplicações na segunda parte.

O texto começa com espaços vetoriais e aborda matrizes somente após transformações lineares. Isso é feito por diferentes motivos: primeiro, para que o leitor tenha tempo para digerir os conceitos abstratos apresentados inicialmente. Se a abstração é construída aos poucos, corre-se o risco de não haver tempo para que essas abstrações sejam devidamente digeridas; além disso, para não passar inicialmente a impressão de que a Álgebra Linear trata simplesmente de álgebra de matrizes reais, para que de imediato fique claro que espaços vetoriais não são necessariamente compostos apenas de tuplas (há espaços de dimensão infinita que são facilmente descritos), e também para ilustrar de imediato a natureza abstrata da Álgebra, e da sua relevância em problemas práticos: ao final do primeiro capítulo há vários exemplos de uso de espaços vetoriais em Criptografia, códigos corretores de erros e na solução do cubo mágico. Há também uma boa quantidade de aplicações ao final de todos os outros Capítulos.

Os exemplos e aplicações são incluídos no *final* dos capítulos, e não no início. Isso contraria a idéia de que os conceitos apresentados devem ser motivados. Penso que a motivação deveria ser substituída, pelo menos no início da leitura, por *confiança:* o leitor deve confiar em que existe uma razão para estudar toda a abstração e o ferramental apresentado, por mais estranhos que lhe pareçam. Terminando cada capítulo, haverá a oportunidade de confirmar a utilidade dos tópicos estudados.

Os pré-requisitos imprescindíveis para a leitura deste livro são Cálculo em uma variável real e Geometria Analítica. Alguns dos exemplos farão uso de Cálculo em várias variáveis, números complexos, probabilidade básica, grafos e equações diferenciais – mas estes exemplos podem ser deixados de lado sem comprometer a sequência do texto. Para que o livro seja tão autocontido quanto possível, há um apêndice com uma revisão de sistemas lineares e matrizes, um introduzindo o método da indução finita, e um com noções básicas de Equações Diferenciais.

Seções, exemplos e exercícios marcados com estrela (★) são opcionais, ou porque são difíceis ou porque usam conceitos normalmente não abordados em um primeiro curso de Álgebra Linear, como corpos finitos.

Nomenclatura

Vetores (elementos de um espaço vetorial, não apenas vetores em $\mathbb{R}^n$) são grafados em negrito: $\mathbf{v}, \mathbf{w}, \ldots$.

Representamos vetores em $\mathbb{R}^n$ como vetores-coluna em todo o texto:

$$\mathbf{v} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}.$$

Em texto corrido e em muitas fórmulas, denotamos tais vetores como transpostas de linhas: $\mathbf{v} = (v_1, v_2, \ldots, v_n)^T$.

Em diversas ocasiões, somatórios são denotados apenas por

$$\sum_i \cdots,$$

ao invés de

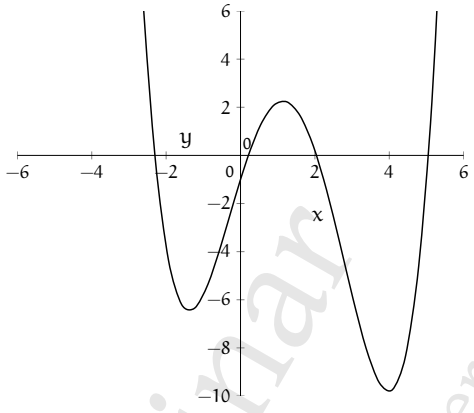
$$\sum_{i=1}^{n} \cdots,$$

sendo sempre possível determinar, a partir do contexto, quais os valores do índice i.

Frações são fatoradas para fora de matrizes sempre que é possível fazê-lo, para tornar matrizes mais facilmente legíveis e simplificar operações de multiplicação:

$$\begin{pmatrix} 0 & \frac{1}{6} & -\frac{1}{6} \\ \frac{7}{6} & \frac{\sqrt{2}}{6} & \frac{5}{6} \\ \frac{1}{3} & \frac{11}{6} & -\frac{13}{6} \end{pmatrix} \longrightarrow \quad \frac{1}{6}\begin{pmatrix} 0 & 1 & -1 \\ 7 & \sqrt{2} & 5 \\ 2 & 11 & -13 \end{pmatrix}.$$

Não usamos setas para representar os eixos em $\mathbb{R}^2$ e $\mathbb{R}^3$, porque as reservamos para vetores. Por exemplo, o gráfico da função $\frac{x^4}{5} - x^3 - x^2 + 5x - 1$ é mostrado na próxima figura.



A nomenclatura usada no livro é detalhada a seguir.

$\lfloor x \rceil$ O inteiro mais próximo de x, página 417

(a_n) sequência, página 18

(f_n) Sequencia de funções, página 430

2^A Conjunto de todos os subconjuntos do conjunto A, página 46

$[\mathbf{v}]_B$ Coordenadas do vetor $\mathbf{v}$ na base B, página 70

$[A]_{ij}$ Matriz A após remoção da linha i e coluna j, página 192

$[X]$ Espaço gerado pelo conjunto de vetores X, página 53

$[x]$ dimensão de uma grandeza física, página 73

$[\mathrm{id}]_{\alpha \to \beta}$ Matriz de mudança de base, de α para β, página 129

$\lceil x \rceil$ "arredondamento para cima" (menor inteiro maior ou igual a x), página 531

$\circ$ Composição de transformações lineares (e de funções), página 90

$\mathrm{cof}(A, i, j)$ Cofator do elemento a_{ij} da matriz A, página 192

$\rho(X, Y)$ Correlação entre variáveis aleatórias X e Y, página 305

$\mathrm{cov}(X, Y)$ Covariância entre variáveis aleatórias X e Y, página 304

$\det A$ Determinante da matriz A, página 183

$\mathrm{diag}(A_1, \ldots A_k)$ Matriz diagonal com blocos $A_1, \ldots, A_k$ formando a diagonal., página 120

$\mathrm{diag}(a_1, \ldots, a_n)$ Matriz diagonal com elementos $a_1, \ldots, a_n$ na diagonal., página 459

$\dim V$ Dimensão do espaço vetorial V, página 59

$\mathbf{v} \times \mathbf{w}$ Produto vetorial dos vetores $\mathbf{v}$ e $\mathbf{w}$, página 3

$\operatorname{vol} A$ volume do objeto geométrico A, página 415

$\operatorname{vol} A$ volume do objeto geométrico A, página 182

$\wedge$ "E" lógico, página 8

A^* Conjugado transposto de A, página 157

A^+ Pseudoinversa da matriz A, página 327

A^H Conjugado transposto de A, página 157

A^H Matriz adjunta de A, página 234

$C[a, b]$ Conjunto (e espaço vetorial) das funções contínuas em $[a, b]$, página 30

C^0 Conjnuto (e espaço vetorial) das funções contínuas em $\mathbb{R}$, página 30

C^k Conjnuto (e espaço vetorial) das funções k vezes diferenciáveis em $\mathbb{R}$, página 30

$d(\mathbf{v}, \mathbf{w})$ Distância entre os vetores $\mathbf{v}$ e $\mathbf{w}$, página 280

E_n Erro na aproximação de série com n termos, página 431

L^2 Espaço de funções quadrado-integráveis, página 432

L_G Matriz Laplaciana do grafo G, página 262

$M_{m,n}$ Conjunto (e espaço vetorial) das matrizes $m \times n$, página 65

$O(B)$ Orientação da base B, página 183

S_n Conjunto de todas as permutações de n elementos, página 194

S_n Soma parcial de série, página 431

$V(k_1, \ldots, k_n)$ Matriz de Vandermonde obtida de $k_1, \ldots, k_n$, página 210

V^* Espaço dual, página 450

V^* Espaço dual, página 141

Capítulo 1

Espaços Vetoriais

A Álgebra Linear pode ser vista como uma generalização natural da Geometria Analítica. Da mesma forma que, na Geometria, somamos pares de vetores e multiplicamos vetores por escalares, podemos fazê-lo com outros objetos – matrizes ($A + B$, kA), funções ($(f + g)(x)$, $kf(x)$), sequências ($(a_n) + (b_n)$, $k(a_n)$).

A Álgebra tem como objeto de estudo o comportamento de operações definidas sobre conjuntos. A Álgebra Linear trata epecificamente de *espaços vetoriais*: conjuntos onde são definidas as operações de soma e multiplicação, de forma que fique bem definida também a expressão $ax + b$.

Os espaços vetoriais são um dos mais importantes exemplos de estrutura algébrica. A idéia abstrata de espaço vetorial generaliza o conceito de vetores no espaço tridimensional de duas maneiras. Primeiro, espaços vetoriais podem ter dimensão maior que tres. E segundo, definimos espaços vetoriais não apenas com vetores "geométricos", mas com diferentes objetos matemáticos (por exemplo números, matrizes, polinômios, funções) – e podemos tratar desses objetos de forma unificada.

A fim de melhor contextualizar a definição de espaço vetorial, este Capítulo traz uma breve descrição do que é uma estrutura algébrica, descrevendo também grupos e corpos.

1.1 Estruturas algébricas

Além de números, podemos somar e multiplicar outros objetos – o exemplo mais simples talvez seja o de matrizes. Quando definimos soma e multiplicação para objetos diferentes, estas operações podem ou não ter propriedades semelhantes. Tanto para números reais como para matrizes, a soma é associativa: $a + (b + c) = (a + b) + c$. No entanto, a multiplicação de números reais é comutativa ($ab = ba$), mas a comutatividade não vale, de forma geral, para a multiplicação de matrizes.

Ao estudar diferetes tipos de objetos e operações definidas sobre eles, identificamos algumas classes de objetos para os quais as operações se comportam de maneira semelhante. Damos a essas classes de objetos com operações algébricas o nome de *estrutura algébrica*.

Estrutura algébrica (ou *sistema algébrico*) é o nome dado a um conjunto com algumas operações definidas sobre ele. Por exemplo, o conjunto dos números reais com as operações de soma e multiplicação, $(\mathbb{R}, +, \cdot)$ é uma estrutura algébrica. O conjunto das matrizes com a operação de soma de matrizes e a operação de multiplicação por escalar $(M, +, \cdot)$ é outra estrutura algébrica. Um terceiro exemplo de estrutura algébrica é o conjunto dos inteiros com a operação de soma, $(\mathbb{Z}, +)$. Cada um destas estruturas tem características diferentes, e pode ser classificada de maneiras diferentes, como veremos a seguir.

Antes de definirmos algumas estruturas algébricas, definimos o tipo de operação que acompanharão estas estruturas. Neste texto, trataremos de operações com dois argumentos, chamadas de *operações binárias*.

Definição 1.1 (Operação binária)**.** Uma *operação* em um conjunto A é uma função que leva um ou mais elementos de A em outro elemento de A – ou seja, é uma função $f : A \times A \times \cdots \times A \to A$.

Dizemos que uma operação é *binária* se aceita dois argumentos – ou seja, é da forma $f : A \times A \to A$.

Dizemos que uma operação binária é *associativa*, se $a \star (b \star c) = (a \star b) \star c$ e *comutativa*, se $a \star b = b \star a$.

Um elemento $e \in A$ é *neutro* para a operação $\star$ se para todo $a \in A$, $a \star e = e \star a = a$. ♦

Exemplo 1.2. Em $\mathbb{R}$, as operações de soma e multiplicação são associativas e comutativas, porque

$$x + y = y + x \qquad \text{(comutatividade)}$$
$$x + (y + z) = (x + y) + z \qquad \text{(associatividade)}$$

$$xy = yx \qquad \text{(comutatividade)}$$
$$x(yz) = (xy)z \qquad \text{(associatividade)}$$

No entanto, as operações de divisão e subtração não são comutativas. A subtração é associativa, e a divisão não é:

$$x - y \neq y - x \qquad \text{(não vale a comutatividade)}$$
$$x - (y - z) = (x - y) - z \qquad \text{(associatividade)}$$

$$x/y \neq y/x \qquad \text{(não vale a comutatividade)}$$
$$x/(y/z) \neq (x/y)/z \qquad \text{(não vale associatividade)}$$

O neutro para soma é o zero, e o neutro para multiplicação é o um porque

$$0 + x = x$$
$$(1)x = x$$

Não definimos neste texto neutro para subtração e divisão, porque as operações não são comutativas, e o neutro e teria que satisfazer $x - e = e - x = x$, e $x/e = e/x = x$, que não sería possível. ◀

Exemplo 1.3. No conjunto de matrizes quadradas de ordem n, a operação de soma é comutativa e associativa, porque para duas matrizes A e B, temos

$$A + B = B + A \qquad \text{(comutatividade)}$$
$$A + (B + C) = (A + B) + C \qquad \text{(associatividade)}$$

No entanto, a operação de multiplicação é associativa, mas não comutativa:

$$AB \neq BA \qquad \text{(não vale a comutatividade)}$$
$$A(BC) = (AB)C \qquad \text{(associatividade)}$$

O neutro para a soma de matrizes é a matriz zero (ou seja, a matriz cujos elementos são todos zero).

O neutro para multiplicação de matrizes é a identidade, porque, *apesar da multiplicação de matrizes não ser comutativa*, temos

$$\mathcal{I}A = A\mathcal{I} = A,$$

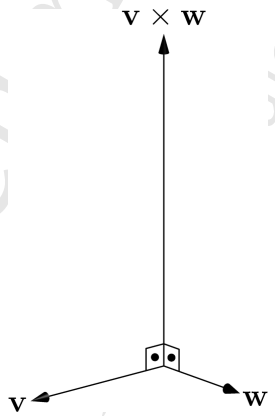
para toda matriz quadrada A. ◀

Exemplo 1.4. O produto vetorial em $\mathbb{R}^3$ é definido como

$$\begin{aligned}\mathbf{v} \times \mathbf{w} = &(x_2y_3 - x_3y_2)\mathbf{e_1} \\ &+ (x_3y_1 - x_1y_3)\mathbf{e_2} \\ &+ (x_1y_2 - x_2y_1)\mathbf{e_3},\end{aligned}$$

onde $\mathbf{e_1}$, $\mathbf{e_2}$ e $\mathbf{e_3}$ são os vetores unitários nas direções dos eixos **x**, **y** e **z** (também os chamamos de *versores*).

O resultado do produto vetorial $\mathbf{v} \times \mathbf{w}$ é um vetor **s**, perpendicular tanto a **v** como a **w**. Por exemplo, se $\mathbf{v} = (3, 0, 0)^T$ e $\mathbf{w} = (0, 2, 0)^T$, o produto vetorial $\mathbf{s} = \mathbf{v} \times \mathbf{w}$ é $(0, 0, 6)^T$, ortogonal a ambos.



A magnitude de **s** é zero quando **v** e **w** são paralelos e é igual ao produto das magnitudes de **v** e **w** quando estes são perpendiculares.

Esta operação não é comutativa, porque

$$\mathbf{v} \times \mathbf{w} = -(\mathbf{w} \times \mathbf{v}).$$

A operação também não é associativa, porque

$$\mathbf{u} \times (\mathbf{v} \times \mathbf{w})$$

é um vetor no mesmo plano que **v** e **w**, enquanto

$$(\mathbf{u} \times \mathbf{v}) \times \mathbf{w}$$

é um vetor no mesmo plano que **u** e **v**. ◀

Definição 1.5 (Fechamento)**.** Seja A um conjunto com uma operação $\star$, e seja $B \subseteq A$. Dizemos que B é dito *fechado* sob a operação $\star$ se e somente se a operação com dois elementos de B sempre resulta em outro elemento de B – ou seja, $\forall x, y \in B, x \star y \in B$. ♦

Exemplo 1.6. As quatro operações aritméticas definidas nos reais são operações binárias. Além disso, nos reais a soma e a multiplicação são comutativas ($a + b = b + a$) e associativas ($a + (b + c) = (a + b) + c$).

Os reais são fechados para as quatro operações.

Poderíamos tentar definir as quatro operações aritméticas para os inteiros, mas não vale o fechamento: a operação de divisão não tem como ser definida. A intuição nos diz que podemos dividir $9/3$ e obter 3, mas não o podemos fazer para *quaisquer* dois inteiros – por isso não definimos esta operação para o conjunto dos inteiros, porque os inteiros não são fechados para a divisão. ◀

1.2 Grupos

Como primeiro exemplo de estrutura algébrica, tomamos os *grupos*.

Definição 1.7 (Grupo)**.** Um grupo é um conjunto não-vazio G associado a uma operação binária $\cdot : G \times G \to G$ tendo as propriedades listadas a seguir.

- **Associatividade:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Existencia de neutro:** Deve existir um elemento neutro $e \in G$ para a operação de grupo: $\exists e \in G : a \cdot e = e \cdot a = a$.
- **Existencia de inverso:** Para todo $a \in G$, há um *inverso* $a' \in G$ tal que $a \cdot a' = a' \cdot a = e$.

Se a operação do grupo for comutativa, dizemos que o grupo é *comutativo* (ou *abeliano*[1]). ♦

Exemplo 1.8. Os inteiros com a operação usual de soma formam um grupo: (i) a soma de dois inteiros é um inteiro; (ii) a soma é associativa; (iii) o inteiro zero é neutro para soma; e (iv), para todo inteiro a, existe um inteiro $-a$ tal que $a + (-a) = 0$. O grupo também é comutativo. ◀

Os conjuntos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ também formam grupo com a operação usual de adição.

Demonstramos um teorema básico sobre grupos.

Teorema 1.9. *Seja* G *um grupo e* $x \in G$*. Então o inverso* x' *de* x *é único em* G*.*

Demonstração. Seja $x \in G$ e a, b inversos de x. Então

$$\begin{aligned} a &= ae && \\ &= a(xb) && xb = e,\ \text{b é inverso de x} \\ &= (ax)b && \text{associatividade} \\ &= eb && ax = e,\ \text{a é inverso de x} \\ &= b. && \end{aligned}$$

■

Exemplo 1.10. O conjunto $\{+1, -1\}$ com a operação usual de multiplicação é um grupo: (i) $1 \cdot 1$, $1 \cdot -1$, $-1 \cdot 1$, $-1 \cdot -1$ pertencem ao grupo; (ii) a operação é associativa; (iii) 1 é neutro; (iv) tanto 1 como -1 são seus próprios inversos. ◀

[1] "Abeliano" refere-se ao matemático Norueguês Niels Henrick Abel, que deerminou que a comutatividade de certos grupos estava relacionada com a possibilidade de cálculo das raízes de polinômios.

Exemplo 1.11. O conjunto de triplas[2] $(x, y, z)^T \in \mathbb{R}^3$, que representam vetores no espaço tridimensional, com a operação de soma de vetores:

$$(x, y, z) + (a, b, c) = (x + a, y + b, z + c)$$

é um grupo: (i) a soma de dois vetores é um vetor também com três números reais; (ii) a soma é associativa; (iii) o vetor zero é neutro; (iv) para todo vetor $\mathbf{v} = (x, y, z)$, existe um vetor $-\mathbf{v} = (-x, -y, -z)$ tal que $\mathbf{v} + (-\mathbf{v}) = (0, 0, 0)$. Além disso, o grupo é comutativo. ◀

Exemplo 1.12. O conjunto $\mathbb{R}^*$ com a operação de exponenciação *não* é um grupo, porque não vale a associatividade ($(a^b)^c \neq a^{(b^c)}$). ◀

Exemplo 1.13. O conjunto de *todas* as funções de $\mathbb{R}$ em $\mathbb{R}$, com a operação de soma de funções, é um grupo.

- A soma de funções é associativa: $f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x)$, para todas funções f, g, h e todo $x \in \mathbb{R}$.
- A função zero, $z(x) = 0$, é o elemento neutro para a operação de soma: $f(x)+z(x) = f(x)+0 = f(x)$, para todos f e x.
- Há um inverso para toda função: $f(x)$ tem como inversa a função $g(x) = -f(x)$, porque $f(x) + [-f(x)] = z(x)$. ◀

Exemplo 1.14. Dadas duas funções f e g, a *composição* de f com g, que denotamos $f \circ g$, é tal que $f \circ g(x) = f(g(x))$.

Por exemplo, se $f(x) = 1/x$ e $g(x) = \log(x)$, então $(f \circ g)(x)$ é $1/\log(x)$.

O conjunto de todas as funções bijetoras de reais em reais com a operação de composição é um grupo:

- a composição de funções é associativa: $f \circ (g \circ h) = (f \circ g) \circ h$.
- A função identidade $f(x) = x$ é o elemento neutro para a operação de composição porque para toda função g, $f(g(x)) = g(x)$.
- Como nos restringimos ao conjunto das funções bijetoras, todas tem inversa: $f \circ f^{-1}$ é a identidade. ◀

Exemplo 1.15. O conjunto das matrizes quadradas de ordem n, com a operação de soma de matrizes, é um grupo, porque:

- A soma de duas matrizes $n \times n$ resulta em outra matriz $n \times n$.
- A soma de matrizes é associativa.
- A matriz Z com todas as entradas iguais a zero funciona como elemento neutro, porque $A + Z = A$ para toda matriz A.
- Toda matriz A tem inverso para a operação de soma: $A + [(-1)A] = Z$, onde "$(-1)A$" é a matriz A com seus elementos multiplicados por -1, e Z é a matriz zero.

[2] Neste texto, adotamos a representação de vetores como coluna por padrão.

Já o mesmo conjunto, das matrizes quadradas de ordem n, com a operação de multiplicação de matrizes, não é um grupo, porque nem toda matriz tem inversa.

No entanto, o conjunto das matrizes *não-singulares* de ordem n, com a operação de multiplicação de matrizes, é um grupo. ◀

Exemplo 1.16. O conjunto $\mathbb{R} \setminus \{-1\}$ com a operação $\star$, definida como

$$a \star b = ab + a + b$$

é um grupo: (i) se $a, b \neq -1$, então $ab + a + b \neq -1$ e portanto pertence ao grupo; (ii) a operação é associativa; (iii) zero é identidade para $\star$; (iv) o inverso de a é $-a/(a+1)$.

Desenvolvemos detalhadamente as propriedades (ii) e (iii).

(ii)

$$\begin{aligned}(a \star b) \star c &= (ab + a + b) \star c \\ &= (ab + a + b)c + (ab + a + b) + c \\ &= abc + ac + bc + ab + a + b + c \\ &= abc + ac + ab + a + bc + b + c \\ &= a(bc + b + c) + a + bc + b + c \\ &= a \star (b \star c)\end{aligned}$$

(iii)

$$\begin{aligned}a \star \frac{-a}{a+1} &= \frac{-a^2}{a+1} + a - \frac{a}{a+1} \\ &= \frac{-a^2}{a+1}\frac{a(a+1) - a}{a+1} \\ &= \frac{-a^2 + a^2 + a - a}{a+1} \\ &= 0.\end{aligned}$$

O grupo também é comutativo. ◀

Exemplo 1.17. Dado um natural $n > 0$, o conjunto de todas as matrizes invertíveis $n \times n$ é um grupo com a operação usual de multiplicação de matrizes: (i) se A, B são $n \times n$, então AB será também uma matriz $n \times n$; (ii) a multiplicação de matrizes é operação associativa; (iii) o elemento identidade é a matriz identidade (iv) todas as matrizes do grupo são invertíveis.

Este grupo, no entanto, não é comutativo, já que a multiplicação de matrizes não é, de maneira geral, comutativa. ◀

1.3 Corpo

Definição 1.18. Um *corpo* consiste de um conjunto e duas operações, denotadas $\cdot$ e $+$, com as propriedades listadas a seguir.

- As duas operações são associativas.

- As duas operações são comutativas.
- Vale a distributividade de $\cdot$ sobre $+$.
- Há elementos neutros 0 para soma e 1 para multiplicação.
- Todo elemento do corpo tem um inverso aditivo.
- Todo elemento diferente de 0 tem inverso multiplicativo. ♦

Exemplo 1.19. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são corpos.
Para todos estes conjuntos,

- $+$ e $\cdot$ são associativas e comutativas para números reais.
- Vale a distributividade: $a(b + c) = ab + ac$ para quaisquer a, b e c reais.
- O zero é neutro para soma de reais: $a+0 = a$ para todo a; O um é neutro para multiplicação: $1a = a$ para todo a.
- Para todo real a existe um inverso aditivo, $(-1)a$, tal que $(-1)a + a = 0$.
- Todo $a \neq 0$ tem inverso multiplicativo, que denotamos a^{-1}, tal que $aa^{-1} = 1$.

O mesmo argumento pode ser repetido para $\mathbb{Q}$ e $\mathbb{C}$.

Há diferenças importantes entre estes três corpos: o corpo dos racionais não é *completo* (não contém os irracionais, que não podem ser representados como fração); o corpo dos reais é completo e ordenado, mas não inclui soluções para a inequação $x^2 < 0$; os complexos já incluem estas soluções, porque contém a unidade imaginária $i = \sqrt{-1}$, mas não se pode ordená-los. ◀

Exemplo 1.20. Fixado um número n, denotamos o conjunto de todas as matrizes de ordem n por $M_{n\times n}$. Este conjunto *não* é um corpo com as operações de soma e multiplicação de matrizes, porque:

- Nem toda matriz diferente de zero tem inversa;
- A operação de multiplicação não é comutativa[3]. ◀

Exemplo 1.21. Seja $\mathbb{Q}[\sqrt{2}]$ o conjunto dos números da forma $a + b\sqrt{2}$, onde $a, b \in \mathbb{Q}$, com adição e multiplicação usuais. Este conjunto é um corpo:

- As operações são as usuais, portanto são associativas e comutativas, e vale a distributividade.
- Há neutros: $0 + 0\sqrt{2}$ para adição e $1 + 0\sqrt{2}$ para multiplicação.
- Para todo $a + b\sqrt{2}$ existe inverso aditivo $-a - b\sqrt{2}$.
- Para todo $(a + b\sqrt{2}) \neq 0$ existe inverso multiplicativo

$$\frac{1}{a + b\sqrt{2}} = \left(\frac{1}{a + b\sqrt{2}}\right)\left(\frac{a - b\sqrt{2}}{a - b\sqrt{2}}\right)$$

[3] Um *anel* é o mesmo que um corpo, exceto que não vale a comutatividade para multiplicação, e os elementos não necessariamente tem inverso multiplicativo (ou seja, não se define a operação de divisão). $M_{n\times n}$ é um anel.

$$= \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$
$$= \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2},$$

e o inverso multiplicativo de $a + b\sqrt{2}$ também é da forma $x + y\sqrt{2}$. Observamos que $a^2 - 2b^2 \neq 0$ quando $a, b \neq 0$.

- Finalmente, a soma e multiplicação de elementos em $\mathbb{Q}[\sqrt{2}]$ resulta em elementos em $\mathbb{Q}[\sqrt{2}]$. Somando,
$$a + b\sqrt{2} + x + y\sqrt{2} = (a + x) + (b + y)\sqrt{2}.$$
Multiplicando:
$$\begin{aligned}(a + b\sqrt{2})(x + y\sqrt{2}) &= ax + ay\sqrt{2} + bx\sqrt{2} + b\sqrt{2}y\sqrt{2} \\ &= ax + ay\sqrt{2} + bx\sqrt{2} + 2by \\ &= (ax + 2by) + (ay + bx)\sqrt{2}.\end{aligned}$$ ◀

O próximo exemplo é o corpo $\mathbb{Z}_2$, de extrema importância em Computação. Este corpo é diferente dos outros corpos que apresentamos por ser finito.

Exemplo 1.22. Neste exemplo exploramos um corpo com apenas dois elementos. Podemos representar os valores lógicos "verdadeiro" e "falso" como 0 e 1, e estes serão os elementos de nosso corpo.

As operações que definiremos são as duas operações lógicas a seguir:

- "**e**", também denotado por $\wedge$. Por definição, o "e" de a e b é um se e somente se tanto a como b valem um. A tabela-verdade da operação é

a	b	$(a \wedge b)$
0	0	0
0	1	0
1	0	0
1	1	1

- "**ou-exclusivo**", também denotado por $\oplus$. Por definição, o ou-exclusivo de a com b é um se e somente se a e b tem valores diferentes (um deles é zero e outro é um). A tabela-verdade da operação é

a	b	$(a \oplus b)$
0	0	0
0	1	1
1	0	1
1	1	0

O conjunto $\{0, 1\}$ com as operações lógicas $\wedge$ ("e") e $\oplus$ ("ou exclusivo") é um corpo: (i) as duas operações são associativas; (ii) as operações são também comutativas; (iii) $\wedge$ é distributiva sobre $\oplus$ – $a \wedge (b \oplus c) =$

$(a \wedge b) \oplus (a \wedge c)$; (iv) há elementos neutros: 0 para $\oplus$ e 1 para $\wedge$; (v) todo elemento do corpo é seu próprio inverso aditivo; (vi) O único elemento diferente de 0 (o 1) tem inverso multiplicativo (ele mesmo).

Este corpo é chamado de $\mathbb{Z}_2$, porque é subconjunto dos inteiros com dois elementos[4]. Observe que as operações $\oplus$ e $\wedge$ também podem ser descritas usando soma e multiplicação: se a e b pertencem a $\{0, 1\}$, então

- $a \oplus b$ é o mesmo que o resto da divisão de $a + b$ por 2, e
- $a \wedge b$ é o mesmo que ab. ◀

As operações em $\mathbb{Z}_2$ (e, ou-exclusivo) são normalmente implementadas por circuitos lógicos usados na construção de computadores e outros dispositivos digitais.

★ **Exemplo 1.23.** Este exemplo está em nível de abstração acima do resto do texto, e deve ser considerado opcional.

Um número é chamado de *algébrico* se é raiz de algum polinômio

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

onde os a_i são inteiros. Um número que não é algébrico é chamado de *transcendental*.

O conjunto de todos os números algébricos é um corpo, chamado de *corpo de números algébricos*, muitas vezes denotado por $\mathbb{A}$. Este corpo contém $\mathbb{Q}$, $i = \sqrt{-1}$, todos os múltiplos de i com coeficientes racionais, a razão áuera[5] φ, mas não contém números transcendentais como π e e. Alguns outros números transcendentais (e que portanto *não* pertencem a $\mathbb{A}$) são

- $2^{\sqrt{2}}$, o número de Hilbert.
- sen 1, e de maneira geral sen x, cos x e tan x para todo número algébrico x diferente de zero.
- $i^i = e^{-\pi/2} = 0.207879576\ldots$
- $0.12345678910111213141516\ldots$, o número de Champernowne, que é construído concatenando os dígitos dos números naturais $1, 2, 3, \ldots$

Há aplicações importantes deste corpo – por exemplo, os números algébricos são usados em um método para obter a fatoração de números inteiros grandes, algo de grande relevância em Criptanálise.

Não mostraremos neste texto que $\mathbb{A}$ é um corpo. ◀

[4] Este corpo também é chamado de GF_2, onde GF significa "*Galois Field*", corpo de Galois – um corpo "de Galois" é um corpo finito. O nome é referencia ao matemático Francês Évariste Galois, que foi quem introduciu a idéia de corpos com quantidade finita de elementos.

[5] φ é a razão a/b para todos reais tais que $\frac{a+b}{a} = \frac{a}{b}$. A razão áurea está presente na Natureza de diversas formas, e é importante em muitas áreas das Ciências e Artes. Seu valor é $\frac{1+\sqrt{5}}{2}$, também igual à fração

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}.$$

★ 1.3.1 Operando com corpos

Tudo o que pudermos fazer usando as operações de corpo em números reais, também podemos fazer com outros corpos. Em particular, é interessante observar que podemos resolver equações e sistemas de equações em qualquer corpo.

Exemplo 1.24. Facilmente resolvemos a equação linear $2x + 3 = 10$ em $\mathbb{R}$, isolando x e obtendo

$$x = \frac{10-3}{2} = \frac{7}{2}.$$

Agora resolvemos equações lineares em corpos diferentes. Por *lineares* entendemos equações onde uma incógnita pode aparecer multiplicada por uma constante (ou seja, um elemento do corpo), mas não por outra incógnita ou por ela mesma.

Primeiro, resolvemos $3x + 10 + \sqrt{2} = 1 + 16\sqrt{2}$ em $\mathbb{Q}[\sqrt{2}]$: isolamos x e obtemos

$$\begin{aligned} 3x &= 1 - 10 + 16\sqrt{2} - \sqrt{2} \\ 3x &= -9 + 15\sqrt{2} \\ x &= -3 + 5\sqrt{2}. \end{aligned}$$

Este exemplo parece bastante natural, porque realizamos as operações usuais de soma e multiplicação, e suas inversas (subtração e divisão). Resolvemos agora uma equação em $\mathbb{Z}_2$. Como os elementos do corpo são apenas 0 e 1, somente eles podem ser usados na equação (ou seja, as constantes e incógnitas valem 0 ou 1). Em $\mathbb{Z}_2$, as operações que usamos são soma (ou exclusivo) e multiplicação ("e" lógico). Observamos que neste corpo a função inversa da soma é ela mesma, porque

$$1 \oplus 1 = 0.$$

Embora isto possa, em um primeiro contato, parecer incorreto, nada na definição de corpo impede que somar dois números seja o mesmo que somar um número com seu inverso aditivo.

Resolveremos agora a equação $1 \wedge x \oplus 1 = 1$. Isolamos x:

$$\begin{aligned} 1 \wedge x \oplus 1 &= 0 \\ x \oplus 1 &= 0 && \text{(porque } 1 \wedge x = x\text{)} \\ x \oplus 1 \oplus 1 &= 0 \oplus 1 \\ x \oplus 0 &= 1 \\ x &= 1. \end{aligned}$$

◄

Exemplo 1.25. Também podemos resolver sistemas de equações lineares. Neste exemplo denotamos $\wedge$ por $\cdot$ para que a notação fique mais limpa; por exemplo, ao invés de $1 \wedge a \oplus 0 \wedge b$, escrevemos $1a + 0b$.

Em $\mathbb{Z}_2$, resolvemos um sistema 2×2.

$$\begin{cases} 1x \oplus 1y = 1 \\ 0x \oplus 1y = 1 \end{cases}$$

Como $0x = 0$, e $1y = 1$, da segunda equação temos $0 \oplus y = 1$, e segue imediatamente que $y = 1$. Substituindo na primeira equação, obtemos

$$1x \oplus 1 \cdot 1 = 1$$

$$\begin{aligned} x \oplus 1 \cdot 1 &= 1 && (1x = x) \\ x \oplus 1 &= 1 && (1 \cdot 1 = 1) \\ x &= 0 \end{aligned}$$

Verificamos agora a solução que encontramos ($x = 0, y = 1$):

$$\begin{cases} +1(0) \oplus 1(1) = 1 \\ +0(0) \oplus 1(1) = 1 \end{cases}$$

que se traduz em

$$\begin{cases} +0 \oplus 1 = 1 \\ +0 \oplus 1 = 1 \end{cases}$$

que está de acordo com o que esperávamos.

A solução de sistemas de equações em $\mathbb{Z}_2$ é de grande importância em Criptografia e Criptanálise. ◀

1.4 Espaços vetoriais

Um espaço vetorial é uma estrutura que generaliza as propriedades de vetores em $\mathbb{R}^3$, como as conhecemos da Geometria Analítica. Em um espaço vetorial podemos somar elementos e realizar multiplicação – não por elementos do próprio espaço, mas por *escalares*, que são elementos de um outro conjunto (um corpo).

Definição 1.26 (Espaço Vetorial)**.** Um espaço vetorial sobre um corpo K é um conjunto V com duas operações, *adição de vetores*, denotada por $+$ e *multiplicação por escalar*, denotada por concatenação. A soma opera em pares de vetores e retorna um vetor ($+ : V \times V \to V$), e a multiplicação por escalar opera em pares de escalar e vetor, retornando um vetor ($\cdot : K \times V \to V$). Para que V e K com as duas operações formem um espaço vetorial as operações devem ter as seguintes propriedades:

- As duas operações são associativas:

$$\begin{aligned} c(d\mathbf{v}) &= (cd)\mathbf{v} \\ \mathbf{u} + (\mathbf{v} + \mathbf{w}) &= (\mathbf{u} + \mathbf{v}) + \mathbf{w}. \end{aligned}$$

- A soma de vetores ($+$) é comutativa: $\mathbf{u} + \mathbf{w} = \mathbf{w} + \mathbf{u}$.
- A multiplicação por escalar ($\cdot$) é distributiva, tanto sobre adição de vetores como sobre adição de escalares:

$$\begin{aligned} c(\mathbf{v} + \mathbf{w}) &= c\mathbf{v} + c\mathbf{w} \\ (c + d)\mathbf{v} &= c\mathbf{v} + d\mathbf{v}. \end{aligned}$$

- Existe um vetor $\mathbf{0}$, neutro para adição: $\mathbf{v} + \mathbf{0} = \mathbf{v}$.
- Para todo vetor $\mathbf{v}$ existe um vetor $-\mathbf{v}$, tal que $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$.
- $1\mathbf{v} = \mathbf{v}$ (a multiplicação pela identidade do corpo não modifica um vetor).

Dizemos que K é o *corpo subjacente* ao espaço vetorial V.

O espaço vetorial com um único elemento é chamado de *espaço trivial*. ♦

É de vital importância observar que definimos as operações como $+ : V \times V \to V$ e $\cdot : K \times V \to V$, e que portanto o vetor que resulta da aplicação delas deve *sempre* pertencer ao espaço V onde são definidas.

No espaço trivial, o único elemento deve necessariamente ser o vetor zero, porque a existência do neutro aditivo é requisito.

É interessante observar que não definimos em um espaço vetorial o produto de um vetor por outro, e isto está em consonancia com o nome "álgebra *linear*": em uma forma linear, $ax+b$, multiplica-se a variável x por um escalar a, mas não pelo próprio x ou por outra variável. Por exemplo, a forma $ax^2 + bx + c$ é quadrática, e não linear.

A seguir temos exemplos de diferentes espaços vetoriais. Mostramos que são realmente espaços vetoriaois: para isso mostramos que as operações de soma e multiplicação resultam em um vetor no mesmo espaço, e que as operações tem as propriedades listadas na definição de espaço vetorial.

Exemplo 1.27 (vetores no plano)**.** O conjunto de todos os vetores no plano com as operações de soma de vetores e multiplicação por escalar é um espaço vetorial sobre $\mathbb{R}$, porque:

- Os vetores são pares de números reais, que podemos representar como vetores coluna.
- O corpo é $\mathbb{R}$
- A operação de soma de vetores e a de multiplicação por escalar são associativas.
- A soma de vetores no plano é comutativa ($\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$).
- Vale a distributividade de $\cdot$ sobre $+$. Se representarmos os vetores por $\mathbf{v} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$, etc, temos:

$$c\left[\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} + \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}\right] = c\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} + c\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$
$$(c+d)\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = c\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} + d\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}.$$

- O vetor zero, $\mathbf{0} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, quando somado a qualquer outro vetor $\mathbf{v}$, resulta em $\mathbf{v}$.
- Para todo vetor $\mathbf{v}$ há um outro vetor $\mathbf{u}$, de mesma magnitude e orientação oposta, tal que $\mathbf{v} + \mathbf{u} = \mathbf{0}$.
- A multiplicação de um vetor qualquer por 1 não altera o vetor.

Um vetor no plano é representado por dois números (ordenada e abscissa), e portanto podemos associar cada vetor com o produto cartesiano de $\mathbb{R}$ com $\mathbb{R}$. Por isso o plano é denotado $\mathbb{R}^2$, e o espaço tridimensional é denotado $\mathbb{R}^3$. De amneira geral, denotamos o espaço de n dimensões por $\mathbb{R}^n$ (claro, para $n > 3$ perdemos a possibilidade de visualizar o espaço, mas ainda assim as operações com n coordenadas são análogas àquelas em $\mathbb{R}^2$ e $\mathbb{R}^3$). ◄

Exemplo 1.28. Considere o conjunto de vetores em $\mathbb{R}^2$, com as seguintes operações:

- A operação usual de multiplicação or escalar

- A seguinte operação de soma de vetores:

$$(a, b)^T \boxplus (x, y)^T = \left(\sqrt{ax}, \sqrt{by}\right)^T.$$

Se trocarmos a soma de vetores por esta operação, não teremos um espaço vetorial, porque esta operação não é associativa, como fica claro ao calcularmos (i) $(\mathbf{u} \boxplus \mathbf{v}) \boxplus \mathbf{w}$ (a seguir, à esquerda); e (ii) $\mathbf{u} \boxplus (\mathbf{v} \boxplus \mathbf{w})$ (a seguir, à direita):

(i)

$$\begin{aligned}(\mathbf{u} \boxplus \mathbf{v}) \boxplus \mathbf{w} &= (\sqrt{u_1 v_1}, \sqrt{u_2 v_2})^T \boxplus (w_1, w_2)^T \\ &= \left(\sqrt{w_1 \sqrt{u_1 v_1}}, \sqrt{w_2 \sqrt{u_2 v_2}}\right)^T\end{aligned}$$

(ii)

$$\begin{aligned}\mathbf{u} \boxplus (\mathbf{v} \boxplus \mathbf{w}) &= (u_1, u_2)^T \boxplus (\sqrt{v_1 w_1}, \sqrt{v_2 w_2})^T \\ &= \left(\sqrt{u_1 \sqrt{v_1 w_1}}, \sqrt{u_2 \sqrt{v_2 w_2}}\right)^T\end{aligned}$$

Assim, $(\mathbb{R}^2, \boxplus, \cdot)$ não é espaço vetorial. ◀

Antes dos próximos exemplos, demonstramos alguns fatos básicos a respeito de espaços vetoriais.

Teorema 1.29. *Seja V um espaço vetorial e $\mathbf{u}, \mathbf{v} \in V$. Então*

i) *Se $\mathbf{u} + \mathbf{v} = \mathbf{v}$ então $\mathbf{u} = \mathbf{0}$.*

ii) $0\mathbf{v} = \mathbf{0}$.

iii) *Para todo $\mathbf{v}$, $-\mathbf{v}$ é único, e $-\mathbf{v} = (-1)\mathbf{v}$.*

iv) $c\mathbf{0} = \mathbf{0}$ *para qualquer escalar* c

v) *Existe um único $\mathbf{w} \in V$ tal que $\mathbf{u} + \mathbf{w} = \mathbf{v}$.*

Demonstração. Demonstraremos cada item na ordem em que aparecem no enunciado.
(i)

$$\begin{aligned}\mathbf{u} + \mathbf{v} &= \mathbf{v} \\ \mathbf{u} + \mathbf{v} + (-\mathbf{v}) &= \mathbf{v} + (-\mathbf{v}) \\ \mathbf{u} &= \mathbf{0}\end{aligned}$$

(ii) $0\mathbf{v} = (0 + 0)\mathbf{v} = (0\mathbf{v}) + (0\mathbf{v})$. Pela propriedade anterior – (i) – temos necessariamente $\mathbf{v} = \mathbf{0}$.
(iii) Sejam $-\mathbf{v}$ e $\mathbf{v}'$ dois opostos de $\mathbf{v}$, ou seja,

$$\begin{aligned}-\mathbf{v} + \mathbf{v} &= \mathbf{0} \\ \mathbf{v}' + \mathbf{v} &= \mathbf{0}.\end{aligned}$$

Então $-\mathbf{v}$ e $\mathbf{v}'$ são iguais:

$$\begin{aligned}-\mathbf{v} = -\mathbf{v} + 0 &= -\mathbf{v} + (\mathbf{v} + \mathbf{v}') \\ &= (-\mathbf{v} + \mathbf{v}) + \mathbf{v}' \\ &= \mathbf{0} + \mathbf{v}' \\ &= \mathbf{v}.\end{aligned}$$

Além disso, temos

$$\mathbf{v} + (-1)\mathbf{v} = 1\mathbf{v} + (-1)\mathbf{v} = (1-1)\mathbf{v} = 0\mathbf{v} = \mathbf{0}.$$

e portanto $= \mathbf{v} = (-1)\mathbf{v}$.
(iv) $k\mathbf{0} = k(\mathbf{v} + (-\mathbf{v}))$ para todo $\mathbf{v}$. Usando (iii) que acabamos de provar, temos

$$\begin{aligned} k(\mathbf{v} + (-\mathbf{v})) &= k(\mathbf{v} + (-1)(\mathbf{v})) \\ &= k\mathbf{v} + (-k)(\mathbf{v}) \\ &= (k-k)\mathbf{v} \\ &= 0\mathbf{v}, \end{aligned}$$

que pela propriedade (ii) acima, é igual a $\mathbf{0}$.
(v) Sejam $\mathbf{u}, \mathbf{v}, \mathbf{w}$ tais que $\mathbf{u} + \mathbf{w} = \mathbf{v}$. Então

$$\begin{aligned} \mathbf{u} + \mathbf{w} &= \mathbf{v} \\ \mathbf{u} - \mathbf{u} + \mathbf{w} &= \mathbf{v} - \mathbf{u} \\ \mathbf{w} &= \mathbf{v} - \mathbf{u}. \end{aligned}$$

Como $\mathbf{v} + (-\mathbf{u})$ é definido de forma única porque $-\mathbf{u}$ é único (conforme a propriedade (iii) acima), $\mathbf{w}$ é único. ■

Exemplo 1.30 (polinômios)**.** Denotamos o conjunto de todos os polinômios em x com grau $\leq n$ e coeficientes reais por $\mathbb{R}_n[x]$.

Polinômios podem ser somados e multiplicados por escalares:

- A soma de dois polinômios $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ e $b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$ é

$$(a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_0 + b_0). \tag{1.1}$$

  Por exemplo,

$$\begin{aligned} \Big(3x^3 + 2x^2 - 8\Big) + \Big(-x^3 + x + 1\Big) &= (3-1)x^3 + (2+0)x^2 + (0+1)x + (-8+1) \\ &= 2x^3 + 2x^2 + x - 7. \end{aligned}$$

- A multiplicação de um real k por um polinômio $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ é igual a

$$ka_n x^n + ka_{n-1}x^{n-1} + \cdots + ka_0. \tag{1.2}$$

  Por exemplo,

$$\begin{aligned} 7\Big(3x^3 + 4x^2 - 1\Big) &= 7(3)x^3 + 7(4)x^2 + 7(-1) \\ &= 21x^3 + 28x^2 - 7. \end{aligned}$$

Para qualquer $n \geq 0$, $\mathbb{R}_n[x]$ é um espaço vetorial.

- Como estamos trabalhando com polinômios reais, consideramos que o o corpo subjacente com sendo $\mathbb{R}$.

- A soma de dois polinômios de grau $\leq n$ resulta em outro polinômio de grau $\leq n$, conforme a equação 1.1.
- A multiplicação de um polinômio de grau $\leq n$ por um escalar resulta em outro polinômio de mesmo grau (ou em zero, se o escalar for zero), conforme a equação 1.2.
- A soma de polinômios é associativa: dados tres polinômios $p(x)$, $q(x)$, e $r(x)$, então

$$(p(x) + q(x)) + r(x) = p(x) + (q(x) + r(x)).$$

- A multiplicação de um polinômio por um escalar é associativa: sejam $p(x)$, $q(x)$, e $r(x)$ três polinômios e c, d números reais. Então

$$c\big[dp(x)\big] = (cd)p(x)$$
$$p(x) + \big[q(x) + r(x)\big] = \big[p(x) + q(x)\big] + r(x).$$

- A soma de polinômios é comutativa: $p(x) + q(x) = q(x) + p(x)$.
- Vale a distributividade da multiplicação sobre a soma. Sejam $p(x)$ e $q(x)$ polinômios e c, d números reais. Temos

$$c\big[p(x) + q(x)\big] = cp(x) + cq(x)$$
$$(c + d)p(x) = cp(x) + dp(x)$$

- O número zero é, ele mesmo, um polinômio, e a soma de um polinômio $p(x)$ com zero resulta em $p(x)$. Assim, 0 é elemento neutro para soma.
- para todo polinômio $p(x)$ com grau $\leq n$ há um outro, de mesmo grau ($-p(x)$, o polinômio $p(x)$ multiplicado por -1), tal que $p(x) + (-p(x)) = 0$.
- A multiplicação de um polinômio por 1 não modifica o polinômio. ◀

Exemplo 1.31. Considere o conjunto de pontos definido no plano pela função $y = \frac{x^2}{2}$. Tratamos cada ponto como um vetor, e definimos as duas operações:

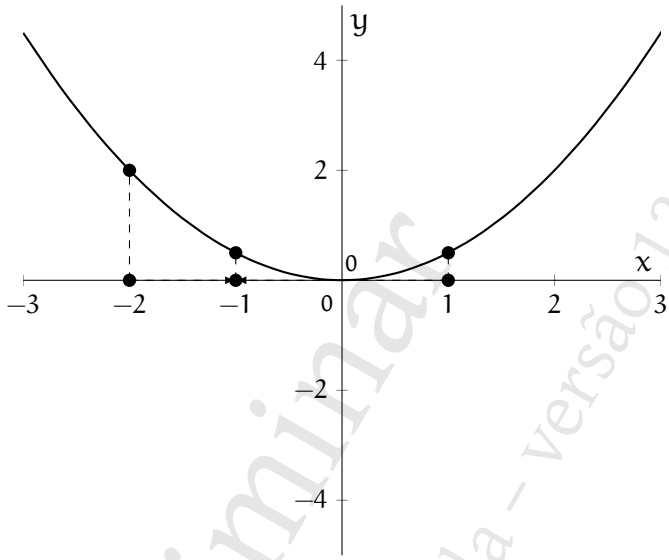
soma de vetores Somamos as primeiras coordenadas dos pontos, e calculamos a segunda.

$$(x, 2x^2) + (a, 2x^2) = (x + a, 2(x + a)^2).$$

multiplicação por escalar multiplicamos a primeira coordenada do ponto pelo escalar, e calculamos a segunda.

$$k(x, 2x^2) = (kx, 2[kx]^2)$$

A próxima figura ilustra geometricamente a operação de soma de vetores; a de multiplicação é análoga.



- As operações são associativas;
- A soma é comutativa;
- A multiplicação por escalar é distributiva.
- O vetor $(0,0)$ pertence ao nosso espaço, e é neutro para adição.
- Todo vetor tem um inverso aditivo: se $\mathbf{v} = (x, \frac{x^2}{2})$, então $-\mathbf{v} = (-x, \frac{x^2}{2})$. Temos $\mathbf{v} + (-\mathbf{v}) = (0,0)$.
- A multiplicação de um vetor por um não o modifica: $1(x, \frac{x^2}{2}) = (x, \frac{x^2}{2}$.

◀

Exemplo 1.32 (funções)**.** Seja $\mathcal{F}(\mathbb{R})$ o conjunto de todas as funções de $\mathbb{R}$ em $\mathbb{R}$. Por exemplo, $f(x) = 2x$, $g(x) = \tan(x)$ são elementos de $\mathcal{F}(\mathbb{R})$. Podemos somar duas funções e multiplicar uma função por um escalar: sejam $f, g \in \mathcal{F}$. Então,

- A soma de f com g é $f + g$, tal que $(f + g)(x) = f(x) + g(x)$.
- A multiplicação de f por um número real k é kf, tal que $(kf)(x) = k(f(x))$.

O conjunto $\mathcal{F}$, com as operações de soma de funções e multiplicação por escalar, é um espaço vetorial:

- A soma de funções é comutativa:

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x).$$

- A multiplicação de função por escalar é associativa:

$$c(d(f(x)) = (cd)f(x)$$

- A soma de funções é associativa:

$$\begin{aligned}\big[(f+g)+h\big](x) &= \big[f(x)+g(x)\big]+h(x)\\ &= f(x)+g(x)+h(x)\\ &= f(x)+\big[g(x)+h(x)\big]\\ &= \big[f+(g+h)\big](x).\end{aligned}$$

- Vale a distributividade da multiplicação sobre a soma:

$$k(f+g)(x) = k\big(f(x)+g(x)\big) = kf(x)+kg(x).$$

- A função constante $f(x) = 0$ é o neutro aditivo: para toda função g,

$$(f+g)(x) = f(x)+g(x) = 0+g(x) = g(x).$$

- Toda função f tem um inverso aditivo, que é $(-1)f$.

$$\big[f+(-1)f\big](x) = f(x)+(-1)f(x) = f(x)-f(x) = 0 = z(x),$$

  onde $z(x)$ é a função constante zero.

- A multiplicação de uma função por 1 não a modifica. ◀

Exemplo 1.33 (números reais, operações trocadas)**.** As operações usadas em espaços vetoriais não precisam ser a soma e multiplicação usuais. Elas precisam apenas ter as propriedades listadas na definição de espaço vetorial. Por exemplo, podemos definir o seguinte espaço vetorial:

- O conjunto de vetores é $\mathbb{R}^*$ (os números reais exceto o zero);
- O corpo usado é $\mathbb{R}$;
- A operação de soma de vetores é a multiplicação de reais: $u \oplus v = uv$
- A operação de multiplicação por escalar é a exponenciação: $c \odot v = v^c$

Neste espaço, o elemento identidade para soma deve ser necessariamente 1: $x \cdot 1 = x$. O inverso aditivo de cada elemento x é x^{-1}. ◀

Exemplo 1.34 (matrizes)**.** O conjunto de todas as matrizes reais $m \times n$, que denotamos $\mathcal{M}_{m\times n}$, é um espaço vetorial: podemos somar matrizes e multiplicá-las por escalares reais, e as propriedades necessárias são mantidas. Este é um espaço vetorial sobre $\mathbb{R}$, já que os escalares que multiplicamos pelas matrizes são reais. ◀

★ **Exemplo 1.35.** Este exemplo aborda a relação entre os vetores de um espaço e o corpo subjacente, e ilustra um fato muito importante. Tentaremos construir um espaço vetorial de duas maneiras parecidas. Uma delas funcionará e a outra não.

Se tomarmos todas as matrizes 2×2 com coeficientes *reais*, mas usarmos o corpo $\mathbb{Q}$ para os escalares, não teremos problemas. Ao multiplicarmos um escalar racional pela matriz real, obtemos outra matriz real. Por exemplo,

$$\frac{m}{n}\begin{pmatrix}\pi & 0\\ e & \sqrt{2}\end{pmatrix} = \begin{pmatrix}\frac{\pi m}{n} & 0\\ \frac{em}{n} & \frac{m\sqrt{2}}{n}\end{pmatrix}.$$

Assim, podemos ter o corpo subjacente igual a $\mathbb{Q}$, mas com matrizes reais como vetores. Temos um espaço vetorial sobre $\mathbb{Q}$.

Já o contrário não é possível: suponha que queiramos usar apenas matrizes 2×2 racionais e escalares reais, portanto V é o conjunto destas matrizes – e excluímos assim todas as matrizes que tem elementos irracionais. As operações poderão resultar em matrizes reais:

$$\sqrt{3}\begin{pmatrix} 1 & 0 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} \sqrt{3} & 0 \\ 3\sqrt{3} & -2\sqrt{3} \end{pmatrix}.$$

Esta última matriz tem elementos irracionais, e não pertence a V, portanto não temos um espaço vetorial. ◀

Exemplo 1.36 (sequências)**.** Começamos este exemplo com a definição de *sequências*.

Definição 1.37 (sequência)**.** Uma *sequência* é uma função de $\mathbb{N}^*$ em $\mathbb{R}$. Sequencias normalmente são denotadas por (a_n), (b_n). O n-ésimo termo da sequência (ou seja, a valor função para o argumento igual a n) é usualmente denotado por a_n, b_n, etc, sem os parênteses, ao invés da notação tradicional para funções $a(n)$, $b(n)$, etc. ♦

Por exemplo, podemos definir uma sequência (a_n):

$$\begin{aligned} a_1 &= 2 \\ a_n &= 2a_{n-1} + 1 \end{aligned}$$

Temos então $a_1 = 5$, $a_2 = 11$, $a_3 = 23$, ...

Um exemplo bastante conhecido é a *sequência de Fibonacci*, dada por

$$\begin{aligned} F_1 &= 1 \\ F_2 &= 1 \\ F_n &= F_{n-1} + F_{n-2}. \end{aligned}$$

A seguir mostramos os primeiros números da sequência de Fibonacci.

$$\begin{aligned} F_1 &= 1 \quad F_5 = 5 \\ F_2 &= 1 \quad F_6 = 8 \\ F_3 &= 2 \quad F_7 = 13 \\ F_4 &= 3 \quad F_8 = 21 \end{aligned}$$

Sejam (a_n), (b_n), ... sequências. Definimos as operações de soma de sequências e multiplicação de sequência por escalar da maneira natural:

- A soma de duas sequências $(c_n) = (a_n) + (b_n)$ é sequencia onde cada termo c_i é a soma de termos $a + i + b_i$.
- A multiplicação de uma sequência (a_n) por um númeor real k é a sequência $(c_n) = k(a_n)$, cujos termos são $c_i = kc_i$.

Por exemplo, se $(a_n) = (2, 4, 6, 8, \ldots)$ é a sequencia dos pares começando com dois, e $(b_n) = (10, 20, 30, 40, \ldots)$ é a sequência dos múltiplis de dez, começando com dez, então

$$\begin{aligned} (a_n) + (b_n) &= (12, 24, 36, 48, \ldots) \\ 3(a_n) &= (6, 12, 18, 24, \ldots) \end{aligned}$$

Então o conjunto de todas as sequencias é um espaço vetorial:

i) a soma de sequências é associativa e comutativa;

ii) a multiplicação de sequência por escalar é associativa;

iii) a sequência $z_n = 0$ é neutra para soma de sequências;

iv) para toda sequência (a_n), existe uma sequencia $(-a_n)$ tal que $(a_n) + (-a_n) = (z_n)$. ◀

★ **Exemplo 1.38** (soluções de equação diferencial)**.** Uma *equação diferencial ordinária* é uma equação envolvendo uma função e uma ou mais de suas derivadas. Uma resumida introdução às Equações Diferenciais é dada no Apêndice δ.

Considere a equação diferencial

$$y'' - y = 0. \tag{1.3}$$

- A equação é *linear*, porque é da forma $a_n y^{(n)} + a_{n-1} y^{(n-1)} + \cdots + a_1 y + a_0 = f(x)$.
- A equação é *homogênea*, porque apenas a variável dependente aparece na equação – não vemos a variável independente nem constantes ($a_0 = 0, f(x) = 0$).

As soluções da equação 1.3 são da forma

$$y = ae^x - be^{-x},$$

porque para todo $x \in \mathbb{R}$,

$$\frac{d^2}{dx^2} ae^n - be^y - \frac{d}{dx} ae^n - be^y = 0.$$

onde a e b são constantes arbitrárias. As soluções formam um espaço vetorial: a soma de duas soluções resulta em outra solução – sejam (a,b) e (α, β) as constantes que determinam duas soluções diferentes para a EDO. Então

$$ae^x - be^{-x} + \alpha e^x - \beta e^x = (a + \alpha)e^x - (b + \beta)e^{-x}$$

A multiplicação por escalar também resulta em outra solução:

$$c(ae^x + be^{-x}) = (ca)e^x + (cb)e^{-x}.$$

Finalmente, as propriedades de espaço vetorial valem: (i) a soma de soluções é associativa e comutativa; (ii) a multiplicação por escalar é associativa; (iii) $y = 0$ é solução (com $a = b = 0$), e funciona como neutro aditivo; (iv) toda solução tem oposto – basta multiplicá-la por -1; (v) multiplicar 1 por uma solução não a modifica.

O conjunto de soluções para *qualquer* EDO linear homogênea é sempre um espaço vetorial.

Uma excelente introdução às Equações Diferenciais é o livro de Tenenbaum em Pollard [TP63]. Mais resumidos, os livros de Coddington [Cod61] e Bear [Bea62] são também ótimos textos sobre o assunto. ◀

Exemplo 1.39 (variáveis aleatórias)**.** Seja Ω o espaço amostral de um experimento aleatório. Uma *variável aleatória real* é uma função $X : \Omega \to \mathbb{R}$.

Por exemplo, se o espaço amostral é o conjunto de pessoas em um prédio, a função que mapeia cada pessoa em sua massa corporal é uma variável aleatória.

O conjunto de todas as variáveis aleatórias em Ω é um espaço vetorial quando usamos a operação usual de soma de variáveis aleatórias, e a multiplicação de uma variável aleatória por escalar real.

Sejam A e B duas variáveis aleatórias definidas no mesmo espaço amostral Ω, e seja $C = A + B$. Para todo evento simples $\omega \in \Omega$, $C(\omega) = A(\omega) + B(\omega)$. Fica portanto claro que:

- A soma de variáveis aleatórias é associativa e comutativa.
- A multiplicação de variável aleatória por escalar é distributiva sobre a soma.
- A variável aleatória Z, que leva todo elemento de Ω em 0, é o elemento neutro para adição.
- Se A é variável aleatória, então a variável aleatória $-A$, que leva os elementos do espaço amostral aos valores opostos aos que A leva, também é.
- Multiplicar uma variável aleatória por 1 não a modifica.

Mostramos então que o conjunto das variáveis aleatórias reais em um mesmo espaço amostral é um espaço vetorial sobre $\mathbb{R}$. ◀

★ **Exemplo 1.40** (sequências de bits)**.** Mencionamos no exemplo 1.22 o corpo $\mathbb{Z}_2$, onde as operações são o "e" ($\wedge$) e o "ou-exclusivo" ($\oplus$). Definimos agora um espaço vetorial sobre este corpo, de maneira análoga a $\mathbb{R}^n$ sobre os reais. Cada vetor é uma sequência de n bits, e as operações são:

- *Soma:* é feita elemento a elemento – somar o vetor $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ com o vetor $\mathbf{b}' = (b'_1, b'_2, \ldots, b'_n)$ resulta em $(b_1 \oplus b'_1, b_2 \oplus b'_2, \ldots, b_n \oplus b'_n)$. Por exemplo,

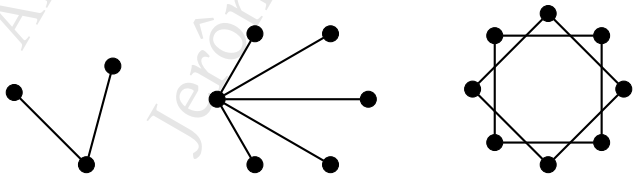
$$\begin{array}{r} (0,1,0,1,1) \\ \oplus\ (0,0,1,1,0) \\ \hline = (0,1,1,0,1) \end{array}$$

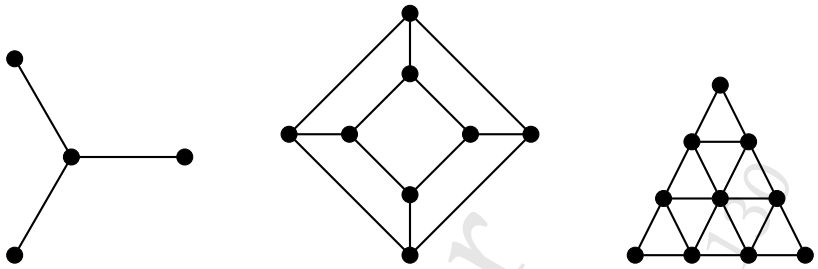
- *Multiplicação por escalar:* é feita elemento a elemento – multiplicar c pelo vetor $(b_1, b_2, \ldots, b_n)$ resulta em $(cb_1, cb_2, \ldots, cb_n)$. Como há somente dois escalares no corpo (0 e 1), listamos aqui o efeito da multiplicação de vetores por eles.

$$1 \wedge (b_1, b_2, \ldots, b_n) = (b_1, b_2, \ldots, b_n)$$
$$0 \wedge (b_1, b_2, \ldots, b_n) = (0, 0, \ldots, 0).$$

Este espaço é chamado de $\mathbb{Z}_2^n$. ◀

★ **Exemplo 1.41** (ciclos em grafo)**.** Um *grafo* é uma representação gráfica de uma relação em um conjunto. Grafos tem aplicação em uma enorme quantidade de áreas das Engenharias, da Computação e da Matemática. A figura a seguir mostra exemplos de grafos.

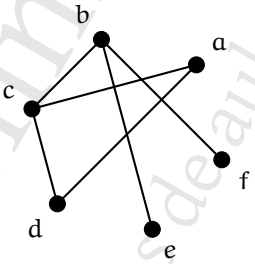




É usual dar nomes aos nós, e desenhar o grafo com os nomes de cada nó seu lado.

Para poder trabalhar com grafos como objetos matemáticos, precisamos dar a eles uma definição formal. Definimos um grafo como um par (V, E), onde V é um conjunto de *vértices* (representados graficamente como "pontos") e E um conjunto de *arestas* (graficamente são os "traços" que unem vértices), de forma que cada aresta em E seja um conjunto de dois dos vértices em V.

Damos um exemplo de grafo na próxima figura.



O conjunto de vértices do grafo é

$$V = \{a, b, c, d, e, f\}.$$

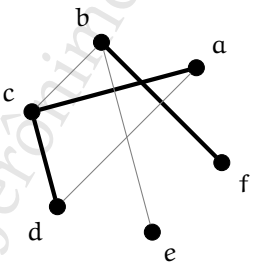
As arestas são

$$E = \begin{Bmatrix} \{a, c\}, & \{a, d\}, & \{b, c\}, \\ \{b, e\}, & \{b, f\}, & \{c, d\} \end{Bmatrix}.$$

Um *subgrafo* é uma "parte" de um grafo.

Definição 1.42 (subgrafo)**.** Seja $G = (V, E)$ um grafo. Um *subgrafo* de G é um grafo $G' = (V', E')$ tal que $V' \subseteq V$ e $E' \subseteq E$. ♦

O grafo em negrito na figura a seguir é um subgrafo do grafo anterior. Neste texto, quando quisermos mostrar um subgrafo, ele será desenhado em negrito sobre o grafo original, que será desenhado em tom de cinza claro.



O *vetor característico* de um conjunto de arestas é um vetor com E posições. A posição i do vetor é um se e_i está no subgrafo, e zero se não está. Por exemplo, o vetor característico do subgrafo que mostramos é

$$\begin{matrix}\{a,b\}\to\\ \{a,c\}\to\\ \{a,d\}\to\\ \{a,e\}\to\\ \{a,f\}\to\\ \{b,c\}\to\\ \{b,d\}\to\\ \{b,e\}\to\\ \{b,f\}\to\\ \{c,d\}\to\\ \{c,e\}\to\\ \{c,f\}\to\\ \{d,e\}\to\\ \{d,f\}\to\end{matrix}\begin{pmatrix}0\\1\\0\\0\\0\\0\\0\\0\\1\\1\\0\\0\\0\\0\end{pmatrix}$$

Os elementos do vetor característico são 0 e 1. Será conveniente usarmos as operações de $\mathbb{Z}_2$ nestes vetores. Multiplicar um vetor por 1 é o mesmo que realizar a operação de "e", e portanto resulta no mesmo vetor (não modifica o subgrafo):

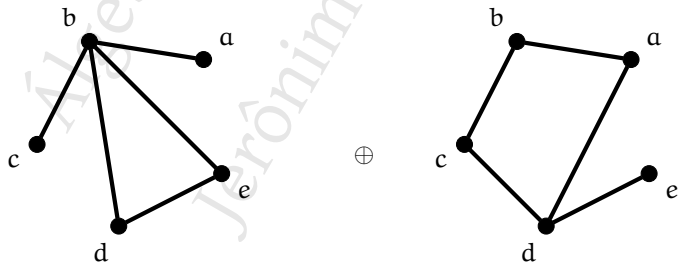
$$1\cdot(0,1,1,0,0,1)^T=(0,1,1,0,0,1)^T.$$

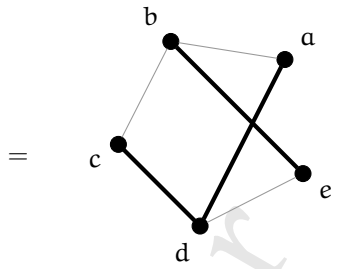
A multiplicação por zero resulta no vetor zero (e portanto no grafo sem arestas, contendo somente os vértices), ou seja, multiplicar um subgrafo por zero o faz "desaparecer".

A soma de dois vetores é feita elemento-a-elemento, com a operação de soma em $\mathbb{Z}_2$ (ou seja, usando ou-exclusivo):

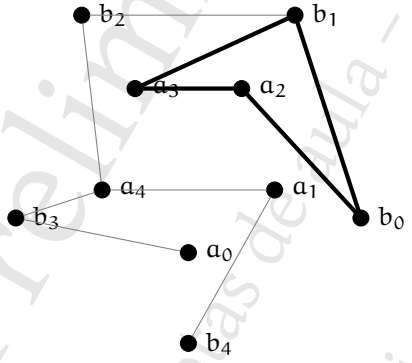
$$(0,1,1,0,0,1)^T\oplus(1,1,0,1,0,1)^T=(1,0,1,1,0,0)^T.$$

Em um grafo, esta operação representa a soma de dois subrafos: se uma aresta existe somente em um dos subgrafos, ela passa a existir na soma. Se uma aresta existe *nos dois* subgrafos, ela deixa de existir na soma. A figura a seguir ilustra a soma de dois subgrafos. Observe que as arestas (a,b), (b,c) e (d,e) existiam em ambos os grafos, e não existem na soma (elas aparecem em cinza claro na ilustração, apenas para facilitar sua identificação).

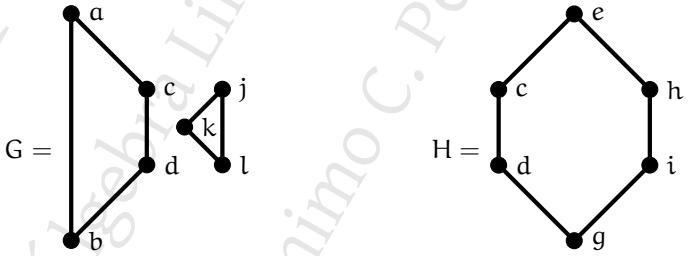




Um *ciclo* em um grafo é uma sequência de arestas $(e_1, e_2, \ldots, e_k)$ formam um caminho, iniciando com um vértice e terminando nele mesmo[6]. A figura a seguir ilustra um ciclo em um grafo; o ciclo é formado pelos vértices (a_2, a_3, b_1, b_0).

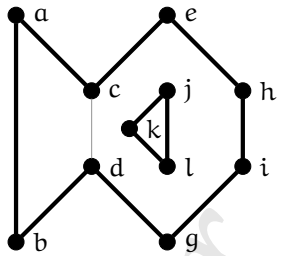


Quando somamos dois grafos, cada um composto por *ciclos disjuntos* (isto é, ciclos que não compartilham arestas), o resultado também é um grafo composto por ciclos disjuntos. Não demonstraremos este fato, mas ilustramos com um exemplo. A figura a seguir mostra dois grafos, G e H. Estes grafos tem dois vértices (c e d) e uma aresta (c——d) em comum.



O resultado da soma dos dois grafos, G ⊕ H, é mostrado a seguir.

[6]Esta definição está simplificada. Para mais detalhes, o leitor poderá consultar a literatura de Teoria dos Grafos – por exemplo, o livro de Bondy e Murty [BM08]



Seja C a união dos subgrafos sem arestas com o conjunto dos subgrafos de G que consistem de uniões de ciclos. C com as operações que definimos é um espaço vetorial sobre $\mathbb{Z}_2$:

- Grafos sem arestas são o elemento neutro (zero), e sua soma com qualquer outro grafo de ciclos resulta no próprio grafo de ciclos;
- A soma de dois ciclos resulta em um ciclo;
- A multiplicação de um elemento por 1 resulta no próprio elemento; por 0 resulta no grafo sem arestas. ◀

1.5 Subespaços

Definição 1.43 (Subespaço)**.** Seja V um espaço vetorial, e seja também $U \subseteq V$. Se as mesmas operações que tornam V um espaço vetorial[7] também tornam U um espaço vetorial, então U é um *subespaço* de V. ♦

Teorema 1.44. *Todo espaço vetorial V não trivial tem pelo menos dois subespaços: o próprio V e o espaço trivial.*

Demonstração. O espaço trivial é subespaço de qualquer espaço V porque

- $\{\,\mathbf{0}\,\} \subseteq V$.
- Como só há um elemento no espaço trivial, não há vetores a somar.
- A multiplicação de qualquer escalar por $\mathbf{0}$ é associativa: $(cd)\mathbf{0} = c(d\mathbf{0}) = \mathbf{0}$.
- O zero é neutro para adição ($\mathbf{0} + \mathbf{0} = \mathbf{0}$).
- Para todo vetor no espaço trivial (ou seja, somente para o zero), $\mathbf{0} + -\mathbf{0} = \mathbf{0}$.
- A multiplicação de 1 por $\mathbf{0}$ é igual a $\mathbf{0}$ (ou seja, não modifica o vetor zero).

Claramente V também é subespaço de V, porque $V \subseteq V$. ■

Exemplo 1.45. Considere o espaço $\mathbb{R}^3$. O conjunto de pontos da forma $(v_1, v_2, 0)$ é um subespaço, porque: (i) a soma de dois pontos desta forma resulta em outro também da mesma forma: $(u_1, u_2, 0) + (v_1, v_2, 0) = (u_1 + v_1, u_2 + v_2, 0)$, e (ii) a multiplicação por escalar também resulta em outro ponto da mesma forma:

[7] Alguns autores dizem que U é "munido" das mesmas operações de V.

$c(v_1, v_2, 0) = (cv_1, cv_2, 0)$. Além disso, (i) a soma de vetores (os pontos) é associativa e comutativa; (ii) a multiplicação de vetores por escalar é associativa:

$$\begin{aligned} c(d\mathbf{u}) &= c(d(u_1, u_2, 0)) \\ &= c(du_1, du_2, 0) \\ &= (cdu_1, cdu_2, 0) \\ &= (cd)(u_1, u_2, 0) \\ &= (cd)\mathbf{u}, \end{aligned}$$

e

$$\begin{aligned} \mathbf{u} + (\mathbf{v} + \mathbf{w}) &= (u_1, u_2, 0) + [(v_1, v_2, 0) + (w_1, w_2, 0)] \\ &= (u_1, u_2, 0) + (v_1 + w_1, v_2 + w_2, 0) \\ &= (u_1 + v_1 + w_1, u_2 + v_2 + w_2, 0) \\ &= [(u_1 + v_1, u_2 + v_2, 0)] + (w_1, w_2, 0) \\ &= [(u_1, u_2, 0) + (v_1, v_2, 0)] + (w_1, w_2, 0) \\ &= (\mathbf{u} + \mathbf{v}) + \mathbf{w}; \end{aligned}$$

(iii) a multiplicação por escalar é distributiva:

$$\begin{aligned} c(\mathbf{u} + \mathbf{v}) &= c\,[(u_1, u_2, 0) + (v_1, v_2, 0)] \\ &= c(u_1, u_2, 0) + c(v_1, v_2, 0) \\ &= c\mathbf{u} + c\mathbf{v}, \end{aligned}$$

e

$$\begin{aligned} (c + d)\mathbf{v} &= (c + d)(v_1, v_2, 0) \\ &= c(v_1, v_2, 0) + d(v_1, v_2, 0) \\ &= c\mathbf{v} + d\mathbf{v}; \end{aligned}$$

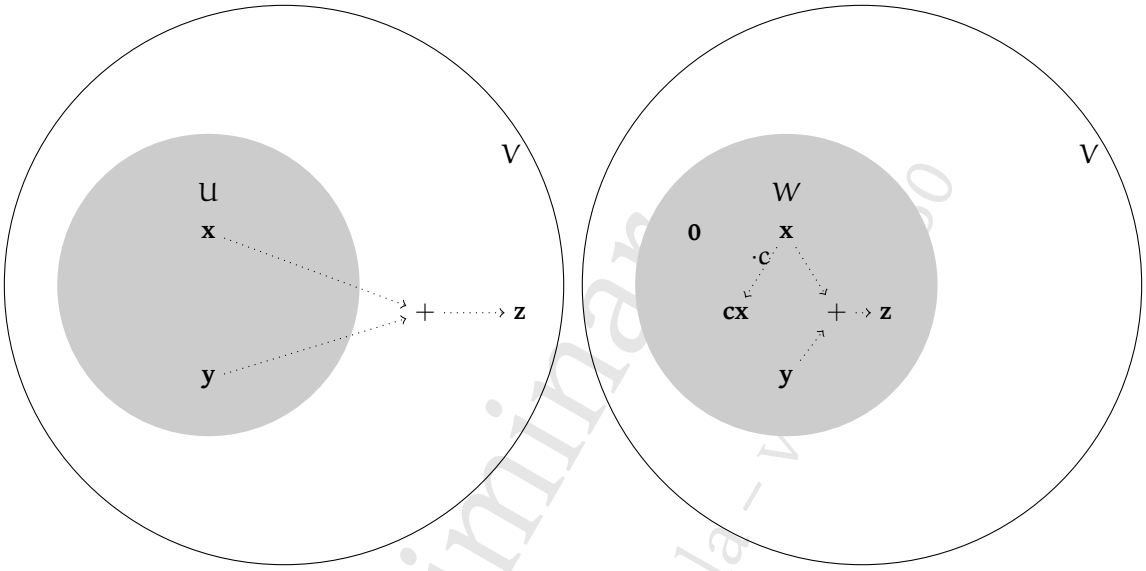
(iv) o vetor $\mathbf{0} = (0, 0, 0)$ é neutro para soma; (v) para todo vetor $(u_1, u_2, 0)$ existe um vetor $(-u_1, -u_2, 0)$ tal que $(u_1, u_2, 0) + (-u_1, -u_2, 0) = \mathbf{0}$; (vi) multiplicar 1 por um vetor $\mathbf{v}$ não modifica o vetor.

Este exemplo mostra também que podemos visualizar $\mathbb{R}^2$ como subespaço de $\mathbb{R}^3$ uma vez que ignorando a terceira coordenada (que é igual a zero), temos um plano. ◀

Exemplo 1.46. Sabemos que os reais são um espaço vetorial (os vetores são números reais, e o corpo subjacente é o próprio $\mathbb{R}$). Os racionais *não* são subespaço dos reais, porque a multiplicação de $x \in \mathbb{Q}$ por escalar real não necessariamente é racional: $\pi \cdot (2/3) = 2\pi/3$. ◀

Se sabemos que V é um espaço vetorial e $U \subseteq V$, já sabemos também que todas as propriedades das operações em V também valem em U (porque as operações são as mesmas). Resta apenas determinar se este subconjunto é fechado para as operações de soma de vetores e multiplicação por escalar. Para isso, verificamos que: (i) o vetor zero pertence a U; (ii) as operações de soma e multiplicação por escalar de elementos de U resultam em elementos também de U.

A figura a seguir mostra, por exemplo, dois subconjuntos de um espaço vetorial V. No primeiro caso, U é subconjunto, mas há vetores $\mathbf{x}$ e $\mathbf{y}$ tais que $\mathbf{x} + \mathbf{y} = \mathbf{z} \notin U$. Como esta condição já não é satisfeita, podemos dizer que U não é subespaço de V. No segundo caso, a soma de quaiquer $\mathbf{x}$ e $\mathbf{y}$ está em W, o zero está em W, e para todo $\mathbf{x}$ e todo c, $c\mathbf{x}$ está em W, portanto W é subespaço de V.



Teorema 1.47. *Se V é um espaço vetorial e $U \subseteq V$, de forma que $\mathbf{0} \in U$ e U é fechado para as operações de multiplicação por escalar e soma de vetores, então U é subespaço de V.*

Exemplo 1.48. Considere o subconjunto de $\mathbb{R}^2$, $X = \{(x, y) : \ x + y = 0\}$. X é subespaço de $\mathbb{R}^2$, porque $(0, 0) \in X$; a soma de dois vetores de X resulta em outro vetor de X. Sejam (a, b) e (x, y) pontos de X.

$$(a, b) + (x, y) = (a + x, b + y)$$

Somando as coordenadas do novo vetor, temos

$$(a + x) + (b + y) = (a + b) + (x + y) = 0 + 0 = 0.$$

a multiplicação de vetores de X por escalar resulta em outro vetor de X. Seja (x, y) vetor em X e c um escalar.

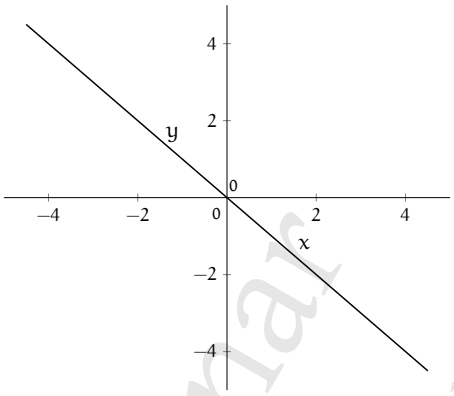
$$c(x, y) = (cx, cy)$$

Então

$$cx + cy = c(x + y) = 0c = 0.$$

O conjunto X definido acima é a reta $y = -x$. Há outras retas que são subespaços de $\mathbb{R}^2$: basta que passem pela origem (porque precisamos do vetor **0**).

Geometricamente, podemos verificar que a adição de vetores nesta reta resulta sempre em outro vetor também sobre a mesma reta – e que a multiplicação por escalar também mantémos vetores na reta. Como além disso a reta pasa pela origem, o vetor zero está também na reta, e portanto, como soma e multiplicação por escalar resultam em vetores na reta, e ela contém o zero, trata-se de um subespaço de $\mathbb{R}^2$.



O raciocínio geométrico que fizemos obviamente vale para qualquer reta passando pela origem (e realmente, são todas subespaços de $\mathbb{R}^2$).

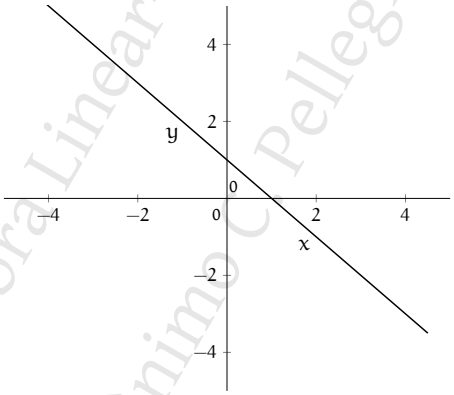
De maneira geral, o conjunto $\{(x_1, x_2, \ldots, x_n) : \sum x_i = 0\}$ é subespaço de $\mathbb{R}^n$. ◀

Exemplo 1.49. Considere o conjunto de pontos $X = \{(x, y) : x + y = 1\}$. X é sub*conjunto* de $\mathbb{R}^2$, mas *não* é um sub*espaço* de $\mathbb{R}^2$, porque

i) $(0, 0) \notin X$.

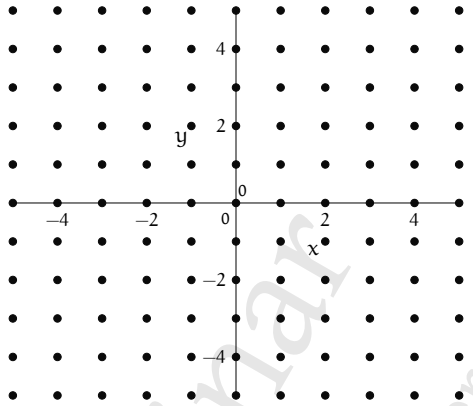
ii) A soma de dois vetores de X não resulta em outro vetor de X.

iii) A multiplicação de um vetor de X por escalar não resulta em outro vetor de X.



◀

Exemplo 1.50. Considere o conjunto de pontos $X = \{(x, y) : x, y \in \mathbb{Z}\}$, ilustrado na figura a seguir.



X é sub*conjunto* de $\mathbb{R}^2$, mas *não* é um sub*espaço* de $\mathbb{R}^2$, porque a multiplicação de um vetor de X por escalar *real* não resulta em outro vetor de X. Os escalares em um espaço vetorial não podem ser inteiros, porque isto seria o mesmo que definir o espaço vetorial sobre $\mathbb{Z}$, que não formam um corpo. ◀

Exemplo 1.51. Considere o subconjunto de $\mathbb{R}^3$, $X = (x, 2x, x^2)^T$, ou seja, vetores onde a segunda coordenada é o dobro da primeira e a terceira é o quadrado da primeira. X *não* é um subespaço vetorial de $\mathbb{R}^3$, porque $(1, 2, 1)^T$ e $(2, 4, 4)^T$ pertencem a X, mas sua soma, $(3, 6, 5)^T$ não pertence a X (porque $3^2 \neq 5$). ◀

Exemplo 1.52. Para $r \in \mathbb{R}$, o conjunto de pontos em uma circunferência, $C = \{ x^2 + y^2 \leq r^2 \}$ não é subespaço de $\mathbb{R}^2$: a multiplicação por escalar leva pontos de C a pontos fora de C: para todo r podemos encontrar um c tal que $cx^2 + cy^2 > r$. Geometricamente, o conjunto C define os vetores dentro de uma circunferência com raio r – e qualquer vetor em C diferente de zero pode ser multiplicado por algum escalar grande o suficiente para passar a ter magnitude maior que o raio. ◀

Exemplo 1.53. Podemos também voltar a atenção para o conjunto das funções contínuas cujo domínio é $\mathbb{R}$, que é denotado C^0.

Para verificar que C^0 é um espaço vetorial, verificamos que é um conjunto de funções de $\mathbb{R}$ em $\mathbb{R}$, e portanto valem os argumentos postos nos itens do exemplo 1.32 – e de fato, este conjunto é subconjunto de $\mathcal{F}(\mathbb{R})$. No entanto, como o conjunto é diferente, precisamos garantir a presença do vetor (função) zero e o fechamento das operações:

- A função constante zero, $z(x) = 0$, é contínua e está definida em $\mathbb{R}$.
- A soma de duas funções contínuas definidas em $\mathbb{R}$ também é contínua em $\mathbb{R}$.
- A multiplicação de uma função contínua por um escalar resulta em outra função, também contínua.

◀

Exemplo 1.54. Uma função contínua pode não ser diferenciável (como $|x|$, por exemplo) ou pode ser derivável k vezes (onde k pode ser infinito). O conjunto de funções k vezes diferenciáveis (ou seja, para as quais a k-ésima derivada é definida) é denotado por C^k.

Verificamos que C^k é um espaço vetorial:

- A função constante zero, $z(x) = 0$, é derivável infinitas vezes.
- A soma de duas funções com a k-ésima derivada definida será uma função também k vezes derivável.

- A multiplicação de uma função com a k-ésima derivada definida por um escalar resulta em outra função, também k vezes derivável. ◀

Exemplo 1.55. O conjunto das funções $f : \mathbb{R} \to \mathbb{R}$ contínuas em um dado intervalo $[a, b]$ é denotado por $C[a, b]$. Para qualquer intervalo $[a, b]$ não-vazio de $\mathbb{R}$, $C[a, b]$ é um espaço vetorial.

Para verificar que este é um espaço vetorial, observamos inicialmente que este *não* é um subconjunto de $\mathcal{F}(\mathbb{R})$, porque os domínios das funções são diferentes: $f : \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2$ é diferente de $g : [a, b] \to \mathbb{R}, \quad g(x) = x^2$. No entanto, podemos argumentar que o conjunto formado pelas funções em $\mathcal{F}(\mathbb{R})$, restritas ao intervalo $[a, b]$ é um espaço vetorial, e que $C[a, b]$ é subespaço desse conjunto, pelos mesmos argumentos que apresentamos para mostrar que C^0 é subespaço de $\mathcal{F}(\mathbb{R})$. ◀

★ **Exemplo 1.56.** Vimos no exemplo 1.38 que o conjunto de soluções de uma EDO linear homogênea é um espaço vetorial. Mencionamos ali também que as soluções de

$$y'' - y = 0$$

são as funções da forma

$$y(x) = ae^x - be^{-x} = 0.$$

O conjunto de funções

$$g(x) = ae^x$$

é subespaço das soluções para esta EDO:

- A função zero é da forma ae^x, com $a = 0$;
- A soma é fechada: $ae^x + \alpha e^x = (a + \alpha)e^x$;
- A multiplicação por escalar é fechada: $k(ae^x) = (ka)e^x$.

A solução geral especifica duas constantes arbitrárias, a e b. Fixando qualquer uma delas em zero, temos um subespaço. ◀

Exemplo 1.57. As funções pares, ímpares, racionais e as funções definidas por polinômios são também subespaços de $\mathcal{F}(\mathbb{R})$. ◀

Exemplo 1.58. Considere o sistema homogêneo de equações lineares, com n variáveis e m equações.

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= 0 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= 0 \end{aligned}.$$

O mesmo sistema pode ser escrito da forma $A\mathbf{x} = \mathbf{0}$, onde A é uma matriz $m \times n$, com o coeficiente a_{ij} na linha i e coluna j, $\mathbf{x}$ é o vetor coluna $(x_1, \ldots, x_n)^T$ e $\mathbf{0}$ é o vetor coluna zero. Assim, podemos dizer que as soluções para $A\mathbf{x} = \mathbf{0}$ são todos os vetores coluna $\mathbf{x} \in \mathbb{R}^n$ que satisfazem o sistema homogêneo de equações definido por A. Este conjunto de vetores é subespaço de $\mathbb{R}^n$, como verificamos a seguir.

Faremos a demonstração de duas maneiras: primeiro, com o sistema na forma de equações, e depois usando a forma matricial.

i) A solução com $x_1 = x_2 = \cdots = x_n = 0$ sempre é válida para sistemas homogêneos (ou seja, o vetor $\mathbf{0}$ sempre é solução). Para cada linha i, temos

$$\begin{aligned} & a_{i1}x_1 + a_{i2}x_1 + \cdots + a_{in}x_n \\ &= a_{i1}(0) + a_{i2}(0) + \cdots + a_{in}(0) \\ &= 0. \end{aligned}$$

ii) A soma de duas soluções é uma solução: Sejam $(x_1, x_2, \ldots, x_n)$ e $(y_1, y_2, \ldots, y_n)$ duas soluções para o sistema. Então $(x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$ também é solução: para cada linha i, verificamos que

$$\begin{aligned} & a_{i1}(x_1 + y_1) + a_{i2}(x_2 + y_2) + \cdots + a_{in}(x_n + y_n) \\ &= a_{i1}x_1 + a_{i1}y_1 + a_{i2}x_2 + a_{i2}y_2 + \cdots + a_{in}x_n + a_{in}y_n \\ &= \Big(a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n + a_{in}x_n\Big) + \Big(a_{i1}y_1 + a_{i2}y_2 + \cdots + a_{in}y_n + a_{in}y_n\Big) \\ &= 0. \end{aligned}$$

iii) A multiplicação de uma solução por escalar resulta em outra solução. O exercício 25 pede a demonstração deste item.

i) A solução com $\mathbf{x} = \mathbf{0}$ sempre é válida para $A\mathbf{x} = \mathbf{0}$, porque $A\mathbf{0} = \mathbf{0}$.

ii) A soma de duas soluções é uma solução: Se $A\mathbf{x} = \mathbf{0}$ e $A\mathbf{y} = \mathbf{0}$, então

$$\begin{aligned} A(\mathbf{x} + \mathbf{y}) &= A\mathbf{x} + A\mathbf{y} && \text{(multiplicação é distributiva para matrizes)} \\ &= \mathbf{0} + \mathbf{0} \\ &= \mathbf{0}. \end{aligned}$$

iii) A multiplicação de uma solução por escalar resulta em outra solução. Se $A\mathbf{x} = \mathbf{0}$, então

$$\begin{aligned} A(k\mathbf{x}) &= kA\mathbf{x} \\ &= k\mathbf{0} \\ &= \mathbf{0}. \end{aligned}$$

Note que sistemas homogêneos de equações lineares podem ser também definidos com coeficientes e variáveis em corpos diferentes de $\mathbb{R}$. Assim, As soluções de um sistema deste tipo onde as variáveis e coeficientes são complexos formam um subespaço de $\mathbb{C}^n$, e de maneira geral, a soluções de um sistema como este em um corpo K qualquer é subespaço de K^n. ◀

★ **Exemplo 1.59.** No espaço $\mathbb{Z}_2^5$, os vetores da forma 0xxx0 (ou seja, o primeiro e último elemento são zero) formam um subespaço:

- O vetor zero – 00000 está contido no subespaço;
- A soma 0xxx0 $\oplus$ 0yyy0 resulta em um vetor da forma 0zzz0;
- A multiplicação por escalar também resulta em vetores da mesma forma: $0 \wedge (0xxx0) = (00000)$, e $1 \wedge (0xxx0) = 0xxx0$. ◀

★ **Exemplo 1.60.** Considere o espaço $\mathbb{Z}_2^4$. O conjunto a seguir é seu subespaço:

$$C = \{0000, 0011, 1101, 1110\}.$$

- $0000 \in C$.
- A soma ($\oplus$) de elementos de C resulta em outro elemento de C:

$$0011 \oplus 1101 = 1110$$
$$0011 \oplus 1110 = 1101$$
$$1101 \oplus 1110 = 0011$$

  Além disso, a soma de qualquer vetor com ele mesmo resulta em 0000, e a soma de qualquer vetor com zero resulta no próprio vetor.

- A multiplicação ($\wedge$) pelos escalares resulta em elemento de C: $0 \wedge x = 0$ e $1 \wedge x = x$.

◀

Teorema 1.61. *Sejam U, W subespaços de um espaço vetorial V. Então $U \cap W$ também é subespaço de W.*

Demonstração. Como ambos são subconjuntos de V, basta mostrar que $U \cap W$ é fechado para as operações.

Sejam $\mathbf{x}, \mathbf{y} \in U \cap W$ e c um escalar. Como $\mathbf{x} \in U$ e $\mathbf{x} \in W$, temos $c\mathbf{x} \in U$ e $c\mathbf{x} \in W$, e portanto $c\mathbf{x} \in U \cap W$,

Similarmente, como $\mathbf{x}, \mathbf{y}$ estão tanto em U como em W, $\mathbf{x} + \mathbf{y}$ também devem pertencer a U e a W. Concluímos que $\mathbf{x} + \mathbf{y} \in U \cap W$. ■

Exemplo 1.62. Considere os subespaços de $\mathbb{R}^3$:

$$A = \left\{ (x, y, 0)^T : \ x, y \in \mathbb{R} \right\}$$
$$B = \left\{ (x, y, 2y)^T : \ x, y \in \mathbb{R} \right\}.$$

Estes subespaços são planos passando pela origem. A interseção deles é $R = \left\{ (x, y, 0)^T : \ x \in \mathbb{R} \right\}$, que também é subespaço de $\mathbb{R}^3$. ◀

Exemplo 1.63. Seja A o espaço das matrizes diagonais de ordem tres, e B o espaço das matrizes quadradas de ordem tres com traço zero.

A interseção $A \cap B$ é o conjunto das matrizes diagonais de ordem tres com traço zero. Este é, também um espaço vetorial, com as mesmas operações usuais de soma de matrizes e multiplicação por escalar. ◀

Exemplo 1.64. Seja $\mathcal{F}(\mathbb{R})$ o espaço vetorial das funções reais. Considere dois subespaços de $\mathcal{F}(\mathbb{R})$:

i) O conjunto das funções reais contínuas, C^0;

ii) O conjunto das funções reais pares P.

A interseção desses dois é formada pelo conjunto das funções reais contínuas pares. Esta interseção é também subespaço de $\mathcal{F}(\mathbb{R})$:

- A função constante zero é contínua e par;

- Multiplicar uma função contínua e par por um escalar resulta em outra função contínua e par;
- A soma de duas funções contínuas pares é uma função contínua par. ◀

Exemplo 1.65. Seja A o espaço de todas as sequencias reais constantes, e B o espaço de todas as sequencias de números inteiros pares. A interseção dos dois conjuntos é o conjunto das sequencia de constantes inteiros pares, que é também espaço vetorial. ◀

Definição 1.66 (Soma de espaços vetoriais)**.** Se V é um espaço vetorial e $U, W \subset V$, então dizemos que

$$U + W = \{u + w : u \in U, w \in W\}$$

é a *soma* de U e W. ⧫

Exemplo 1.67. Os conjuntos A, da forma $(0, x, y, 0)^T$, B da forma $(0, 0, y, z)^T$ são subespaços de $\mathbb{R}^4$. A soma destes dois subespaços é

$$A + B = \{\, \mathbf{u} + \mathbf{v} : \ \ \mathbf{u} \in A, \mathbf{v} \in B \,\}.$$

o conjunto $A + B$ contém vetores da forma $(0, x, y, 0)^T + (0, 0, y, z)^T$, que é o mesmo que $(0, x, 2y, z)^T$, ou $(0, x, y, z)^T$ – a primeira coordenada é zero, e as outras três são livres (nenhuma depende da outra).

Note que há muitos vetores em $A \cap B$. Por exemplo, $(0, 0, 1, 0)^T$ está tanto em A como em B, assim como $(0, 0, 2, 0)^T$ – na verdade, $(0, 0, c, 0)^T \in A \cap B$ para todo $c \in \mathbb{R}$. ◀

Definição 1.68 (Soma direta)**.** Seja um espaço vetorial V com subespaços U e W. Dizemos que V é *soma direta* de U e W se V é soma de U e W, e $U \cap W = \{\, \mathbf{0} \,\}$. Denotamos a soma direta por $V = U \oplus W$. ⧫

Proposição 1.69. *Seja V um espaço vetorial com subespaços U e W. Então $V = U \oplus W$ se e somente se, para todo $\mathbf{v} \in V$, existe um único $\mathbf{u} \in U$ e um único $\mathbf{w} \in W$ tal que $\mathbf{v} = \mathbf{u} + \mathbf{w}$,*

Exemplo 1.70. Seja A o subespaço de $\mathbb{R}^3$ formado pelos vetores da forma $(x, y, 0)^T$, e seja B o subespaço de $\mathbb{R}^3$ formado por vetores da forma $(0, 0, z)^T$. Qualquer vetor de $\mathbb{R}^3$ pode ser descrito de forma única como a soma de um vetor de A com outro de B:

$$(x, y, z)^T = (x, y, 0)^T + (0, 0, z)^T,$$

portanto $\mathbb{R}^3 = A \oplus B$. Outra maneira de decompor $\mathbb{R}^3$ é em três subespaços, X, Y e Z, contendo vetores da forma $(x, 0, 0)^T$, $(0, y, 0)^T$ e $(0, 0, z)^T$, respectivamente. Um vetor de $\mathbb{R}^3$ então pode ser decomposto unicamente em

$$(x, y, z)^T = (x, 0, 0)^T + (0, y, 0)^T + (0, 0, z)^T.$$

Podemos generalizar, definindo que para qualquer n, $\mathbb{R}^n$ pode ser decomposto em subespaços onde cada subespaço representa algumas das dimensões:

$$\begin{aligned}(v_1, v_2, \ldots, v_n)^T = &(v_1, 0, 0, \ldots)^T \\ &+ (0, v_2, v_3, 0, 0, \ldots)^T \\ &+ \ldots \\ &+ (0, 0, \ldots, v_n)^T.\end{aligned}$$

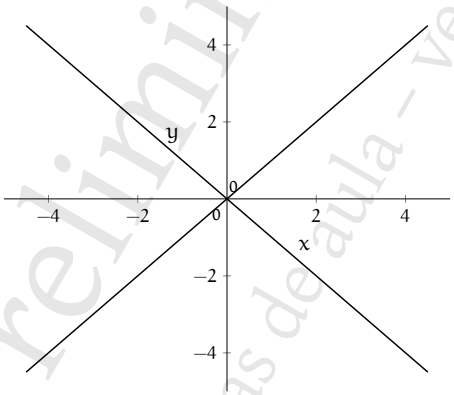
De maneira geral, $\mathbb{R}^3$ pode ser decomposto na soma direta de três retas não colineares, ou de um plano e uma reta não pertenente a este plano (todos sempre passando pela origem). ◀

Exemplo 1.71. A soma do exemplo 1.67 *não* é soma direta, porque um vetor $(0, a, b, c)$ em $A + B$ pode ser decomposto de diferentes maneiras:

$$\begin{aligned}(0,a,b,c)^T &= (0,a,b,c)^T + (0,0,0,0)^T \\ &= (0,a,0,c)^T + (0,0,b,0)^T \\ &= (0,a,\frac{b}{2},0)^T + (0,0,\frac{b}{2},c)^T \\ &\vdots\end{aligned}$$

◀

Exemplo 1.72. Os conjuntos $A = \{(x,y)^T : \ x+y=0\}$ e $B = \{(x,y)^T : \ x-y=0\}$ descrevem duas retas em $\mathbb{R}^2$, ambas contendo a origem.



Então

$$A + B = \{(x,y)^T : \ x+y=0 \text{ ou } x-y=0\},$$

mas como $A \cap B = \{\mathbf{0}\}$ e $A + B = \mathbb{R}^2$, logo temos

$$A \oplus B = A + B = \mathbb{R}^2.$$

Podemos também observar que é possível escrever qualquer vetor de $\mathbb{R}^2$ como soma de um vetor dentro de cada reta na figura. ◀

Exemplo 1.73. Seja $\mathbb{R}_n[x]$ o espaço vetorial dos polinômios com grau máximo n e coeficientes reais. Considere os dois subconjuntos de $\mathbb{R}_n[x]$:

- $\mathbb{R}_{m-1}[x]$, o espaço dos polinômios com grau máximo $m-1$;
- $\mathbb{R}_{m..n}[x]$, o espaço dos polinômios com grau entre m e n, *mais o polinômio zero*, com $0 < m < n$.

Qualquer polinômio de $\mathbb{R}_n[x]$ pode ser descrito unicamente como a soma de um polinômio de $\mathbb{R}_{m-1}(x)$ com outro de $\mathbb{R}_{m..n}[x]$:

$$\begin{aligned}&a_n x^n + a_{n-1}x^{n-1} + \ldots + a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 \\ &= \underbrace{\left(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_m x^m\right)}_{\in \mathbb{R}_{m..n}[x]} + \underbrace{\left(a_{m-1}x^{m-1} + \ldots + a_1 x + a_0\right)}_{\in \mathbb{R}_{m-1}[x]}.\end{aligned}$$

Note que o lado esquerdo pode ser zero (que pertence a $\mathbb{R}_{m..n}[x]$) se todos os coeficientes ali forem zero. Assim, temos $\mathbb{R}_n[x] = \mathbb{R}_m[x] \oplus \mathbb{R}_{m..n}[x]$.

Mais concretamente: seja $\mathbb{R}_4[x]$ o conjunto de todos os polinômios com grau no máximo 4. Então $\mathbb{R}_4[x]$ pode ser decomposto, por exemplo, em

- $\mathbb{R}_2[x]$, o espaço dos polinômios com grau máximo 2;
- $\mathbb{R}_{3..4}[x]$, o espaço dos polinômios com grau entre 3 e 4, *mais o polinômio zero*.

Qualquer polinômio de grau menor ou igual a quatro pode ser escrito como a soma de (i) um polinômio de grau entre 3 e 4, ou zero, e um polinômio de grau no máximo 2:

$$\begin{aligned} & a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \\ = & \underbrace{\left(a_4x^4 + a_3x^3\right)}_{\in \mathbb{R}_{3..4}[x]} + \underbrace{\left(a_2x^2 + a_1x + a_0\right)}_{\in \mathbb{R}_2[x]}. \end{aligned}$$

◀

★ **Exemplo 1.74.** Sejam

i) A o espaço gerado pelas sequencias de bits 0110 e 1001;

ii) B o espaço gerado pela sequencia de bits 0100;

iii) C o espaço gerado pela sequencia de bits 1000.

O espaço $\mathbb{Z}_2^4$ é igual a $A \oplus B \oplus C$. Temos

$$\begin{aligned} A &= \{0000, 0110, 1001, 1111\}, \\ B &= \{0000, 0100\}, \\ C &= \{0000, 1000\}. \end{aligned}$$

Qualquer vetor (sequencia de bits) de $\mathbb{Z}_2^4$ pode ser escrita como soma de vetores desses conjuntos. ◀

1.6 Aplicações

Esta Seção detalha três exemplos práticos do uso de estruturas algébricas: o primeiro e o terceiro em Criptografia; o segundo na determinação de um método para resolver o cubo mágico (ou cubo de Rubik); o terceiro em Criptanálise; e o último em códigos corretores de erros. Grupos são também muito usados em algumas áreas da Química e da Física [Bis93; Ham89; Cor97].

1.6.1 Protocolo Diffie-Hellman para acordo de chaves [grupo]

A Criptografia nos oferece métodos para realizar comunicação privada, mesmo que o canal (meio) usado seja público. Por exemplo, podemos usar Criptografia para enviar mensagens secretas pela Internet, e para acessar sistemas bancários sem que intrusos obtenham nossa senha, e poderíamos citar uma grande quantidade de outras situações onde a Criptografia nos protege, garantindo sigilo.

Antes da era moderna da Criptografia, o método usado para encriptar e decriptar mensagens envolvia apenas uma chave secreta: se uma mensagem é encriptada com chave ("senha") k, ela pode ser decriptada por qualquer um que conheça aquela chave.

Suponha que Alice e Bob queiram trocar mensagens em segredo[8], mas estejam fisicamente distantes

[8] É comum em Criptografia darmos nomes aos dois usuários de um sistema criptográfico de "Alice" e "Bob".

(em países diferentes, por exemplo). Suponha também que eles só podem se comunicar por um canal inseguro: cartas que são bisbilhotadas pelo serviço secreto, telefone grampeado, ou conexão insegura por rede de computadores. Aparentemente é impossível que os dois consigam fazê-lo sem se encontrarem fisicamente, porque teriam que definir uma chave secreta para poderem encriptar as mensagens – e ambos precisam conhecer a mesma chave.

Em 1976, Whitfield Diffie e Martin Hellman mostraram como resolver este problema, apresentando um método para que duas pessoas possam definir conjuntamente um segredo, comunicando-se apenas por canais públicos[9]. Este método foi publicado com o título "New directions in Cryptography" [DH76]. Hoje o método é conhecido como *protocolo Diffie-Hellman para acordo de chaves*. A seguir descrevemos de maneira simplificada o método desenvolvido por eles.

Alice e Bob deverão portanto determinar, de comum acordo, um segredo (a chave criptográfica para se comunicarem, por exemplo) – mas que só podem se comunicar em público (postando recados em um quadro de avisos, usando uma linha telefônica grampeada, ou através de uma rede de computadores desprotegida).

O protocolo Diffie-Hellman usa operações em um grupo. Para um exemplo simples[10], usaremos um grupo definido da seguinte forma: o conjunto de elementos é $\{1, 2, \ldots, p-1\}$, onde p é um número primo. A operação de grupo para dois elementos a e b é $a \cdot b$ = resto da divisão de ab por p. Por exemplo, se $p = 7$, então para calcular $5 \cdot 6$, fazemos $5 \times 6 = 30$, e tomamos o resto da divisão de 30 por 7, que é 2.

Observe que como p (neste exemplo, 5 é primo), o resultado da operação nunca será zero, portanto nunca obteremos um elemento fora do

Exemplo 1.75. Escolhemos, para fins didáticos[11], $p = 5$. Os elementos do grupo são $\{1, 2, 3, 4\}$.

Calculamos como exemplo $2 \cdot 2$. Temos $2 \times 2 = 4$, e o resto de $4 \div 5$ é 4, portanto $2 \cdot 2 = 4$.

Agora calculamos $3 \cdot 2$. Temos $3 \times 2 = 6$. O resto de $6 \div 4$ é 2, portanto $3 \cdot 2 = 2$. ◀

Em grupos definidos desta forma, sempre haverá pelo menos um elemento g que podemos usar para escrever todos os outros elementos usando a operação de grupo. Chamamos este elemento de *gerador* do grupo. No exemplo anterior, podemos escrever todos os elementos usando somente $g = 2$. Por exemplo,

- O elemento 4 pode ser escrito como $2 \cdot 2$, porque calculamos $2 \times 2 = 4$, e o resto de $4 \div 5$ é 4.
- O elemento 3 pode ser escrito como $2 \cdot 2 \cdot 2$:

$$\begin{aligned} 2 \cdot 2 \cdot 2 &= (2 \cdot 2) \cdot 2 && \text{(a operação é associativa)} \\ &= 4 \cdot 2 && \text{(já calculado antes, } 2 \cdot 2 = 4) \\ &= \text{resto de } 8 \div 5 \\ &= 3. \end{aligned}$$

O mesmo pode ser feito para o elemento 1:

$$\begin{aligned} 2 \cdot 2 \cdot 2 \cdot 2 &= (2 \cdot 2) \cdot (2 \cdot 2) && \text{(a operação é associativa)} \\ &= 4 \cdot 4 && \text{(já calculado antes, } 2 \cdot 2 = 4) \\ &= \text{resto de } 16 \div 5 \\ &= 1. \end{aligned}$$

[9] O método funciona de forma que duas pessoas poderiam usá-lo em uma sala com diversas outras pessoas: os dois participantes ditam em voz alta números um ao outro, e depois de um tempo ambos conhecem um segredo que ninguém mais na sala conhece.

[10] Em situações práticas, há diversas restrições quanto à forma como o grupo é definido; a apresentação do protocolo neste texto foi simplificada.

[11] Na prática, p deve ser muito grande.

Vemos portanto que podemos escrever todos os elementos usando somente 2:

$$
\begin{aligned}
2 &= 2 \\
4 &= 2 \cdot 2 && (2 \times 2 = 4.\ \text{Resto de } 4 \div 5 \text{ é } 4) \\
3 &= 2 \cdot 2 \cdot 2 && (\text{Resto de } 8 \div 5 \text{ é } 3) \\
1 &= 2 \cdot 2 \cdot 2 \cdot 2 && (\text{Resto de } 16 \div 5 \text{ é } 1)
\end{aligned}
$$

É comum usar a notação g^a para $\overbrace{ggg\cdots g}^{a \text{ vezes}}$, portanto

$$
\begin{aligned}
2 &= 2^1 \\
4 &= 2^2 \\
3 &= 2^3 \\
1 &= 2^4
\end{aligned}
$$

Em grupos como este, calcular g^a a partir de g e a pode ser feito rapidamente, mas calcular a a partir de g^a é extremamente demorado: para p perto de 2^{2048}, um computador demoraria centenas de anos para terminar o cálculo.

Depois de definir p e determinar g (que podem ser públicos), Alice e Bob seguem os passos a seguir.

1. Alice escolhe aleatoriamente seu segredo, $1 < a < p$.
2. Bob também escolhe seu segredo, $1 < b < p$.
3. Alice envia para Bob g^a.
4. Bob envia para Alice g^b.
5. Alice, tendo o valor enviado por Bob, calcula $(g^b)^a$, que é igual a g^{ab} (verifique!).
6. Bob faz o mesmo, e calcula $(g^a)^b$, obtendo também g^{ab}.

Agora Alice e Bob tem o mesmo valor, g^{ab}, que pode ser usado como senha, porque é conhecido apenas por eles. Os dados enviados em público e que podem ser capturados pelo adversário são g^a e g^b, mas com estes dois valores seria difícil calcular a, b ou g^{ab}, e portanto Alice e Bob atingiram seu objetivo.

O grupo que apresentamos neste exemplo não é o único usado com o protocolo Diffie-Hellman – em aplicações práticas grupos diferentes, com operações mais complexas são usados. No entanto, o protocolo é definido para quaisquer grupos onde haja um gerador[12], facilitando sua exposição e estudo.

A dificuldade de determinar a dado g^a neste grupo é fundamental em Criptografia: dizemos que $f(a) = g^a$ é uma "função de mão única", porque é fácil de calcular mas difícil de inverter[13] (a definição precisa de "difícil" fica fora do escopo deste texto, mas está relacionada com o tempo necessário para efetuar a operação).

A exposição do protocolo Diffie-Hellman e de diferentes usos de grupos em Criptografia é padrão na literatura da área. O livro de Douglas Stinson é bastante acessível [Sti06]; o de Katz e Lindell traz uma discussão mais aprofundada dos fundamentos teóricos [KL08].

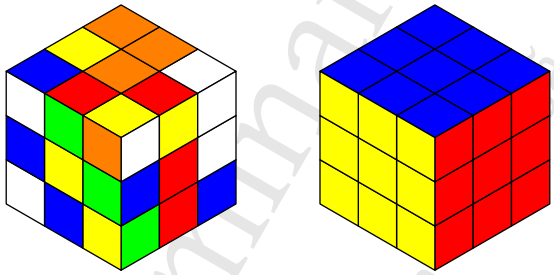
[12] Há grupos que não são gerados por um único elemento.

[13] Mais precisamente, dado $y = f(x)$, é difícil encontrar algum elemento em sua pré-imagem.

1.6.2 Cubo de Rubik [grupo]

Grupos são usados no estudo do método para solução do cubo de Rubik, e este é um exemplo importante de grupo (e de estrutura algébrica) porque os elementos do grupo são *movimentos*.

O cubo de Rubik é um quebra-cabeças tridimensional no formato de cubo que permite rotacionar cada uma de suas seis faces nos dois sentidos (horário e anti-horário). Desta forma, o cubo tem cada face dividida em nove pequenos quadrados, e cada face tem inicialmente uma cor diferente das outras.



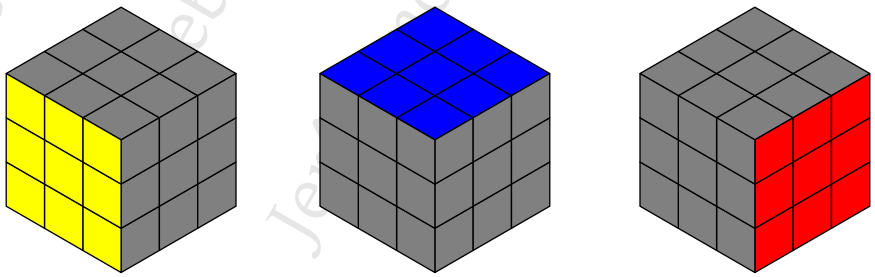
Ao rotacionar as faces, elas ficam em *configurações* diferentes. Em cada configuração as faces podem apresentar suas partições (os pequenos quadrados) com diversas cores diferentes.

O objetivo do jogador é levar o cubo da configuração em que estiver para a configuração inicial, com cada face tendo uma única cor.

O grupo usado no estudo do cubo de Rubik tem como elementos o conjunto de todas as possíveis modificações na configuração do cubo (ou seja, todas as sequências de rotações das faces) mais o movimento nulo, e a operação do grupo é a concatenação (aplicação em sequência). As rotações são descritas usando a seguinte notação:

- F é a face da frente (“*Front*”);
- B é a face de trás (“*Back*”);
- U é a face de cima (“*Up*”);
- D é a dace de baixo (“*Down*”);
- L é a face da esquerda (“*Left*”);
- R é a face da direita (“*Right*”).

A figura a seguir mostra as faces F, T e R.



Denotamos a rotação no sentido horário pelo nome da face: "F" é a rotação da face frontal 90º no sentido horário.

A rotação no sentido anti-horário é denotada pelo nome da face com a marca de um apóstrofo: F' é a rotação da face frontal 90º no sentido anti-horário.

Duas rotações iguais em seguida formam uma rotação de 180º, que é denotada pelo nome da face com uma indicação: F^2 é o mesmo que F seguida de F.

Os elementos do grupo são as rotações básicas, já mencionadas (F, B, U, ..., F', ..., F^2, ...) e suas composições em sequência, FUB, F^2DU, etc. Note que $FFF = F^2F = F'$.

O movimento nulo é denotado por E (*"Empty"*).

Verificamos que o conjunto e operação dados é realmente um grupo:

- A operação de grupo (duas rotações) resulta em outro elemento do grupo.
- A operação é associativa.
- O movimento nulo é o elemento neutro.
- Para cada rotação existe outra no sentido contrário, e se as realizarmos em sequência não alteramos a configuração do cubo (e isso portanto é equivalente ao movimento nulo).

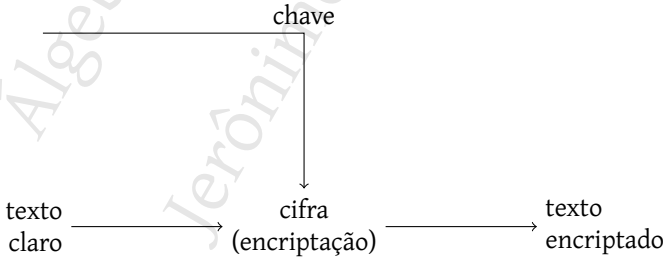
A operação do grupo não é comutativa – basta observar que de maneira geral, FR leva a uma configuração diferente de RF.

Um dos fatos básicos sobre grupos que podemos usar ao raciocinar sobre o cubo é o primeiro teorema que provamos: todo elemento em um grupo tem um único inverso – e portanto toda sequencia de movimentos, da maneira como as definimos, tem uma única sequência inversa.

O grupo descrito nesta Seção pode ser usado para derivar um método para solução do cubo de Rubik (onde "solução" significa levar o cubo de qualquer configuração para a inicial) – o leitor poderá consultar, por exemplo os livros "Notes on Rubik's 'Magic Cube'", de David Singmaster [Sin81] e "Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and Other Mathematical Toys", de David Joyner [Joy08].

★ 1.6.3 Criptanálise moderna [corpo; sistemas lineares em corpos]

Uma *cifra* é uma ferramenta criptográfica usada para garantir sigilo em comunicações: uma mensagem qualquer, representada como uma sequência de bits (e portanto um elemento de $\mathbb{Z}_2^n$), é "misturada" a uma chave secreta (que é outra sequência de bits), de forma que um intruso não possa identificar mais a mensagem (e nem possa, é claro, obter a chave secreta). Quando a mensagem chegar ao destinatário, a chave secreta é novamente usada para decodificar a mensagem.



A *Criptanálise* trata de verificar se uma ferramenta criptográfica é segura: tenta-se "quebrar" métodos criptográficos a fim de realizar algo semelhante a um controle de qualidade.

O método da *criptanálise algébrica* consiste em representar um criptossistema como um sistema de equações. A solução deste sistema poderá ser uma chave ou mensagem secreta (e portanto resolver o sistema deveria ser difícil).

Desenvolveremos um exemplo muito simplificado de cifra e mostraremos como ele pode ser quebrado.

Suponha que a entrada seja uma sequência de quatro bits, $b = b_3b_2b_1b_0$, e uma chave, que é uma sequência de quatro bits, $k = k_3k_2k_1k_0$. A saída é uma sequência de quatro bits, $c = c_3c_2c_1c_0$, e a cifra opera da seguinte maneira:

$$\begin{aligned} k_1 \oplus b_0 \oplus b_3k_2 &= c_3 \\ k_2 \oplus b_1 \oplus b_2k_3 &= c_2 \\ k_3 \oplus b_2 \oplus b_1k_0 &= c_1 \\ k_0 \oplus b_3 \oplus b_0k_1 &= c_0 \end{aligned}$$

Se conhecermos um par de texto claro e encriptado, podemos simplesmente substituir os b_i e c_j, obtendo um sistema linear. Suponha, por exemplo, que $b = 1001$ e $c = 1010$. Então o sistema linear a resolver em $\mathbb{Z}_2$ é

$$\begin{cases} k_1 \oplus 1 \oplus 1k_2 = 0 \\ k_2 \oplus 0 \oplus 0k_3 = 1 \\ k_3 \oplus 0 \oplus 0k_0 = 0 \\ k_0 \oplus 1 \oplus 1k_1 = 1 \end{cases}$$

Facilmente determinamos que a chave usada foi

$$k = k_3k_2k_1k_0 = 0100,$$

como é fácil verificar subtituindo k e b e obtendo o texto cifrado c.

O sistema descrito é fácil de quebrar por vários motivos, mas o mais evidente é que ele se resume a um sistema linear. Suponha que a cifra fosse, ao invés disso, determinada por

$$\begin{aligned} k_1k_2 \oplus b_0 \oplus b_3k_0k_1k_2 &= c_3 \\ k_2k_3 \oplus b_1 \oplus b_2k_1k_2k_3 &= c_2 \\ k_3k_0 \oplus b_2 \oplus b_1k_0k_1 &= c_1 \\ k_0k_1 \oplus b_3 \oplus b_0k_3k_2 &= c_0 \end{aligned}$$

Ainda que conheçamos um par de texto claro e o texto cifrado obtido dele, não é tão simples determinar a chave: supondo que $b = 1100$ e $c = 1010$, o sistema que teríamos que resolver é

$$\begin{cases} k_1k_2 \oplus 0 \oplus 1k_0k_1k_2 = 1 \\ k_2k_3 \oplus 0 \oplus 1k_1k_2k_3 = 0 \\ k_3k_0 \oplus 1 \oplus 0k_0k_1 = 1 \\ k_0k_1 \oplus 1 \oplus 0k_3k_2 = 0 \end{cases}$$

que não é linear, e envolve equações de grau três. Assim, a não-linearidade é uma essencial para a segurança de uma cifra criptográfica.

Algoritmos criptográficos são projetados como sequencias de operações em estruturas algébricas, de forma que seja fácil executá-las e que seja difícil invertê-las sem a chave.

Alguns exemplos de critpossistemas quebrados usando criptanálise algébrica são o AS/5, usado no padrão GSM de telefonia móvel, e o Keeloq, usado em dispositivos digitais em chaves de automóveis.

O livro de Douglas Stinson [Sti06] traz uma breve introdução à Criptanálise, embora não aborde a Criptanálise Algébrica, que tem como pré-requisito um curso básico de Álgebra Abstrata. Sobre Criptanálise Algébrica há o livro de Gregory Bard [Bar09] e o de Andreas Klein [Kle13] (estes dois últimos requerem considerável capacidade de abstração e preparo em Álgebra, Combinatória e Estatística).

1.6.4 Códigos corretores de erros [espaço vetorial; subespaço]

Quando uma mensagem eletrônica é transmitida na forma de sequência de bits, é possível que a transmissão inclua erros na mensagem – alguns dos bits podem vir trocados, porque os canais de transmissão não são perfeitos. Para detectar e automaticamente corrigir estes erros as mensagens podem ser codificadas de uma forma especial, usando um *código corretor de erros*.

Ao usar um código corretor de erros, enviamos mais informação do que apenas a mensagem, para que seja possível detectar quando um erro ocorre. É fácil perceber que informação adicional permite detectar e corrigir erros: se enviarmos cada mensagem cinco vezes, e em uma das vezes ela for transmitida com erro, o receptor decidirá que as quatro mensagens iguais devem ser aquela correta, e a quinta, diferente, deve ter sido transmitida com erro. O envio de múltiplas cópias, no entanto, não é eficiente: na verdade é possível corrigir erros usando menos redundância.

Em códigos corretores de erros é necessário medir quão diferentes duas palavras são. Para isso é usada a *distância de Hamming*[14].

Definição 1.76 (Distância de Hamming)**.** A *distância de Hamming* entre duas sequências de bits (ou seja, entre dois vetores de $\mathbb{Z}_2^n$) é a quantidade de posições em que eles diferem. Denotamos a distância de Hamming entre a e b por $d(a, b)$. ♦

Exemplo 1.77. Exemplificamos com a distância entre alguns vetores.

$$\begin{aligned} d(01011, 01000) &= 2 \\ d(0101, 0101) &= 0 \\ d(0001, 1010) &= 3. \end{aligned}$$ ◄

Supomos aqui que as mensagens a serem enviadas são divididas em blocos de k bits.

O emissor *codifica* as mensagens de k bits em palavras maiores, com $n > k$ bits. Os bits adicionais serão usados para permitir a detecção e correção de erros. Por exemplo, suponha que $k = 2$ e $n = 5$. O emissor então transforma as mensagens originais de 2 bits em outras mensagens com 5 bits:

$$\begin{aligned} 00 &\to 00000 \\ 01 &\to 01011 \\ 10 &\to 10110 \\ 11 &\to 11101 \end{aligned}$$

Este é um código que permite representar 4 palavras diferentes usando 5 bits, por isso é chamado de $[5, 4]$-código. Está claro que o emissor não usará todas as possíveis sequências de 5 bits.

A palavra enviada do emissor ao receptor é sempre uma daquelas quatro palavras de cinco bits. A mensagem codificada tem mais bits para adicionar *redundância.* O código que demos de exemplo transforma

[14] Trataremos em mais detalhes da definição de distância no Capítulo 7.

mensagens de dois bits em mensagens codificadas de cinco bits:

$$(m_1, m_2) \xrightarrow{\text{codificação}} (c_1, c_2, c_3, c_4, c_5).$$

Observamos que, como há somente 2^2 palavras de dois bits, que estamos descrevendo com cinco bits, não temos como usar todas as palavras de $\mathbb{Z}_2^5$ – as palavras codificadas formam um *subespaço* de $\mathbb{Z}_2^5$: o zero está contido no conjunto; a multiplicação ($\wedge$) por 0 ou por 1 resulta em palavra também no conjunto; e finalmente, a soma também resulta em palavra deste conjunto:

$$\begin{aligned} 01011 \oplus 10110 &= 11101 \\ 01011 \oplus 11101 &= 10110 \\ 10110 \oplus 11101 &= 01001 \end{aligned}$$

Após uma mensagem ser enviada, o receptor terá cinco bits. Se os bits corresponderem a uma das quatro palavras do código, ele decidirá que não houve erro e aceitará a mensagem. Se os bits não formarem uma palavra do código (ou seja se os bits pertencerem a $\mathbb{Z}_2^5$ mas não ao subespaço do código), ele decidirá que houve um erro.

Quando o receptor detecta um erro, ele automaticamente troca a mensagem recebida por uma do código – aquela que for mais próxima (usando a distância de Hamming) da que foi recebida.

Um subespaço de $\mathbb{Z}_2^n$ pode então ser visto como um código corretor de erros. O fato de códigos deste tipo serem descritos como subespaços de $\mathbb{Z}_2^n$ não é coicidência: para que os algoritmos usados para detectar e corrigir erros funcionem como projetados, o código deve necessariamente ser subespaço de $\mathbb{Z}_2^n$, e não apenas subconjunto.

Discutiremos mais sobre códigos corretores de erros na seção 4.8.4.

O livro de Hefez e Villela [HV08] é um texto introdutório aos códigos corretores de erros.

Exercícios

Ex. 1 — Mostre que $(\{0, 1\}, \oplus)$ é um grupo.

Ex. 2 — Na Seção 1.6.1 apresentamos uma estrutura e dissemos que é um grupo. Verifique que de fato se trata de um grupo (isso inclui, além de demonstrar que as propriedades valem, mostrar também que a operação de grupo sempre resulta em outro elemento do grupo – e que nunca resultará em zero, que não pertence ao grupo). Também dissemos que usando aquela operação do grupo, $(g^a)^b = g^{ab}$. Mostre que isso é verdade.

Ex. 3 — Prove que em qualquer grupo, o elemento neutro é único.

Ex. 4 — No exemplo 1.21 exibimos o corpo $\mathbb{Q}[\sqrt{2}]$, formado pelos números da forma $a + b\sqrt{2}$. Pode-se obter infinitos corpos como este, trocando $\sqrt{2}$ por outros números. Que números são estes? Demonstre o que foi afirmado neste exercício (que realmente se pode obter infinitos corpos desta forma).

Ex. 5 — O *produto de Hadamard* de duas matrizes A e B é a matriz C tal que $c_{ij} = a_{ij} b_{ij}$. Dados m e n, seja M o conjunto de matrizes $m \times n$ com coeficientes reais. Determine se $(M, +, \odot)$ é um corpo, onde $\odot$ é o produto de Hadamard.

Ex. 6 — Prove que o conjunto de todas as sequências de Fibonacci é um espaço vetorial (há infinitas possíveis sequências de Fibonacci, cada uma começando com diferentes valores para f_1 e f_2).

Ex. 7 — Além da operação lógicas **e** (denotada por $\wedge$) definida no texto, em Lógica definimos a operação **ou**, denotada por $\vee$, de forma que $a \vee b = 1$ se e somente se pelo menos um dentre a e b for 1. Determine se $(\{0, 1\}, \vee, \wedge)$ é um corpo.

Ex. 8 — Seja $X = \left\{ \frac{p(x)}{q(x)} \right\}$ onde p e q são polinômios com $q(x) \neq 0$. X é o conjunto de todas as funções racionais. Determine se X é um corpo com as operações usuais de soma e multiplicação para polinômios.

Ex. 9 — No exemplo 1.22, definimos as operações "E" lógico ($\wedge$) e "Ou-exclusivo" ($\oplus$). Verifique que estas duas operações são na verdade o mesmo que multiplicar e tomar o resto da divisão por 2; somar e tomar o resto da divisão por 2.

★ **Ex. 10 —** Resolva o sistema em $\mathbb{Z}_2$:

$$\begin{cases} 1x \oplus 1y \oplus 1z = 1 \\ 0x \oplus 1y \oplus 0z = 1 \\ 1x \oplus 0y \oplus 1z = 0. \end{cases}$$

Ex. 11 — Mostre um sistema linear em $\mathbb{Z}_2$ que não tenha solução.

Ex. 12 — Diga se são espaços vetoriais. Quando não especificadas, as operações são a soma e multiplicação usuais; o corpo usado nos espaços vetoriais é sempre $\mathbb{R}$.

i) O conjunto das funções constantes de $\mathbb{R}$ em $\mathbb{R}$.

ii) $\{ (a, b) \in \mathbb{R}^2 : \ a < b \}$.

iii) O conjunto das matrizes diagonais.

iv) O conjunto das matrizes triangulares superiores.

v) O conjunto dos números complexos com coeficientes racionais ($a + bi, \ a, b \in \mathbb{Q}$).

★ vi) O conjunto de todas as distribuições de probabilidade sobre um conjunto finito e enumerável. A operação de soma de vetores $\mathbf{p} = (p_1, p_2, \ldots, p_n)$ e $\mathbf{q} = (q_1, q_2, \ldots, q_n)$ é a distribuição onde cada evento i tem probabilidade $(p_i + q_i)/2$:

$$\mathbf{p} + \mathbf{q} = \left(\frac{(p_1 + q_1)}{2}, \frac{(p_2 + q_2)}{2}, \ldots, \frac{(p_n + q_n)}{2} \right)$$

O corpo é $\mathbb{R}$. O vetor $\mathbf{p}$ multiplicado pelo escalar c é

$$\begin{aligned} \mu &= \frac{1}{n} \sum_i p_i \\ k &= \operatorname{sen}^2 \left(\frac{\pi c}{2} \right) \\ c\mathbf{p} &= (kp_1 + (1-k)\mu, kp_2 + (1-k)\mu, \ldots, kp_n + (1-k)\mu) . \end{aligned}$$

vii) O conjunto de todas as funções $f : \mathbb{R} \to \mathbb{R}$ com período π.

viii) O conjunto de pontos com coordenadas pares em $\mathbb{R}^2$.

ix) O conjunto dos pontos com pelo menos uma coordenada prima em $\mathbb{R}^2$.

x) O conjunto de todas as funções reais com derivada positiva em todo o domínio.

★ xi) Dada uma partição dos reais em intervalos, o conjunto de funções que tem derivada com o mesmo sinal em cada um dos intervalos.

xii) Os vetores em $\mathbb{R}^n$ que, quando lidos, são palíndromos (ou seja, todos os vetores da forma[15] $(x_1, x_2, x_3, \ldots, x_{\lceil n/2 \rceil}, \ldots, x_3, x_2, x_1)$).

xiii) O conjunto de funções $F = \{ f(x) = a \cos x + b \operatorname{sen} x : \quad a, b \in \mathbb{R} \}$

Ex. 13 — Demonstre a proposição 1.69.

Ex. 14 — Dissemos no exemplo 1.38 que o conjunto de soluções para *qualquer* EDO linear homogênea é um espaço vetorial. Demonstre este fato.

Ex. 15 — Mostre que há equações diferenciais não lineares cujas soluções também formam um espaço vetorial.

Ex. 16 — Mostre que para a EDO $y'' + y' = 0$, as funções da forma $g(x) = ae^x - be^x$, com $a + b = 0$, são um subespaço do conjunto de soluções.

Ex. 17 — Prove que em qualquer espaço vetorial o elemento neutro para adição é único.

Ex. 18 — O conjunto de matrizes reais simétricas quadradas é subespaço do espaço de matrizes reais quadradas?

Ex. 19 — Seja A uma matriz $m \times n$. Para quais vetores $\mathbf{b}$ o conjunto $\{ \mathbf{x} : \quad A\mathbf{x} = \mathbf{b} \}$ é subespaço de $\mathbb{R}^n$?

Ex. 20 — Prove que em um espaço vetorial,

i) $0\mathbf{v} = \mathbf{0}$.

ii) $-1\mathbf{v} + \mathbf{v} = \mathbf{0}$.

iii) $c\mathbf{0} = \mathbf{0}$.

iv) Se $\mathbf{u} + \mathbf{v} = \mathbf{u}$ então $\mathbf{v} = \mathbf{0}$.

v) Dado $\mathbf{v}$, $-\mathbf{v}$ é único.

vi) Se $c\mathbf{v} = \mathbf{0}$ então $c = 0$ ou $\mathbf{v} = \mathbf{0}$.

Ex. 21 — Prove que a quantidade de vetores em um espaço vetorial sobre um corpo F é finita se e somente se F é finito.

Ex. 22 — O primeiro quadrante é um subespaço de $\mathbb{R}^2$? Ou, de maneira geral, o primeiro ortante é subespaço de $\mathbb{R}^n$?

Ex. 23 — Encontre subespaços não-triviais do espaço vetorial de n bits, definido no exemplo 1.40.

[15] Na fórmula descrevendo o vetor, $\lceil n/2 \rceil$ é o menor inteiro maior ou igual a $n/2$. Por exemplo, $\lceil 3 \rceil = 3$ e $\lceil 4.2 \rceil = 5$.

Ex. 24 — O exemplo 1.57 lista alguns subespaços de $\mathcal{F}(\mathbb{R})$. Prove que são de fato subespaços.

Ex. 25 — No exemplo 1.58 não verificamos que a multiplicação de uma solução por escalar resulta em outra solução. Verifique.

Ex. 26 — Considere os dois sistemas lineares com os mesmos coeficientes (a mesma matriz A):

i) $A\mathbf{x} = \mathbf{0}$

ii) $A\mathbf{x} = \mathbf{b}$

Se $\mathbf{v}$ é solução para (i) e $\mathbf{w}$ é solução para (ii), então $\mathbf{v} + \mathbf{w}$ é soluçào para um dos dois sistemas. Qual deles? Explique.

Ex. 27 — No exemplo 1.58 verificamos que o conjunto de soluções para um sistema homogêneo de equações lineares é subespaço de $\mathbb{R}^n$. Explique porque isso não vale para sistemas não homogêneos.

Ex. 28 — Para qualquer conjunto X, denotamos por 2^X o conjunto de todos os subconjuntos de X. Por exemplo,

$$\begin{aligned} A &= \{1, 2, 3\} \\ 2^A &= \{\emptyset, \{1\}, \{2\}, \{3\}, \\ &\quad \{1, 2\}, \{1, 3\}, \{2, 3\}, \\ &\quad \{1, 2, 3\}\} \end{aligned}$$

Agora considere as seguintes operações que levam um elemento de $\mathbb{Z}_2$ (ou seja, 0 ou 1) e um conjunto em um outro conjunto:

$$\begin{aligned} 1 \otimes A &= A \\ 0 \otimes A &= \emptyset \end{aligned}$$

Dado um conjunto X, determine se 2^X com a operação $\otimes$ é um espaço vetorial sobre $\mathbb{Z}_2$.

Ex. 29 — Considere o conjunto de todas as matrizes reais diagonais de ordem n, para algum n fixo. Quais são as duas operações que poderíamos usar sobre este conjunto para obter um corpo?

Ex. 30 — Mostre que o conjunto de todas as variáveis aleatórias relacionadas a um mesmo experimento *e que tenham variância finita* formam um espaço vetorial quando usamos a operação usual de soma de variáveis aleatórias e a multiplicação de uma variável por número real.

Ex. 31 — Mostre que as funções constantes de $\mathbb{R}$ em $\mathbb{R}$ são subespaço de $C[-a, b]$.

Ex. 32 — Mostre que um conjunto de pontos (x, y) tais que $y = p(x)$, onde p é um polinômio de grau maior ou igual a dois, *não* é subespaço de $\mathbb{R}^2$.

★ **Ex. 33 —** Mostramos neste texto que o conjunto grafos de ciclos disjuntos é um espaço vetorial. usando as mesmas operações, diga se são espaços vetoriais:

i) O conjunto de subgrafos de um grafo;

ii) O conjunto de subgrafos conexos de um grafo (um grafo é *conexo* se sempre há caminho entre quaisquer dois de seus vértices).

Ex. 34 — Em $M_{n\times n}$, a função que dá o *traço* (somatório da diagonal) de uma matriz é $\mathrm{Tr} : M_{n\times n} \to \mathbb{R}$. Mostre que o conjunto das matrizes $n \times n$ com traço zero é um subespaço de $M_{n\times n}$.

Ex. 35 — Identifique o complemento do subespaço mencionado no exercício 34.

Ex. 36 — Sabemos que $M_{n\times n}$ é espaço vetorial. Prove que o conjunto das matrizes simétricas $S_{n\times n}$ é subespaço de $M_{n\times n}$, e que o conjunto $\overline{S}_{n\times n}$ das matrizes antissimétricas é complemento de $S_{n\times n}$.

Ex. 37 — O conjunto $\mathcal{F}(\mathbb{R})$ de funções reais é soma direta dos conjuntos de funções pares e funções ímpares?

Ex. 38 — O conjunto $M_{3\times 3}$ das matrizes quadradas de ordem 3 pode é soma direta de:

i) Matrizes de ordem 3 não-positivas e matrizes de ordem 3 não-negativas?

ii) Matrizes de ordem 3 singulares e matrizes não-singulares?

Ex. 39 — Diga quando se trata de soma, soma direta ou nenhum deles.

i) Sequências reais; sequências constantes; sequências não constantes.

ii) Sequências estritamente crescentes; sequências não estritamente crescentes.

iii) Todas as soluções da equação diferencial $y'' - y = 0$; as soluções da forma ke^{-x}; a solução trivial mais as soluções da forma $je^{x} - ke^{-x}$, com $k, j \neq 0$.

Capítulo 2

Dimensão e Bases

Neste Capítulo, revemos os conceitos de combinação e dependência linear, presumidamente já estudados em Geometria Analítica, desta vez de forma mais abstrata, e os usamos para construir os conceitos de *base* de um espaço vetorial e de *coordenadas* de vetores em diferentes bases.

2.1 Dependência linear

Definição 2.1 (Combinação linear)**.** Uma *combinação linear* de um conjunto finito de vetores $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ em um espaço vetorial V sobre um corpo F é um vetor da forma

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \ldots + a_k\mathbf{v}_k$$

onde os a_i são escalares (elementos do corpo F). ♦

Exemplo 2.2. Em $\mathbb{R}^3$, considere os vetores $u = (0, 2, 0)^T$ e $v = (0, 0, 1)^T$. Então os seguintes vetores são combinações lineares de u e v:

$$\begin{aligned} u + v &= (0, 2, 1) \\ u + 2v &= (0, 2, 2) \\ u/2 + v &= (0, 1, 1) \\ 10u &= (0, 20, 0) \end{aligned}$$

Note que não há combinação linear de u e v com o primeiro elemento diferente de zero. ◄

Definição 2.3 (Dependência linear)**.** Seja $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ um conjunto de vetores em um espaço vetorial V. Se um dos vetores em S puder ser escrito como combinação linear dos outros, o conjunto S é *linearmente dependente*, ou *LD*. Caso contrário, é *linearmente independente*, ou *LI*. ♦

Equivalentemente, um conjunto de vetores $\mathbf{v}_1, \ldots \mathbf{v}_k$ é LI se a combinação linear

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \ldots + a_k\mathbf{v}_k = 0$$

implica em $a_1 = a_2 = \ldots = a_k = 0$.

Exemplo 2.4. Temos a seguir conjuntos de vetores em $\mathbb{R}^2$.

$$\begin{aligned} A &= \{(1,1)^T, (2,2)^T\} \\ B &= \{(1,1)^T, (-1,-1)^T\} \\ C &= \{(1,1)^T, (1,2)^T\} \\ D &= \{(1,1)^T, (1,2)^T, (-1,1)^T\} \end{aligned}$$

os conjuntos A, B e D são LD, porque

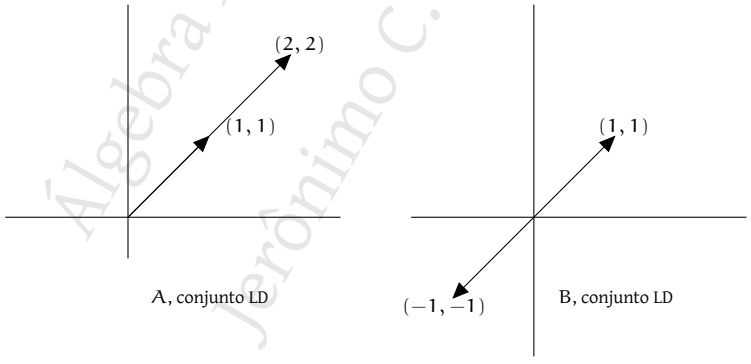
$$\begin{aligned} 2(1,1)^T &= (2,2)^T \\ -1(1,1)^T &= (-1,-1)^T \\ \frac{3}{2}(1,1) + \frac{1}{2}(-1,1) &= (1,2)^T \end{aligned}$$

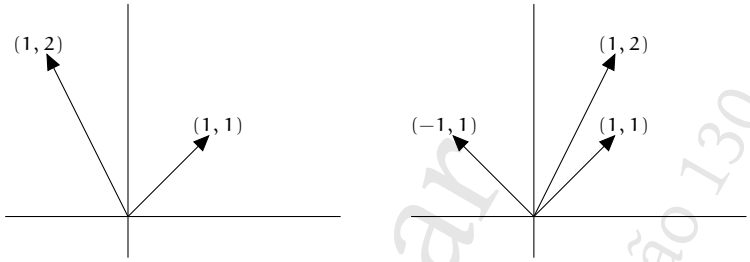
O conjunto C é LI. Se tentarmos obter valores a e b tais que $a(1,1)^T = b(1,2)^T$, teremos

$$\begin{aligned} a &= b, \\ a &= 2b, \end{aligned}$$

o que só é possível com $a = b = 0$.

A Figura a seguir ilustra geometricamente estes conjuntos de vetores.





C, conjunto LI D, conjunto LD

O conjunto C tem exatamente dois vetores não colineares. Os outros tem vetores colienares (A, B) ou tem mais de dois vetores (D). ◀

Exemplo 2.5. Em $\mathbb{R}^3$, os vetores

$$\begin{aligned}\mathbf{u} &= (-1/2, -1, 1/2)^T,\\ \mathbf{v} &= (-1/2, 2, 1)^T,\\ \mathbf{w} &= (1/4, 2, 0)^T\end{aligned}$$

são LD, porque $\mathbf{u} = -\mathbf{v} + (1/2)\mathbf{w}$. ◀

Exemplo 2.6. No espaço de polinômios $\mathbb{R}_2[x]$, os vetores (polinômios) x^2+2, $x-1$ e $3x^2+2x+4$ são um conjunto L.D., porque o último é combinação linear dos outros dois: $3x^2+2x+4 = 3(x^2+2)+2(x-1)$. ◀

Exemplo 2.7. No espaço das funções de $\mathbb{R}$ em $\mathbb{R}$, os vetores (ou seja, as funções) $f(x) = 3x$, $g(x) = \cos(x)$ e $h(x) = \ln(x)$ são L.I., porque nenhuma delas pode ser escrita como combinação linear das outras: não existem a, b e c diferentes de zero tais que

$$a(3x) + b\cos(x) + c\ln(x) = 0 \tag{2.1}$$

para todo x. Para mostrar este fato, supomos que existam b e c tais que a equação 2.1 valha. Então, teríamos

$$a = \frac{-c\ln(x) - b\cos(x)}{3x}, \tag{2.2}$$

para *todo* x, com b e c constantes. Mas o valor de a, que presumimos ser constante, dependeria do valor de x, porque o lado direito da equação 2.2 não é constante: como contraexemplo basta tomar $x = e$, $x = 1$, $x = \pi$ e $x = 2\pi$, por exemplo, e temos

$$\begin{aligned}a &= \frac{-c\ln(1) - b\cos(1)}{3} \approx -0.1801c,\\ a &= \frac{-c\ln(\pi) - b\cos(\pi)}{3\pi} \approx 0.1061b - 0.1214c,\\ a &= \frac{-c\ln(2\pi) - b\cos(2\pi)}{6\pi} \approx -0.0530b - 0.0975c,\end{aligned}$$

$$a = \frac{-c\ln(e) - b\cos(e)}{3e} \approx 0.1118b - 0.1226c.$$

Este sistema linear só tem a solução trivial com $a = b = c = 0$, que é portanto a única maneira de satisfazer a equação 2.1. ◀

Exemplo 2.8. As matrizes A, B e C a seguir formam um conjunto L.I.

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix} \quad C = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

No entanto, A, B, C acima junto com a matriz D abaixo formam um conjunto L.D., porque $D = (-1/7)B + C$, ou seja,

$$D = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}. \quad ◀$$

★ **Exemplo 2.9.** No espaço das funções contínuas complexas, e^{ix}, e^{-ix}, seno e cosseno são LD, porque as duas últimas podem ser escritas como combinações lineares das duas primeiras:

$$\cos\theta = \frac{1}{2}e^{i\theta} + \frac{1}{2}e^{-i\theta},$$
$$\sin\theta = -\frac{1}{2}ie^{i\theta} + \frac{1}{2}ie^{-i\theta}.$$

Note que especificamos o espaço das funções contínuas *complexas*, porque as funções e^{ix} e e^{-ix} são complexas ◀

Exemplo 2.10. No espaço $\mathbb{Z}_2^5$, os vetores 01101 e 11100 são linearmente independentes, porque nenhum é múltiplo de outro. Mas se tomarmos também o vetor 10001, obteremos o conjunto

$$\{01101, 11100, 10001\},$$

que é linearmente dependente, porque

$$1(01101) \oplus 1(11100) = 01101 \oplus 11100 = 10001. \quad ◀$$

Teorema 2.11. *Qualquer conjunto que contenha o vetor zero,* $\mathbf{0}$*, é linearmente dependente.*

Demonstração. Seja $A = \{\mathbf{0}, \mathbf{v}_1, \mathbf{v}_2, \ldots\}$. Então

$$\mathbf{0} = 1(\mathbf{0}) + 0(\mathbf{v}_1) + 0(\mathbf{v}_2), \ldots,$$

e como há uma combinação linear dos vetores com um coeficiente não-nulo resultando em zero, o conjunto é linearmente dependente. ■

2.2 Conjuntos geradores e bases

Um espaço vetorial, mesmo tendo infinitos elementos, pode ser descrito por uma quantidade finita deles.

Na leitura da definição a seguir deve-se ter em mente que uma combinação linear sempre é de uma quantidade finita de vetores, mesmo que estes sejam escolhidos de um conjunto infinito (ou seja, não consideramos somas infinitas da forma $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots$).

Definição 2.12 (Gerador)**.** Seja V um espaço vetorial e S um subconjunto não vazio de V. O conjunto de todas as combinações lineares[1] de vetores de S é denotado por $[S]$. Dizemos que S *gera* $[S]$. ♦

Exemplo 2.13. Considere $X = \{(1,2,0)^T, (2,1,0)^T\}$, subconjunto de $\mathbb{R}^3$. Então $[X]$ é o conjunto de todas as combinações lineares de $(1,2,0)^T$ e $(2,1,0)$. Este é exatamente o conjunto de vetores da forma $(x,y,0)$. ◀

Exemplo 2.14. O seguinte conjunto,

$$\left\{\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \quad \begin{pmatrix}0 & 0\\ 0 & -1\end{pmatrix}\right\},$$

gera as matrizes diagonais de ordem dois. Por exemplo, seja $A = \left(\begin{smallmatrix}a & 0\\ 0 & b\end{smallmatrix}\right)$. Esta matriz é uma combinação linear das duas matrizes acima:

$$A = a\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} - b\begin{pmatrix}0 & 0\\ 0 & -1\end{pmatrix}. \qquad ◀$$

Exemplo 2.15. O conjunto de polinômios $\{1, x^2, x^4\}$ gera os polinômios de grau zero, dois e quatro em x:

$$\begin{aligned}
a_0 &= a_0(1)\\
a_0 + a_1x^2 &= a_0(1) + a_1(x^2)\\
a_1x^2 &= a_1(x^2)\\
&\vdots\\
a_0 + a_1x^2 + a_2x^4 &= a_0(1) + a_1(x^2) + a_2(x^4)\\
&\vdots
\end{aligned}$$

O conjunto $\{1, x^2 + x^4, x^4\}$ também gera os mesmos polinômios:

$$\begin{aligned}
a_0 &= a_0(1)\\
a_0 + a_1x^2 &= a_0(1) + a_1(x^2 + x^4) - a_1(x^4)\\
a_1x^2 &= a_1(x^2 + x^4) - a_1(x^4)\\
&\vdots\\
a_0 + a_1x^2 + a_2x^4 &= a_0(1) + a_1(x^2 + x^4) + (a_2 - a_1)(x^4)\\
&\vdots
\end{aligned}$$ ◀

[1] O conceito de gerador na verdade é semelhante em espaços vetoriais e grupos (geradores de grupos são abordados brevemente na seção 1.6.1, página 35), embora os tenhamos apresentado de formas ligeiramente diferentes. Um subconjunto $S \subseteq A$ *gera* o conjunto A se podemos descrever A somente com elementos de S, combinados de alguma forma. Em grupos, "combinar" é usar a operação de grupo. Em espaços vetoriais, podemos "combinar" os elementos do conjunto S através de combinações lineares. O gerador descreve de maneira compacta o conjunto. Por exemplo, o conjunto $\{2,3\}$ gera o grupo formado pelos múltiplos de dois e de três, com a operação de multiplicação. Para outro exemplo, podemos exibir o conjunto $\{a, b\}$, que contém dois elementos, "a" e "b", e a operação de "concatenação". Os elementos do conjunto são as sequências de símbolos "a", "b", "aa", "bb", "ab", "ba", e todas as sequencias que se pode construir com "a" e "b".

Exemplo 2.16. O conjunto $\{f(x) = e^x, g(x) = \cos(x), h(x) = 1\}$ gera o conjunto de todas as funções da forma

$$j(x) = ae^x + b\cos(x) + c,$$

com $a, b, c \in \mathbb{R}$. ◀

★ **Exemplo 2.17.** O conjunto de sequências de bits

$$\{1000,\ 0110,\ 0001\}$$

gera as sequências de bits da forma $abbc$:

0000,1000
0001,0110
1001,1111 ◀

Teorema 2.18. *Se V é um espaço vetorial e S subconjunto não vazio de V, então $[S]$ é subespaço de V*

Demonstração. Sejam $S \subseteq V$,

Claramente zero pertence a $[S]$: basta escolher a combinação linear com todos os coeficientes iguais a zero e qualquer vetor de S.

Se $\mathbf{u}, \mathbf{v} \in [S]$, então existem $\mathbf{s_1}, \mathbf{s_2}, \ldots, \mathbf{s_k} \in S$ tais que

$$\mathbf{u} = a_1\mathbf{s_1} + a_2\mathbf{s_2} + \ldots + a_n\mathbf{s_k}$$
$$\mathbf{v} = b_1\mathbf{s_1} + b_2\mathbf{s_2} + \ldots + b_n\mathbf{s_k}.$$

A multipicação por escalar resulta em outro elemento de $[S]$:

$$k\mathbf{u} = ka_1\mathbf{s_1} + ka_2\mathbf{s_2} + \ldots + ka_n\mathbf{s_k}$$

A soma de $\mathbf{u}$ com $\mathbf{v}$ também:

$$\begin{aligned}\mathbf{u} + \mathbf{v} &= a_1\mathbf{s_1} + a_2\mathbf{s_2} + \ldots + a_n\mathbf{s_k} + b_1\mathbf{s_1} + b_2\mathbf{s_2} + \ldots + b_n\mathbf{s_k} \\ &= (a_1 + b_1)\mathbf{s_1} + (a_2 + b_2)\mathbf{s_2} + \ldots + (a_n + b_n)\mathbf{s_k}.\end{aligned}$$ ■

Exemplo 2.19. Considere o espaço vetorial $\mathbb{R}^4$, e seu subconjunto S formado pelos vetores da forma $(1, 2, 1, 0)^T$ e $(0, 1, 0, 0)^T$. O conjunto gerado por S conterá vetores da forma $(x, y, x, 0)^T$, e este conjunto é um espaço vetorial:

- $[S]$ é fechado para as operações de soma e multiplicação por escalar:
  - $(a, b, a, 0)^T + (x, y, x, 0)^T = (a + x, b + y, a + x, 0)^T$, que também pertence a $[S]$.
  - $k(x, y, x, 0)^T = (kx, ky, kx, 0)^T$, que pertence a $[S]$.
- As operações de soma de vetores e multiplicação por escalar são as mesmas que tínhamos em $\mathbb{R}^4$, portanto são associativas; a soma de vetores é comutativa; e vale a distributividade.
- O vetor zero é da forma $(x, y, x, 0)^T$, com $x = y = 0$.
- Dado um vetor $(x, y, x, 0)^T$, temos o vetor $(-x, -y, -x, 0)^T$, que também pertence a $[S]$. ◀

Teorema 2.20. *Sejam* S *e* U *subconjuntos não vazios de um espaço vetorial* V*. Então*

i) $S \subseteq [S]$.

ii) $[[S]] = [S]$.

iii) $S \subseteq U$ *implica em* $[S] \subseteq [U]$.

iv) $[V] = V$.

Demonstração. (i) Seja $\mathbf{x} \in S$. Então $1\mathbf{x} = \mathbf{x}$ é combinação linear de um elemento de S (o próprio $\mathbf{x}$).

(ii) ($[S] \subseteq [[S]]$) Segue diretamente de (i). ($[[S]] \subseteq [S]$) Se $\mathbf{x} \in [[S]]$, é combinação linear de vetores em $[S]$. Mas a combinação linear de vetores de $[S]$ também está em $[S]$.

(iv) ($[V] \subseteq V$) Seja $\mathbf{x} \in [V]$. Toda combinação linear de vetores de V deve estar em V também, porque é obtida usando soma de vetores e multiplicação por escalares, portanto $\mathbf{x} \in V$. ($V \subseteq [V]$) Segue diretamente de (i). ■

Do item (iv) deste teorema concluimos que se S é subespaço de V, então $[S] = S$.

Teorema 2.21. *Seja* B *um conjunto de* n *vetores L.I. de um espaço vetorial. O maior conjunto L.I. de vetores em* $[B]$ *tem tamanho igual a* n*.*

Demonstração. Seja Y um conjunto gerado por $B = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ (ou seja, $X = [B]$). Seja

$$X = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k\}$$

um conjunto L.I. de vetores de V. Todo vetor de Y pode ser escrito como combinação linear de elementos de B, portanto temos

$$\mathbf{x}_1 = a_1\mathbf{b}_1 + a_2\mathbf{b}_2, + \ldots + a_n\mathbf{b}_n.$$

Como $\mathbf{x}_1 \neq 0$ (porque X é L.I.), então existe algum $a_i\mathbf{b}_i$ na expressão acima com $a_i \neq 0$, e portanto $\mathbf{b}_i$ pode ser escrito como

$$\mathbf{b}_i = c_0\mathbf{x}_1 + c_1\mathbf{b}_1 + c_2\mathbf{b}_2, + \ldots + c_n\mathbf{b}_n.$$

Se removermos $\mathbf{b}_i$ de B, trocando-o por esta expressão, teremos outro conjunto B':

$$\begin{aligned} B' &= \{\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}, [c_0\mathbf{x}_1 + c_1\mathbf{b}_1 + c_2\mathbf{b}_2, + \ldots + c_n\mathbf{b}_n], \mathbf{b}_{i+1}, \ldots, \mathbf{b}_k\} \\ &= \{d_1\mathbf{b}_1, \ldots, d_{i-1}\mathbf{b}_{i-1}, c_0\mathbf{x}_1, d_{i+1}\mathbf{b}_{i+1}, \ldots, d_k\mathbf{b}_k\}. \end{aligned}$$

O conjunto B' também gera X, mas contém o vetor $c_0\mathbf{x}_1$ ao invés de $\mathbf{b}_i$.

Suponha agora que $k > n$. Esta operação (de trocar algum $\mathbf{b}_i$ por sua expressão como combinação de elementos de X) pode ser realizada n vezes, resultando em um conjunto contendo n múltiplos dos $\mathbf{x}_i$. Temos então que n vetores de X geram Y. Se geram Y, também podem ser usados para expressar os outros $\mathbf{x}_i$ restantes – o que contradiz o fato de X ser L.I. ■

Definição 2.22 (Base)**.** Seja V um espaço vetorial e B um subconjunto finito e não-vazio de V. Dizemos que B é uma *base* de V se:

- B é L.I.;
- $[B] = V$ (ou seja, todo vetor de V pode ser escrito como combinação linear de vetores de B, e B é o menor conjunto que permite escrever todos os vetores de V). ♦

Exemplo 2.23. Os vetores $\mathbf{e}_1 = (1,0,0)^T$, $\mathbf{e}_2 = (0,1,0)^T$, e $\mathbf{e}_3 = (0,0,1)^T$ são uma base para o espaço vetorial $\mathbb{R}^3$, já que (i) todos pertencem a $\mathbb{R}^3$ e (ii) todo vetor $(x,y,z)^T$ de $\mathbb{R}^3$ pode ser escrito como combinação linear de $\mathbf{e}_1$, $\mathbf{e}_2$ e $\mathbf{e}_3$:

$$x\mathbf{e}_1 + y\mathbf{e}_2 + z\mathbf{e}_3 = x(1,0,0)^T + y(0,1,0)^T + z(0,0,1)^T = (x,y,z)^T.$$

Outras bases para $\mathbb{R}^3$ são

$$\{(1,2,3)^T, (4,5,0)^T, (6,0,0)^T\}$$
$$\{(1,1,2)^T, (1,2,2)^T, (2,2,2)^T\}$$
$$\{(0,0,\pi)^T, (0,e,0)^T, (\sqrt{2},0,0)^T\}$$ ◀

Exemplo 2.24. Considere $\mathbb{C}$ como um espaço vetorial *sobre* $\mathbb{R}$ – ou seja, o corpo subjacente é o dos reais. Queremos gerar todos os complexos, que são da forma

$$a + bi,$$

e portanto precisamos de dois números na base. Como só os multiplicaremos por reais, precisamos de um real e um complexo:

$$B = \{1, i\}$$

Podemos desta forma gerar qualquer complexo como combinação linear de B, *com coeficientes reais* (porque o corpo subjacente é $\mathbb{R}$).

Se quisermos poder multiplicar por complexos, temos que mudar o corpo subjacente, e usar $\mathbb{C}$. Neste caso, só precisamos de um elemento na base:

$$B' = \{1 + i\},$$

Qualquer complexo pode ser escrito como múltiplo de $1+i$. Suponha que queiramos escrever $a+bi$ como múltiplo de $1+i$. Queremos x, y tais que $(x+yi)(1+i) = a+bi$. Multiplicando, temos

$$(x+yi)(1+i) = (x-y) + (x+y)i.$$

portanto precisamos de x e y tais que

$$a = x - y$$
$$b = x + y,$$

ou seja,

$$x = \frac{b+a}{2}$$
$$y = \frac{b-a}{2}.$$

De fato: considere o complexo $3-5i$. Temos neste caso $a = 3, b = 5$. Precisamos usar, portanto,

$$x = \frac{-5+3}{2} = -1$$
$$y = \frac{-5-3}{2} = -4,$$

e o número que queremos é $-1-4i$. Verificamos:

$$(-4-i)(1+i) = 3-5i.$$ ◀

Definição 2.25 (Base canônica para $\mathbb{R}^n$)**.** No espaço $\mathbb{R}^n$, denotamos por $\mathbf{e}_i$ o vetor coluna com todos os elementos iguais a zero[2], exceto o i-ésimo elemento, que é igual a um. Ou seja,

$$\begin{aligned}\mathbf{e}_1 &= (1,0,0,\ldots,0)^T\\ \mathbf{e}_2 &= (0,1,0,\ldots,0)^T\\ \mathbf{e}_3 &= (0,0,1,\ldots,0)^T\\ &\vdots\\ \mathbf{e}_n &= (0,0,0,\ldots,1)^T\end{aligned}$$

A *base canônica* para $\mathbb{R}^n$ é

$$\{\,\mathbf{e}_1,\mathbf{e}_2,\ldots,\mathbf{e}_n\,\}.$$ ♦

Exemplo 2.26. Para qualquer n inteiro maior que zero, há infinitas bases diferentes para $\mathbb{R}^n$. Por exemplo, os vetores

$$\begin{aligned}\mathbf{b}_1 &= (2,1,1,1,\ldots,1)^T\\ \mathbf{b}_2 &= (2,2,1,1,\ldots,1)^T\\ \mathbf{b}_3 &= (2,2,2,1,\ldots,1)^T\\ &\vdots\\ \mathbf{b}_n &= (2,2,2,,2\ldots,1)^T\end{aligned}$$

também formam uma base para $\mathbb{R}^n$, já que são n vetores LI, todos pertencentes a $\mathbb{R}^n$. ◀

Exemplo 2.27. O espaço $\mathbb{R}_n[x]$ de polinômios com grau $\leq n$ tem como base o conjunto

$$B = \{\,1,x,x^2,x^3,\ldots,x^n\,\}.$$

Esta não é a única base de $\mathbb{R}_n[x]$. Todo polinômio pode também ser escrito como combinação linear de

$$B' = \{\,x,x+1,2x^2,3x^3,\ldots,nx^n\,\}.$$

Por exemplo, o vetor (polinômio) $5x^2+x-3$ pode ser descrito facilmente usando a base B:

$$5x^2+x-3 = 5(x^2)+1(x)-3(1).$$

Para escrever este mesmo polinômio na base B', verificamos primeiro que precisamos da constante -3, e como o único elemento da base que nos dá constantes é "$x+1$", damos a ele o coeficiente -3. Temos então

$$-3x-3,$$

mas precisamos de x, e não $-3x$. Adicionamos então quatro vezes o polinômio x, que também está na base:

$$4(x)-3(x+1) = x-3.$$

Somamos agora 5 vezes x^2 e temos

$$5x^2+x-3 = \frac{5}{2}(2x^2)+4(x)-3(x+1).$$ ◀

[2]Os vetores da base canônica também são chamados de *vetores de Kronecker*. Em $\mathbb{R}^3$, $\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3$ são algumas vezes denotados por $\hat{\imath}$, $\hat{\jmath}$ e $\hat{k}$.

Exemplo 2.28. O espaço $\mathbb{R}[x]$ de todos os polinômios reais, com qualqer grau, não é finitamente gerado (não tem base finita). Uma base para este espaço é o conjunto $\{1, x, x^2, x^3, \dots\}$. ◀

Exemplo 2.29. O espaço das matrizes quadradas 2×2 com coeficientes reais tem como base o conjunto formado pelas quatro matrizes no conjunto B a seguir.

$$B = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Outras bases para este mesmo espaço são

$$B' = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \right\}$$

e

$$B'' = \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix}, \begin{pmatrix} \pi^2 & \pi^3 \\ \pi^5 & \pi^7 \end{pmatrix}, \begin{pmatrix} \sqrt{2} & \sqrt{3} \\ \sqrt{5} & \sqrt{7} \end{pmatrix} \right\}.$$

De maneira geral, o espaço das matrizes $m \times n$ terá uma base com mn matrizes. ◀

★ **Exemplo 2.30.** Como vimos no exemplo 1.38, o espaço vetorial formado pelas soluções da equação diferencial ordinária $y'' - y' = 0$ contém as funções da forma

$$y = ae^x - be^{-x}.$$

Estas funções são claramente combinações lineares de e^x com e^{-x}. Assim, a base do espaço é

$$B = \{f(x) = e^x, g(x) = e^{-x}\},$$

e o espaço tem dimensão dois. poderíamos também ter usado a base

$$B' = \{f(x) = e^x + e^{-x}, g(x) = e^x - e^{-x}\},$$

porque este conjunto também é LI e gera o mesmo espaço. ◀

Para definirmos dimensão precisamos determinar primeiro que as bases para um espaço vetorial tem todas o mesmo tamanho.

Teorema 2.31. *Se um espaço vetorial tem pelo menos uma base com um número finito de elementos, então todas as suas bases tem o mesmo tamanho.*

Demonstração. Seja V um espaço vetorial e B uma base de V com n elementos. Como $V = [B]$, então não pode haver mais que n vetores L.I. em V, e portanto não há base maior que B.

Se houvesse base B' menor que B com $m < n$ vetores, então teríamos $[B'] = V$, e geraríamos V com $m < n$ vetores, e B não poderia ser L.I. (portanto não poderia ser base). ■

O conceito de dimensão captura uma idéia simples: se, para expressar um vetor em um espaço, precisamos de n coordenadas, o espaço tem dimensão n (posto de outra forma, a dimensão é a quantidade de *graus de liberdade* que temos se quisermos escolher um vetor).

Definição 2.32 (Dimensão)**.** Um espaço vetorial tem dimensão finita se é o espaço trivial ou se tem pelo menos uma base com um número finito de elementos[3]. Em outros casos, o espaço tem dimensão infinita.

Se um espaço V tem dimensão finita, então sua *dimensão*, denotada $\dim V$, é o número de vetores em qualquer base de V.

O epaço vetorial trivial $\{\,\mathbf{0}\,\}$ tem, por definição, dimensão zero. ♦

Exemplo 2.33. O espaço $\mathbb{R}^3$ é gerado por bases com três vetores, portanto tem dimensão 3. De forma mais geral, o espaço $\mathbb{R}^n$ pode ser gerado pela base $\{\,\mathbf{e_1}, \ldots, \mathbf{e_n}\,\}$ com n vetores, portanto $\dim(\mathbb{R}^n) = n$. ◀

Exemplo 2.34. O espaço $\mathbb{R}_n[x]$ dos polinômios com grau $\leq n$ é gerado pela base

$$\left\{\, 1, x, x^2, \ldots, x^n \,\right\},$$

que tem $n + 1$ vetores, e portanto $\dim(\mathbb{R}_n[x] = n + 1)$. ◀

O próximo exemplo mostra que se mudarmos o corpo subjacente podemos mudar a dimensão de um espaço vetorial.

Exemplo 2.35. O conjunto de polinômios $\{1, x, x^2, x^3, \ldots\}$ é linearmente independente e suas combinações lineares são os polinômios com coeficientes reais. Embora este conjunto seja de fato uma base para os polinômios em $\mathbb{R}$, não trataremos deste caso, porque o conjunto é infinito. Dizemos que a dimensão do espaço de todos os polinômios em $\mathbb{R}$ é infinita ($\dim \mathbb{R}_n[x] = \infty$). ◀

Exemplo 2.36. O espaço F de todas as funções $f : \mathbb{R} \to \mathbb{R}$ não é gerado por qualquer base finita, portanto tem dimensão infinita. Para verificar, basta observar que cada polinômio determina uma função, e como $\dim \mathbb{R}_n[x] = \infty$, necessariamente $\dim F = \infty$, porque uma base para F deve conter uma base para $\mathbb{R}_n[x]$. ◀

Exemplo 2.37. No exemplo 2.24, mostramos que se quisermos tratar $\mathbb{C}$ como um espaço vetorial *sobre os reais* – ou seja, somamos complexos mas só os multiplicamos por reais – então o espaço poderia ter como base

$$B = \{1, i\},$$

e portanto sua dimensão é dois.

No entanto, se quisermos tratar $\mathbb{C}$ como um espaço vetorial sobre $\mathbb{C}$ – ou seja, se quisermos poder somar *e multiplicar* complexos entre si, podemos usar como base

$$B' = \{1 + i\},$$

e passamos a ter um espaço de dimensão um. ◀

★ **Exemplo 2.38.** Damos como exemplo agora outro espaço de dimensão infinita – o espaço das funções racionais, que definimos a seguir.

Definição 2.39. Uma *função racional* $f(x)$ é a razão de dois polinômios:

$$f(x) = \frac{p(x)}{q(x)},$$

sendo $q(x)$ diferente do polinômio nulo. ♦

[3] É possível generalizar a noção de base, permitindo uma quantidade infinita de elementos, e resultando em espaços vetoriais de dimensão infinita. A descrição das bases para alguns destes espaços vetoriais envolve dificuldades conceituais, e ao longo deste texto os abordaremos em poucos exemplos. O Capítulo 14 trata mais extensivamente de alguns espaços de funções com dimensão infinita.

O conjunto de todas as funções racionais é um espaço vetorial:

i) Este conjunto está contido no conjunto de todas as funções reais, que sabemos ser um espaço vetorial;

ii) A função zero está neste conjunto, com $p(x) = 0$ e $q(x) = 1$;

iii) Tanto a soma de duas funções racionais como a multiplicação de uma função racional por escalar resultam em outra função racional.

Este espaço vetorial tem dimensão infinita. O conjunto

$$\left\{ x^j,\ \frac{1}{(x-a)^{j+1}},\ \frac{1}{(x^2+bx+c)^{j+1}},\ \frac{x}{(x^2+bx+c)^{j+1}}\ :\ j \in \mathbb{N}, a, b, c \in \mathbb{R}, b^2 < 4c \right\}$$

que tem infinitos elementos, é LI e constitui uma base para o espaço vetorial das funções racionais reais. Não demonstraremos aqui estes dois fatos. ◀

Teorema 2.40. *Em um espaço V de dimensão n, qualquer conjunto com n vetores L.I. é uma base.*

Demonstração. Para ser uma base precisamos que o conjunto seja L.I. e que gere o espaço vetorial. Como já temos um conjunto L.I., basta mostrar que os n vetores geram o espaço.

Sejam V um espaço vetorial de dimensão n, e $X = \{ \mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n \}$ um conjunto L.I. de vetores de V.

Mostraremos agora como escrever qualquer vetor $\mathbf{v}$ como combinação linear de elementos de X.

Se adicionarmos um novo vetor a X teremos um conjunto L.D. (porque teremos mais que n vetores). Assim, ao adicionarmos $\mathbf{v} \neq \mathbf{0}$, existem a_i e b tais que

$$a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \ldots + a_n\mathbf{x}_n + b\mathbf{v} = \mathbf{0}$$

mas b deve ser diferente de zero porque X é L.I., e se b fosse zero, teríamos a combinação $a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \ldots + a_n\mathbf{x}_n = \mathbf{0}$, com algum $a_i \neq 0$. Então,

$$\mathbf{v} = \frac{1}{b}\left(-a_1\mathbf{x}_1 - a_2\mathbf{x}_2 - \ldots - a_n\mathbf{x}_n\right). \qquad \blacksquare$$

O próximo teorema nos garante que podemos, a partir de qualquer conjunto L.I., *completar uma base* para um espaço vetorial – algo que faremos em algumas demonstrações mais adiante.

Teorema 2.41. *Seja U um subconjunto linearmente independente de um espaço V de dimensão finita. Se U não gera V, podemos adicionar vetores a U de forma a obter uma base para V.*

Demonstração. Se U não gera V, então existe pelo menos um vetor $\mathbf{v} \in V$ que não pode ser escrito como combinação linear de vetores de U. Adicionamos $\mathbf{v}$ a U, obtendo um novo conjunto de vetores L.I. Repetimos este processo até obter um conjunto que gere V. Tal conjunto será obtido com no máximo n vetores, onde n é a dimensão de V, porque de outra forma teríamos $n + 1$ vetores L.I. em um espaço de dimensão n. ■

Exemplo 2.42. O conjunto

$$X = \{(0,0,1)^T, (0,2,2)^T\}$$

tem dois vetores LI, mas não gera o espaço $\mathbb{R}^3$ (este conjunto só pode gerar vetores com a primeira coordenada igual a zero). podemos completar este conjunto com mais um vetor, obtendo uma base:

$$X' = \{(0,0,1)^T, (0,2,2)^T, (3,3,3)^T\}. \qquad \blacktriangleleft$$

Os próximos teoremas relacionam as dimensões de subespaços somados com a dimensão da soma deles.

Teorema 2.43. *Seja* V *um espaço com dimensão finita, tal que* $V = U \oplus W$*. Então*

$$\dim(U \oplus W) = \dim(U) + \dim(W).$$

Demonstração. Seja n a dimensão de V. Podemos construir uma base para U da seguinte maneira: escolhemos qualquer vetor $\mathbf{u}_1 \in U$ que seja diferente de zero e o incluímos em B. Depois, adicionamos outros vetores de U ao conjunto B, desde que ele continue L.I. Como $U \subseteq V$, haverá no máximo n vetores, portanto B é finito. Como B é o maior subconjunto L.I de U, é base de U.

Suponha que o número de vetores em B seja k. Se $k < n$, podemos adicionar mais vetores de W até formar uma base para V. Seja B' o conjunto destes vetores usados para complementar B. Então $[B'] = W$, e $[B \cup B'] = V$. Já há k vetores em B, portanto W deve ter $n - k$ vetores, porque uma base para V precisa de exatamente n vetores.

Temos então que

$$\dim(U) + \dim(W) = k + (n - k) = n = \dim(V). \qquad \blacksquare$$

Proposição 2.44. *Todo subespaço* U *de um espaço* V *de dimensão finita tem um* complemento *em* V*: este complemento é um outro subespaço* W *tal que* $V = U \oplus W$*.*

Demonstração. A proposição é provada implicitamente na demonstração do teorema 2.43. $\blacksquare$

Note que "complemento" não necessariamente significa complemento de conjuntos; também não é necessário que o complemento seja único, como podemos verificar no exemplo a seguir.

Exemplo 2.45. Seja A o subespaço de $\mathbb{R}^2$ formado pelos vetores (x, y) com $x + y = 0$ (ou seja, a reta $y = -x$ passando pela origem).

A dimensão de A é 1, porque A é gerado por $(1, -1)$.

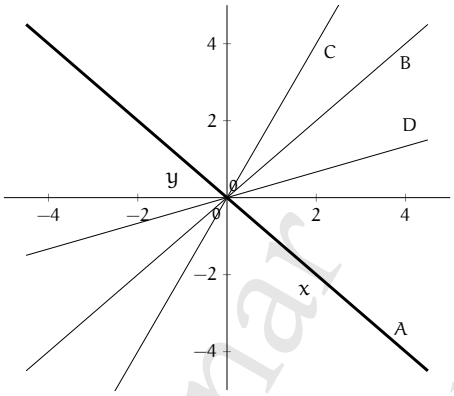
O subespaço $B = \{ (x, y) : \ x - y = 0 \}$ é complemento de A, e $\mathbb{R}^2 = A \oplus B$. A dimensão de B é 1, porque é gerado por $(1, 1)$

Mas o subespaço $C = \{ (x, y) : 2x - y = 0 \}$ também é complemento de A, e $\mathbb{R}^2 = A \oplus C$. A dimensão de C é 1, porque é gerado por $(1, 2)$.

Temos portanto

$$\begin{aligned} \dim(A) + \dim(B) &= 2 = \dim(\mathbb{R}^2) \\ \dim(A) + \dim(C) &= 2 = \dim(\mathbb{R}^2). \end{aligned}$$

Quaisquer duas retas diferentes passando pela origem podem gerar $\mathbb{R}^2$, portanto uma reta tem, em $\mathbb{R}^2$, infinitos complementos. A figura a seguir mostra o subespaço A (a reta $y = -x$) e dois dos seus infinitos complementos: o subespaço B (a reta $y = x$); o outro subespaço C (a reta $y = 2x$); e um outro subespaço, D (a reta $y = x/3$).



Com os vetores da reta A e os vetores de *uma* das outras retas diferentes de A, podemos gerar todos os vetores em $\mathbb{R}^2$. ◀

Exemplo 2.46. Sabemos que $\mathbb{R}_4[x] = \mathbb{R}_2[x] \oplus \mathbb{R}_{3..4}[x]$. Uma base para $\mathbb{R}_2[x]$ é

$$\{\, 1, x, x^2 \,\}$$

e portanto sua dimensão é 3. Uma base para $\mathbb{R}_{3..4}[x]$ é

$$\{\, x^3, x^4 \,\}$$

e portanto $\dim(\mathbb{R}_{3..4}[x]) = 2$.

A dimensão de $\mathbb{R}_4[x]$ deve portanto ser 5. E realmente uma possível base para $\mathbb{R}_4[x]$ é a união das bases dos subespaços que acabamos de mostrar:

$$\{\, 1, x, x^2, x^3, x^4 \,\}.$$

Concluímos portanto que $\dim(\mathbb{R}_4[x]) = 5$.

Observamos também que o complemento de $\mathbb{R}_2[x]$ é $\mathbb{R}_{3..4}[x]$, também subespaço de $\mathbb{R}_4[x]$, conforme a proposição 2.44. ◀

Exemplo 2.47. Seja $\mathcal{F}$ o espaço de funções reais, e K o espaço de funções constantes. Seja N o conjunto

$$N = \{\mathbf{0}\} \cup \mathcal{F} \setminus K,$$

ou seja, N contém todas as funções não constantes e também a função zero. *Embora* N *seja o complemento de* K *na linguagem de conjuntos (*$N = K^C$*, ou* $N = \overline{K}$*), ele não é complemento do espaço vetorial* K.

Para verificar isto, mostramos que N não pode ser espaço vetorial, porque a soma em N não é fechada. De fato, podemos somar duas funções não constantes resultando em uma função constante: seja a função constante $h(x) = k$. Construímos duas funções

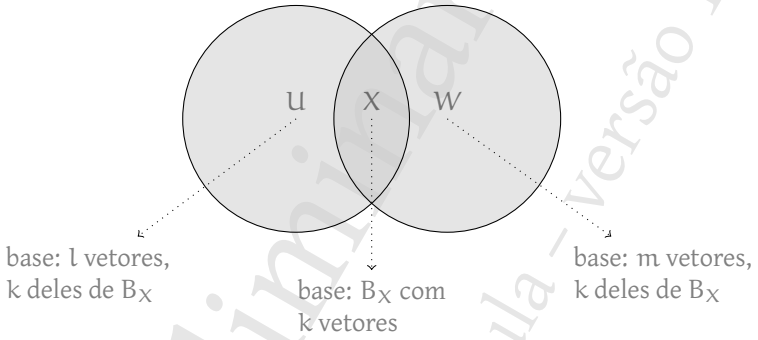
$$f(x) = x + k$$
$$g(x) = -x$$

e temos $(f + g) = h$: a soma de duas funções, uma crescente e uma decrescente, iguais a uma função constante. Assim, a soma não é fechada em N, logo N não é espaço vetorial, e por isso não pode ser complemento de um subespaço. ◀

Teorema 2.48. *Seja V um espaço com dimensão finita igual a n, tal que $V = U + W$. Então*

$$\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W).$$

Demonstração. Seja $X = U \cap W$. Argumentamos que a base de X, com k vetores, pode ser usada como parte das bases de U e W, com $l > k$ e $m > k$ vetores. Assim, ao construir bases para U e W, observamos que $B_X \subseteq B_U$ e $B_X \subseteq W$, e portanto devemos contabilizar os vetores de B_U e B_W descontando o tamanho de B_X, que é subconjunto de ambos.



Mais detalhadamente: sabemos que X é subespaço de V, e podemos construir uma base para X, com vetores

$$B_X = \{ \mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k \},$$

sendo k a dimensão de X. Como $X \subseteq U$, podemos também completar esta base para obter uma base de U com os vetores

$$B_U = \{ \mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{u}_{k+1}, \ldots, \mathbf{u}_l \},$$

onde l é a dimensão de U. Também podemos da mesma forma completar a base de X para ober uma base de W:

$$B_W = \{ \mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{w}_{k+1}, \ldots, \mathbf{w}_m \},$$

onde m é a dimensão de W.

Se um vetor $\mathbf{a}$ pertence a $U + W$, pode ser descrito (não necessariamente de maneira única) como a soma de um vetor de U e um de W ($\mathbf{a} = \mathbf{u} + \mathbf{w}$). Mas $\mathbf{u}$ e $\mathbf{w}$ são combinações lineares de vetores das bases de U e W:

$$\begin{aligned}
\mathbf{a} = {} & \alpha_1\mathbf{x}_1 + \alpha_2\mathbf{x}_2 + \ldots + \alpha_k\mathbf{x}_k + \alpha_{k+1}\mathbf{u}_{k+1} + \ldots + \alpha_l\mathbf{u}_l && \text{(este é } \mathbf{u}\text{)} \\
& + \beta_1\mathbf{x}_1 + \beta_2\mathbf{x}_2 + \ldots + \beta_k\mathbf{x}_k + \beta_{k+1}\mathbf{w}_{k+1} + \ldots + \beta_m\mathbf{w}_m && \text{(este é } \mathbf{w}\text{)} \\
& = (\alpha_1 + \beta_1)\mathbf{x}_1 + (\alpha_2 + \beta_2)\mathbf{x}_2 + \ldots + (\alpha_k + \beta_k)\mathbf{x}_k \\
& + \alpha_{k+1}\mathbf{u}_{k+1} + \ldots + \alpha_l\mathbf{u}_l + \beta_{k+1}\mathbf{w}_{k+1} + \ldots + \beta_m\mathbf{w}_m.
\end{aligned}$$

Este conjunto,

$$B = \{ \mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{u}_{k+1}, \ldots \mathbf{u}_l, \mathbf{w}_{k+1}, \ldots, \mathbf{w}_m \}$$

portanto gera V, e tem $l + m - k$ vetores. Para mostrar que B é uma base de V, falta mostrarmos que B é L.I.

Se B fosse L.D., poderíamos encontrar coeficientes $\alpha_i, \beta_i, \gamma_i$, *não todos zero*, tais que

$$\alpha_1\mathbf{x}_1 + \ldots + \alpha_k\mathbf{x}_k, + \beta_{k+1}\mathbf{u}_{k+1} + \ldots + \beta_l\mathbf{u}_l + \gamma_{k+1}\mathbf{w}_{k+1} + \ldots + \gamma_m\mathbf{w}_m = 0. \tag{2.3}$$

Suponha que algum $\alpha_i \neq 0$. Teríamos então

$$\alpha_1 \mathbf{x}_1 + \ldots + \alpha_i \mathbf{x}_i + \ldots + \alpha_k \mathbf{x}_k = 0,$$

o que não é possível, já que estes vetores são base de X (e portanto L.I.) Como os α_i são zero, temos que supor em seguida que algum β_i é diferente de zero. Mas então teríamos

$$\alpha_1 \mathbf{x}_1 + \ldots + \alpha_k \mathbf{x}_k + \beta_{k+1} \mathbf{u}_{k+1} + \ldots + \beta_i \mathbf{u}_i + \ldots + \beta_l \mathbf{u}_l = 0,$$

o que também não é possível, porque

$$\{ \mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{u}_{k+1}, \ldots, \mathbf{u}_l \}$$

é base para U, e portanto é L.I.

Repetimos o raciocínio para os γ_i, e concluímos que para que a expressão (2.3) valha, todos os coeficientes devem ser zero, e o conjunto B é L.I.

Provamos que B é base para $U + W$, e tem $l + m - k$ vetores. Assim,

$$\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W). \qquad \blacksquare$$

Observe que na demonstração de Teorema 2.48, começamos construindo uma base B_X para a interseção $U \cap W$ justamente para poder construir as outras duas bases B_U e B_W tendo B_X como interseção.

Exemplo 2.49. Sejam $A = \{ (0, w, x, y, z) : \ w, x, y, z \in \mathbb{R} \}$ e $B = \{ (a, 0, b, c, 0) : \ a, b, c \in \mathbb{R} \}$ subespaços de $\mathbb{R}^5$. O espaço A contém todos os vetores onde a primeira coordenada é zero; o espaço B tem os vetores onde a segunda e a quinta coordenada são zero. Temos claramente que

$$A + B = \mathbb{R}^5.$$

Agora calculamos as dimensões destes espaços. Uma base para A poderia ser

$$\begin{aligned} B_A &= \left\{ (0,1,0,0,0)^T, (0,0,1,0,0)^T, (0,0,0,1,0)^T, (0,0,0,0,1)^T \right\} \\ &= \{ \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4, \mathbf{e}_5 \} \end{aligned}$$

e portanto $\dim(A) = 4$. Uma base para B tem três vetores:

$$B_B = \{ \mathbf{e}_1, \mathbf{e}_3, \mathbf{e}_4 \},$$

e $\dim(B) = 3$.

A soma das dimensões de A e B é sete – diferente da dimensão de $\mathbb{R}^5$. Calculamos então a dimensão de $A \cap B$.

Como $A \cap B$ contém vetores que estão em A e também em B, então

$$A \cap B = \left\{ (0,0,d,e,0)^T : \ d, e \in \mathbb{R} \right\}$$

contém vetores com as coordenadas 1, 2 e 5 iguais a zero. Este espaço pode ser gerado pela base

$$B_{AB} = \{ \mathbf{e}_3, \mathbf{e}_4 \},$$

e tem portanto dimensão 2.

Verificamos então que

$$\begin{aligned} \dim(A + B) &= \dim(A) + \dim(B) - \dim(A \cap B) \\ 5 &= 4 + 3 - 2. \end{aligned}$$

◀

2.3 Isomorfismo e coordenadas

Nesta seção mostramos que os espaços que estudamos são aparentemente diferentes, mas na verdade são tão semelhantes aos espaços da família $\mathbb{R}^n$ que é possível restringir nossa discussão somente a estes últimos.

Definição 2.50 (Isomorfismo)**.** Sejam V e U dois espaços vetoriais. Um *isomorfismo* entre V e U é uma bijeção $f : V \to U$ tal que, para todos vetores $\mathbf{v}, \mathbf{w} \in V$ e todo escalar c,

- $f(\mathbf{v} + \mathbf{w}) = f(\mathbf{v}) + f(\mathbf{w})$
- $f(c\mathbf{v}) = cf(\mathbf{v})$.

Neste caso dizemos que V e U são *isomorfos*. ♦

Exemplo 2.51. O espaço $\mathbb{R}_2[x]$ é isomorfo a $\mathbb{R}^3$.

Seja f a bijeção que associa polinômios $a_0 + a_1x + a_2x^2$ ao vetor $(a_0, a_1, a_2)^T$ em $\mathbb{R}^3$ – ou seja,

$$f(a_0 + a_1x + a_2x^2) = (a_0, a_1, a_2)^T.$$

Mostramos agora que f é um isomorfismo. Sejam $\mathbf{u} = u_0 + u_1x + u_2x^2$ e $\mathbf{v} = v_0 + v_1x + v_2x^2$. Primeiro, verificamos a soma:

$$\begin{aligned} f(\mathbf{u} + \mathbf{v}) &= f\left(u_0 + u_1x + u_2x^2 + v_0 + v_1x + v_2x^2\right) \\ &= f\left(u_0 + v_0 + (u_1 + v_1)x + (u_2 + v_2)x^2\right) \\ &= (u_0 + v_0, u_1 + v_1, u_2 + v_2) \\ &= (u_0, u_1, u_2) + (v_0, v_1, v_2) \\ &= f(\mathbf{u}) + f(\mathbf{v}). \end{aligned}$$

Agora a multiplicação por escalar:

$$\begin{aligned} f(c\mathbf{v}) &= f\left(c(v_0 + v_1x + v_2x^2)\right) \\ &= cv_0 + cv_1x + cv_2x^2 \\ &= (cv_0, cv_1, cv_2) \\ &= c(v_0, v_1, v_2) \\ &= cf(v_0 + v_1x + v_2x^2) \\ &= cf(\mathbf{v}). \end{aligned}$$

Assim, f é isomorfismo, e o espaço dos polinômios de grau máximo 2 é isomorfo a $\mathbb{R}^3$.

De forma mais geral, o espaço de polinômios $\mathbb{R}_n[x]$ é isomorfo a $\mathbb{R}^{n+1}$. ◄

Exemplo 2.52. Considere $M_{2,2}$, o espaço das matrizes 2×2. Definimos a seguinte bijeção entre $M_{2,2}$ e $\mathbb{R}^4$:

$$f\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] = (a, b, c, d)^T.$$

Esta bijeção é um isomorfismo: sejam duas matrizes

$$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ e } \mathbf{X} = \begin{pmatrix} w & x \\ y & z \end{pmatrix}.$$

Então

$$\begin{aligned} f(\mathbf{A}+\mathbf{X}) &= f\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} w & x \\ y & z \end{pmatrix}\right] = f\left[\begin{pmatrix} a+w & b+x \\ c+y & d+z \end{pmatrix}\right] \\ &= (a+w, b+x, c+y, d+z)^T = (a,b,c,d)^T + (w,x,y,z)^T \\ &= f\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] + f\left[\begin{pmatrix} w & x \\ y & z \end{pmatrix}\right] = f(\mathbf{A}) + f(\mathbf{X}), \end{aligned}$$

e

$$\begin{aligned} f(k\mathbf{A}) &= f\left[k\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] = f\left[\begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix}\right] \\ &= (ka, kb, kc, kd)^T = k(a,b,c,d)^T \\ &= kf\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] = kf(\mathbf{A}). \end{aligned}$$

O espaço vetorial $M_{m,n}$ será sempre isomorfo a $\mathbb{R}^{mn}$. ◀

Exemplo 2.53. Sabemos que o espaço vetorial das soluções da EDO $y'' - y = 0$ contém funções da forma

$$f(x) = ae^x - be^{-x}.$$

Podemos identificar cada uma destas soluções com um vetor em $\mathbb{R}^2$ através da bijeção

$$g(ae^x - be^{-x}) = (a,b)^T.$$

Verificamos agora que esta bijeção preserva linearidade.

Começamos com a multiplicação por escalar: dado $k \in \mathbb{R}$ e uma solução $ae^x - be^{-x}$,

$$\begin{aligned} g\left[k\left(ae^x - be^{-x}\right)\right] &= g(kae^x - kbe^{-x}) \\ &= (ka, kb)^T \\ &= k(a,b)^T \\ &= kg(ae^x - be^{-x}). \end{aligned}$$

Agora verificamos a soma: dadas duas soluções $ae^x - be^{-x}$ e $\alpha e^x - \beta e^{-x}$,

$$\begin{aligned} g\left[\left(ae^x - be^{-x}\right) + \left(\alpha e^x - \beta e^{-x}\right)\right] &= g\left[(a+\alpha)e^x - (b+\beta)e^{-x}\right] \\ &= (a+\alpha, b+\beta)^T \\ &= (a,b)^T + (\alpha,\beta)^T \\ &= g(ae^x - be^{-x}) + g(\alpha e^x - \beta e^{-x}). \end{aligned}$$

concluímos portanto que g é isomorfismo. ◀

Exemplo 2.54. Considere o sistema

$$\begin{cases} \frac{w}{2} + x \quad - z = 0 \\ \qquad \frac{y}{2} - z = 0, \end{cases}$$

que também pode ser escrito na forma $A\mathbf{x} = \mathbf{0}$, com

$$A = \begin{pmatrix} 1/2 & 1 & 0 & -1 \\ 0 & 0 & 1/2 & -1 \end{pmatrix}.$$

As soluções para este sistema são da forma $(w, x, y, z)^T$, com

$$x = z - \frac{w}{2},$$
$$y = 2z$$

ou seja, uma solução $\mathbf{s}$ é

$$\mathbf{s} = \begin{pmatrix} w \\ z - w/2 \\ 2z \\ z \end{pmatrix}$$

formando um espaço vetorial[4] Temos o seguinte isomorfismo com $\mathbb{R}^2$:

$$g(w, x, y, z)^T = (w, z)^T,$$

já que tanto x como y dependem de w e z.

A demonstração de que g é isomorfismo é pedida no Exercício 54 ◀

Os exemplos anteriores mostram que diversos espaços vetoriais de dimensão finita são isomorfos a $\mathbb{R}^n$. De fato, *todo* espaço vetorial de dimensão finita n é isomorfo a $\mathbb{R}^n$.

Definimos a base de um espaço vetorial como um *conjunto* de vetores, mas em um conjunto não há ordem dfinida para os elementos. Para poder desenvolver o conceito de coordenadas precisaremos identificar a posição de cada elemento na base, por isso definimos *base ordenada* a seguir.

Definição 2.55 (Base ordenada)**.** Seja $B = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ uma base para um espaço vetorial V de dimensão finita. Então a tupla

$$B = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n).$$

é uma *base ordenada* para V. ⧫

Sabemos que é possível descrever qualquer elemento do espaço como combinação linear dos elementos da base,

$$\mathbf{v} = \{a_1\mathbf{b_1} + \cdots + a_n\mathbf{b_n}.\}$$

Como os vetores de uma base ordenada tem posição definida, podemos simplesmente listar os coeficientes $a_1, \ldots, a_n$ para descrever o vetor. Estas são suas *coordenadas* naquela base.

A definição a seguir mostra que todos os espaços de dimensão finita (sejam eles de polinômios, matrizes, funções, ou quaisquer outros objetos) podem ser tratados da mesma forma: ao invés de trabalhar diretamente com esses objetos, trabalhamos com *coordenadas*.

[4] O espaço formado por estas soluções tem dimensão dois (há duas variáveis a escolher), com base

$$B = \left\{ \begin{pmatrix} 0 \\ 1 \\ 2 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -1/2 \\ 0 \\ 0 \end{pmatrix} \right\}.$$

Informalmente, o primeiro vetor nos diz se damos um valor a z, devemos somá-lo também a x, e seu dobro a y. De acordo com o segundo vetor, quando damos um valor a w, devemos subtrair metade dele de x. Observe novamente a fora geral da solução e veja que é exatamente desta forma que x e y podem ser descritas como dependentes de w e z.

Definição 2.56 (Coordenadas em uma base)**.** Seja V um espaço vetorial com base ordenada B. Então um vetor qualquer de V pode ser escrito como $\mathbf{v} = a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \ldots + a_n\mathbf{b}_n$. Os coeficientes $a_1, a_2, \ldots, a_n$ são as *coordenadas* de $\mathbf{v}$ na base B. Denotamos $[\mathbf{v}]_B = (a_1, a_2, \ldots, a_n)^T$, onde a ordem dos coeficientes é a mesma dos vetores $\mathbf{b}_i$ na base B. ♦

Exemplo 2.57. Seja $B = \left(1, x, x^2, x^3\right)$ uma base para $\mathbb{R}_3[x]$. Então

$$p(x) = x^2 - x + 2 = 2(1) - 1(x) + 1(x^2) + 0(x^3),$$

e as coordenadas de $p(x)$ nesta base são

$$[p(x)]_B = (2, -1, 1, 0)^T.$$

Se escolhermos uma base diferente para $\mathbb{R}_3[x]$ – por exemplo,

$$B' = \left\{ 1, 1 + x, 1 + x + x^2, 1 + x + x^2 + x^3 \right\},$$

descrevemos $p(x)$ usando a base B' como

$$p(x) = 3(1) - 2(x + 1) + 1(x^2 + x + 1) + 0(x^3 + x^2 + x + 1),$$

e portanto as coordenadas de $p(x)$ na base B' são

$$[p(x)]_{B'} = (3, -2, 1, 0)^T.$$ ◀

Observe que $[.]_{B'}$ é uma bijeção entre polinômios de $\mathbb{R}_3[x]$ e vetores de $\mathbb{R}^4$ – ou seja, é um isomorfismo.

A escolha de bases diferentes para um espaço vetorial implica na escolha de isomorfismos diferentes com $\mathbb{R}^n$.

Proposição 2.58. *Seja V um espaço vetorial de dimensão finita, e sejam α e β diferentes bases para V. Os isomorfismos entre V e $\mathbb{R}^n$ dados por $f(\mathbf{x}) = [\mathbf{x}]_\alpha$ e $g(\mathbf{x}) = [\mathbf{x}]_\beta$ são diferentes, ou seja, existe $\mathbf{x}$ tal que $f(\mathbf{x}) \neq g(\mathbf{x})$.*

Demonstração. Sejam $\alpha \neq \beta$ bases para um espaço vetorial V. para todo $\mathbf{x} \in V$, existem $a_1, \ldots, a_n$ e $b_1, \ldots, b_n$ tais que

$$[\mathbf{x}]_\alpha = (a_1, a_2, \ldots, a_n)$$
$$[\mathbf{x}]_\beta = (b_1, b_2, \ldots, b_n)$$

Suponha, por hipótese, que $[\mathbf{x}]_\alpha = [\mathbf{x}]_\beta$ para todo $\mathbf{x} \in V$. Então sempre teremos $a_i = b_i$.

Tome o vetor $\mathbf{x} = \alpha_1$. Sua representação na base α é $(1, 0, \ldots, 0)$. Como dissemos que os isomorfismos são iguais, sua representação na base β deve também ser $(1, 0, \ldots, 0)$, e concluímos que $\alpha_1 = \beta_1$. O mesmo vale para todos os outros pares α_i, β_i nas bases α e β – ou seja, as bases devem ser iguais. Como havíamos presumido que as bases são diferentes, chegamos a um absurdo, e devemos negar a hipótese que fizemos ($[\mathbf{x}]_\alpha = [\mathbf{x}]_\beta$ para todo $\mathbf{x} \in V$). ■

Teorema 2.59. *Dois espaços vetoriais de dimensão finita U e V são isomorfos se tem a mesma dimensão.*

Demonstração. Sejam U e V espaços vetoriais com dimensão n (finita). A bijeção

$$f(\mathbf{v}) = [\mathbf{v}]_B,$$

onde B é alguma base de V, mostra que V e $\mathbb{R}^n$ são isomorfos.

Como U, pelo mesmo argumento, deve ser isomorfo a $\mathbb{R}^n$, U e V são isomorfos. ■

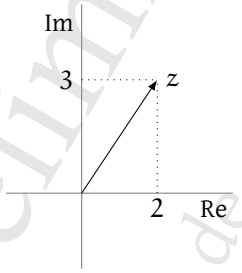
Exemplo 2.60. Um exemplo particularmente importante é o espaço $\mathbb{C}$, onde os vetores são números complexos e o corpo subjacente é $\mathbb{R}$. Claramente, uma base para $\mathbb{C}$ é

$$B = \{1, i\},$$

já que qualquer complexo pode ser escrito como $a + bi$, onde $a, b \in \mathbb{R}$. Como este espaço é sobre o corpo dos reais e tem dimensão dois, ele é isomorfo a $\mathbb{R}^2$. A bijeção é

$$f(a + bi) = (a, b)^T.$$

Assim, associamos a cada número complexo um ponto em $\mathbb{R}^2$. Quando interpretamos $\mathbb{R}^2$ como o conjunto dos complexos, o chamamos de "*plano complexo*", onde o eixo das abscissas representa a parte real de cada número, e o eixo das ordenadas representa a parte imaginária. A figura a seguir mostra a representação do número complexo $z = 2 + 3i$ no plano complexo.



Como se tata de isomorfismo, a soma de complexos é representada no plano pela soma usual de vetores em $\mathbb{R}^2$. Também a multiplicação de complexo por escalar é representada no plano como a multiplicação de vetor por escalar.

É comum adotar a noção de *norma* de vetores em $\mathbb{R}^2$ para números complexos, de forma que a norma de um complexo é

$$|a + bi| = \sqrt{a^2 + b^2}.$$ ◀

Exemplo 2.61. Tanto $\mathbb{R}_3[x]$ como $M_{2\times 2}$ tem dimensão 4. Mostramos agora o isomorfismo entre eles.

Primeiro, $f : \mathbb{R}_3[x] \to \mathbb{R}^4$:

Usaremos para $\mathbb{R}_3[x]$ uma base

$$B = \left(1, x, x^2, x^3\right).$$

Em $M_{2\times 2}$, usaremos a base

$$C = \left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\right).$$

Definimos agora duas bijeções:

$$f(p(x)) = [p(x)]_B$$
$$g(A) = [A]_C$$

Por exemplo, considere $p(x) = x^2 - 1$.

$$f(x^2 - 1) = [x^2 - 1]_B = (-1, 0, 1, 0)^T.$$

Levamos o vetor $p(x)$ de $\mathbb{R}_3[x]$ em $\mathbb{R}^4$. Agora, podemos usar a bijeção g para levar de $\mathbb{R}^4$ em $M_{2\times 2}$:

$$g\left[(-1,0,1,0)^T\right] = \left[(-1,0,1,0)^T\right]_C = \begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix}.$$

A composição das bijeções f e g também é uma bijeção – e portanto temos um isomorfismo entre $\mathbb{R}_3[x]$ e $M_{2\times 2}$.

Agora observamos o que acontece se mudarmos a base de um dos espaços vetoriais. Usaremos para $\mathbb{R}_3[x]$ a base B', diferente de B:

$$B' = \left(x, x+1, x^2+1, x^3\right).$$

Como temos uma nova base, temos também uma nova bijeção,

$$f'(p(x)) = [p(x)]_{B'}$$

Novamente, usamos o isomorfismo para levar o polinômio x^2-1 em $M_{2\times 2}$.

$$f'(x^2-1) = [x^2-1]_{B'} = (2,-2,1,0)^T,$$

porque $2(x) + -2(x+1) + 1(x^2+1) + 0(x^3)$. Agora usamos g para levar este vetor de $\mathbb{R}^4$ em $M_{2\times 2}$, usando a mesma base de antes (C) para $M_{2\times 2}$:

$$g((2,-2,1,0)^T = \left[(2,-2,1,0)^T\right]_C = \begin{pmatrix} 2 & -2 \\ 1 & 0 \end{pmatrix}.$$

Esta matriz é diferente da que havíamos encontrado antes.

Para cada base de $\mathbb{R}_3[x]$ e cada base de $M_{2\times 2}$, teremos duas bijeções f e g. Uma mudança nas bases pode resultar em bijeções completamente diferentes.

O mesmo vale, claramente, para quaisquer outros espaços de dimensão finita. ◀

Como os espaços finitos de dimensão n são todos isomorfos a $\mathbb{R}^n$, podemos desenvolver toda a Álgebra Linear para espaços de dimensão finita trabalhando apenas com $\mathbb{R}^n$.

2.4 Mudança de base

Se tivermos duas bases R e S para um espaço vetorial V, é possível representar cada vetor $\mathbf{v} \in V$ tanto em uma base como em outra. Nesta seção mostramos como obter uma função que, dada $[\mathbf{v}]_R$, determina $[\mathbf{v}]_S$.

Na discussão a seguir, como os somatórios são todos de 1 a n, indicamos apenas o índice em cada um deles ($\sum_i x_i = \sum_{i=1}^n x_i$).

Teorema 2.62. *Sejam $R = (r_1, \ldots, r_n)$ e $S = (s_1, \ldots, s_n)$ duas bases ordenadas diferentes para um espaço V, e seja $\mathbf{v} \in V$. Então as coordenadas de $\mathbf{v}$ na base S podem ser escritas em função das coordenadas de $\mathbf{v}$ na base R.*

Demonstração. Usaremos os seguintes fatos: primeiro, para qualquer $\mathbf{v} \in V$,

$$\mathbf{v} = \sum_i a_i \mathbf{r}_i = \sum_j b_j \mathbf{s}_j.$$

Mas $\mathbf{r}_i \in V$, portanto pode ser escrito usando base S:

$$\mathbf{r}_j = \sum_i q_{ij} \mathbf{s}_i.$$

Escolhemos agora um vetor qualquer $\mathbf{v} \in V$. Temos

$$\begin{aligned}\mathbf{v} &= \sum_j a_j \mathbf{r}_j \\ &= \sum_j a_j \left(\sum_i q_{ij} \mathbf{s}_i \right) \\ &= \sum_j \sum_i a_j q_{ij} \mathbf{s}_i \\ &= \sum_i \left(\sum_j a_j q_{ij} \right) \mathbf{s}_i .\end{aligned}$$

O termo entre parênteses no somatório faz o papel de coeficiente na combinação linear dos $\mathbf{s}_i$, resultando em $\mathbf{v}$ – e portanto deve ser igual a b_i:

$$b_i = \sum_j a_j q_{ij}.$$

Mostramos que cada b_i, coeficiente de $\mathbf{v}$ na base S, pode ser escrito como função dos a_j, coeficientes na base R, usando os q_{ij}, que descrevem os vetores de R na base S. ■

Exemplo 2.63. Considere as duas bases a seguir para $\mathbb{R}_3[x]$:

$$\begin{aligned}A &= \left(1, x, x^2, x^3\right), \\ B &= \left(x, -x^2, x^2 - 2, x^3 - 3\right).\end{aligned}$$

Queremos uma função que leve coordenadas da base A para a base B. Escrevemos cada vetor de A como combinação linear dos vetores de B:

$$\begin{aligned}1 &= 0(x) - \frac{1}{2}(-x^2) - \frac{1}{2}(x^2 - 2) + 0(x^3 - 3), \\ x &= 1(x) + 0(-x^2) + 0(x^2 - 2) + 0(x^3 - 3), \\ x^2 &= 0(x) - 1(-x^2) + 0(x^2 - 2) + 0(x^3 - 3), \\ x^3 &= 0(x) - \frac{3}{2}(-x^2) - \frac{3}{2}(x^2 - 2) + 1(x^3 - 3).\end{aligned}$$

Ou seja, $[1]_B = (0, -1/2, -1/2, 0)^T$, $[x]_B = (1, 0, 0, 0)^T$, $[x^2]_B = (0, -1, 0, 0)^T$ e $[x^3]_B = (0, -3/2, -3/2, 1)^T$.

As coordenadas do polinômio $x^2 - 3$ na base A são

$$[x^2 - 3]_A = (-3, 0, 1, 0)^T,$$

e portanto $a_1 = -3$, $a_2 = 0$. $a_3 = 1$ e $a_4 = 0$.

As coordenadas deste polinômio na base B são $[x^2 - 3]_B = (b_1, b_2, b_3, b_4)^T$, com

$$\begin{aligned}b_1 &= \sum_i a_i q_{i1} = -3(0) + 0(1) + 1(0) + 0(0) = 0 \\ b_2 &= \sum_i a_i q_{i2} = -3(-1/2) + 0(0) + 1(-1) + 0(-3/2) = 1/2\end{aligned}$$

$$b_3 = \sum_i a_i q_{i3} = -3(-1/2) + 0(0) + 1(0) + 0(-3/2) = 3/2$$
$$b_4 = \sum_i a_i q_{i4} = -3(0) + 0(0) + 1(0) + 0(1) = 0$$

E realmente,

$$\begin{aligned} b_1(x) + b_2(-x^2) + b_3(x^2-2) + b_4(x^3-3) &= 0(0) - \frac{x^2}{2} + \frac{3(x^2-2)}{2} + 0(x^3-3) \\ &= \frac{3x^2 - x^2 - 6}{2} = x^2 - 3. \end{aligned}$$

Temos então $[x^2-3]_B = (0, 1/2, 3/2, 0)^T$. Observamos que com os b_j e q_{ij} podemos transformar a representação de *qualquer* vetor da base A para a pase B. ◀

Uma observação importante pode ser feita neste momento: *todo isomorfismo um espaço de dimensão finita nele mesmo representa uma mudança de base.* Isso porque tal isomorfismo leva vetores de V em V, e preserva a linearidade. O que pode mudar após a aplicação do isomorfismo é a base usada para representar os vetores.

Exemplo 2.64. Sejam duas bases para $\mathbb{R}^3$,

$$\begin{aligned} \alpha &= \left\{ (1,0,0)^T, (0,1,0)^T, (0,0,1)^T \right\}, \\ \beta &= \left\{ (1,0,0)^T, (0,1,0)^T, (0,0,1/2)^T \right\}. \end{aligned}$$

Os vetores tem os mesmos coeficientes nas duas bases, exceto que na base β o último coeficiente é o dobro daquele na base α:

$$\left[(1,2,3)^T\right]_\alpha = \left[(1,2,6)^T\right].$$

O isomorfismo $\phi : \mathbb{R}^3 \to \mathbb{R}^3$ tal que

$$\phi(x,y,z)^T = (x,y,2z)^T$$

leva vetores da base α para a base β.

$$\begin{aligned} (x,y,z)^T &= x(1,0,0)^T + y(0,1,0)^T + z(0,0,1)^T \\ \phi(x,y,z)^T &= x\phi[(1,0,0)^T] + y\phi[(0,1,0)^T] + z\phi[(0,0,1)^T] \\ &= (x,0,0)^T + (0,y,0)^T + z(0,0,2)^T \\ &= (x,0,0)^T + (0,y,0)^T + (0,0,2z)^T \\ &= (x,y,2z)^T. \end{aligned}$$ ◀

2.5 Aplicações

2.5.1 Análise Dimensional [base, dependência linear]

Nesta seção tomamos a Análise Dimensional como exemplo de aplicação, de grande importância em muitas Engenharias.

Definição 2.65 (dimensão física)**.** Uma *dimensão física* é uma quantidade física, que pode ser medida em diferentes *unidades*. ♦

Exemplo 2.66. A *quantidade de tempo* entre dois eventos quaisquer é uma dimensão que pode ser medida em diferentes unidades: segundos, horas, dias, etc. A *distância* entre dois objetos também é uma dimensão, que pode ser medida em diferentes unidades: metros, pés, ângstrons, etc.

Ouros exemplos são *pressão*, *carga elétrica*, *massa*, *viscosidade*. ◀

É comum considerar algumas dimensões como fundamentais. Listamos estas dimensões a seguir, cada uma com seu símbolo usual:

- distância (L)
- tempo (T)
- massa (M)
- carga elétrica (Q)

Denotamos a dimensão uma grandeza física x por $[x]$.

Exemplo 2.67. A seguir temos algumas unidades de medida de grandeza física, com suas dimensões.

$$[kg] = M$$
$$[Å] = [cm] = [km] = L$$
$$[s] = [h] = T$$

◀

Usando dimensões fudamentais, construimos dimensões a partir de outras. Por exemplo, usando distância e tempo construímos velocidade e aceleração. Note que o diferencial de uma quantidade física tem a mesma dimensão que a própria quantidade.

$$[v] = \left[\frac{ds}{dt}\right] = \left[\frac{s}{t}\right] = LT^{-1}$$
$$[a] = \left[\frac{dv}{dt}\right] = \left[\frac{d^2s}{dt^2}\right] = \left[\frac{s}{t^2}\right] = LT^{-2}$$

Exemplo 2.68. A seguir temos mais algumas dimensões compostas.

$$\begin{array}{rll} \text{volume} & [m^3] & = L^3 \\ \text{aceleração} & [m/s^2] & = L/T^2 \\ \text{força} & [kg\, m/s^2] & = MLT^{-1} \end{array}$$

A primeira dimensão física mostrada, volume, envolve somente a dimensão fundamental da distancia. A segunda, aceleração, envolve distância e tempo, e a terceira envolve massa, distancia e tempo. ◀

Quando combinamos uma dimensão com ela mesma – por exemplo, quando definimos área e volume a partir de distancia – estamos realizando uma "operação" com um número e aquela dimensão:

$$2 \otimes L = L^2(área)$$
$$3 \otimes L = L^3(volume)$$

Cada dimensão pode, portanto, estar associada a um expoente, e podemos representar dimensões compostas na forma

$$L^{a_1} M^{a_2} T^{a_3}$$

Exemplo 2.69. A tabela a seguir mostra a representação de várias dimensões físicas.

	nome	unidade SI	dimensão física
carga elétrica	Coulomb	C	Q
volume		m^3	M^3
densidade		kg/m^3	ML^{-3}
força (N)	Newton	$N = kg\,m/s^2$	$[N] = MLT^{-2}$
aceleração		m/s^2	$[m/s^2] = LT^{-1}$
pressão (Pa)	Pascal	$Pa = N/m^2$	$[N/m^2] = [(MLT^2)/L^2] = ML^{-1}T^{-2}$
viscosidade		Ns/m^2	$[Ns/m^2] = [MLT^{-2}][T]/[L^{-2}] = ML^{-1}T^{-1}$
energia (J)	Joule	$J = (kg\,m^2)/s^2$	$[kg\,m^2/s^2] = ML^2T^{-2}$
ddp[5]	Volt	V, ou J/C	$[J/C] = ML^2T^{-2}Q^{-1}$
capacitância	Farad	F, ou C/V	$[Q/V] = M^{-1}L^{-2}T^2TQ^2$

◀

Em uma equação envolvendo grandezas físicas, os dois lados devem ter a mesma dimensão – dizemos que a equação deve ser *dimensionalmente homogênea.*

Exemplo 2.70. A equação

$$s = s_0 + v_0 t + \frac{1}{2} a t^2,$$

que descreve o movimento retilíneo uniformemente acelerado, é dimensionalmente homogenea, porque a dimensão do lado esquerdo é $[s] = L$, e do lado direito temos $[s_0] = L$, e

$$\begin{aligned} [v_0 t] &= [v][t] \\ &= \frac{L}{T} T \qquad \text{(velocidade é distância por tempo)} \\ &= L. \end{aligned}$$

$$\begin{aligned} \left[\frac{1}{2} a t^2\right] &= [1/2][a][t^2] \\ &= \mathbf{1}[a][t^2] \\ &= \frac{L}{T^2} T^2 \qquad \text{(aceleração é distância por tempo}^2\text{)} \\ &= L, \end{aligned}$$

e portanto

$$\begin{aligned} [s] &= \left[s_0 + v_0 t + \frac{1}{2} a t^2\right] \\ L &= [s_0] + [v_0 t] + \left[\frac{1}{2} a t^2\right] \\ L &= L + [LT^{-1}]\,[T] + [1/2]\,[LT^{-2}]\,[T^2] \\ L &= L + L + L \end{aligned}$$

◀

Denotamos por **1** a dimensão vazia, que atribuímos a grandezas sem dimensão física.

$$\begin{aligned} [2] &= \mathbf{1} \\ [\cos(x)] &= \mathbf{1} \\ [\theta] &= \mathbf{1} && \text{(se } \theta \text{ é ângulo)} \end{aligned}$$

Exemplo 2.71. A *frequência* é a quantidade de vezes que algo acontece em um período de tempo, e sua dimensão é T^{-1}. Por exemplo, a frequência angular pode ser medida em radianos por segundo; calculamos sua dimensão:

$$\begin{aligned} \left[\frac{\text{rad}}{\text{s}}\right] &= [\text{rad}][1/\text{s}] \\ &= \mathbf{1}[1/\text{s}] && \text{(ângulo tem dimensão } \mathbf{1}\text{)} \\ &= T^{-1}. && \blacktriangleleft \end{aligned}$$

Tendo estes fatos em mente, surge naturalmente a pergunta: as dimensões físicas não formariam um espaço vetorial? A resposta é afirmativa. Observamos na tabela a seguir uma comparação de conceitos. Note que aqui usamos o termo "dimensão física" para elementos de um espaço vetorial.

espaço de dimensões	espaço vetorial
dimensão	vetor
$\mathbf{1}$	$\mathbf{0}$
A^α	$\alpha\mathbf{A}$
A^{-1}	$-\mathbf{A}$
AB	$\mathbf{A}+\mathbf{B}$

As dimensões físicas das variáveis usadas na descrição de fenômenos físicos[6] *formam um espaço vetorial*[7] *sobre* $\mathbb{Q}$*:* sejam A B e C dimensões. Então valem as seguintes propriedades de espaço vetorial.

i) **associatividade:** $(AB)C = A(BC)$, e $(A^p)^q = A^{(pq)}$

ii) **comutatividade:** $AB = BA$

iii) **distributividade:** $A^pA^q = A^{p+q}$, e $(AB)^p = A^pB^p$

iv) **há neutro aditivo:** $\mathbf{1}A = A$

v) **há inversos:** $(A^{-1})A = \mathbf{1}$

vi) **há neutro multiplicativo:** $A^1 = A$

Quando se estabelece uma base para um espaço vetorial de dimensões, dizemos que temos um *sistema*. Por exemplo, se definirmos a base (M, L, T) nos dá o *sistema* MLT. A capacitância, por exemplo, é definida no sistema $MLTQ$, porque depende de massa, distancia, tempo e carga elétrica.

As coordenadas de uma dimensão física no sistema são os expoentes de sua representação.

Exemplo 2.72. As coordenadas da dimensão área são $(0, 2, 0)$, porque

$$[\text{cm}^2] = [\text{m}^2] = L^2 \quad = M^0L^2T^0.$$

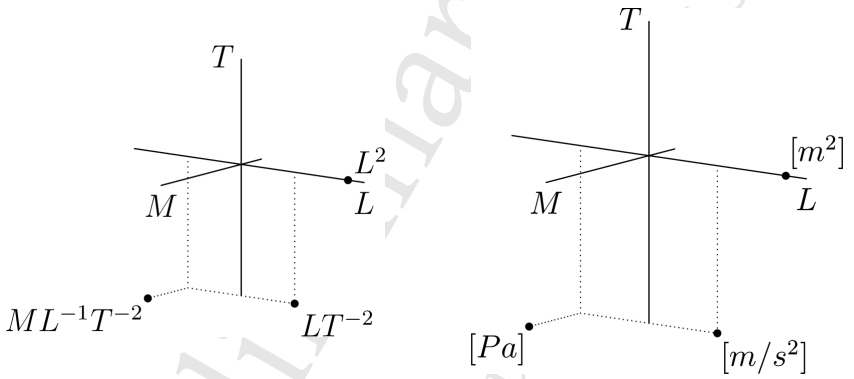
Já as coordenadas da dimensão pressão, $ML^{-1}T^{-2}$ são $(1, -1, -2)$. ◀

[6] Não apenas fenômenos físicos. É um exercício interessante buscar exemplos sem significado físico.

[7] E note que aqui precisamos listar *todas* as condições para caracterizar o espaço vetorial.

As figuras a seguir ilustram o isomorfismo do sistema MLT com $\mathbb{R}^3$ (ambas as figuras mostram os mesmos pontos, mudando apenas seus rótulos). As coordenadas mostradas nas figuras são

$[m^2]$	L^2	$(0,2,0)$
$[Pa]$	$ML^{-1}T^{-2}$	$(1,-1,-2)$
$[m/s^2]$	LT^{-2}	$(0,1,-2)$



É importante observar que os pontos nos gráficos são os vetores do espaço de dimensões – portanto cada um é uma *dimensão*, e *não uma unidade!* Assim, o mesmo ponto rotulado com $[m^2]$ poderia ter sido marcado com $[cm^2]$, $[km^2]$, etc, porque $[m^2] = [cm^2] = [km^2] = L^2$.

Definição 2.73 (dependencia dimensional)**.** Um conjunto de dimensões $A_1, A_2, \ldots, A_n$ é dimensionalmente dependente se é linearmente dependente, com coeficientes racionais. Em outras palavras, é dimensionalmente dependente se existem racionais $\alpha_1, \alpha_2, \ldots, \alpha_n$, nem todos zero, tais que

$$A_1^{\alpha_1} A_2^{\alpha_2} \cdots A_n^{\alpha_n} = \mathbf{1}.$$ ♦

Podemos "traduzir" a definição de dependência dimensional para a nomenclatura e notação com que nos habituamos para espaços vetoriais: ela diz que um conjunto de dimensões (*vetores)* dimensionalmente dependente (*linearmente dependente)* – ou sejam se existem racionais $\alpha_1, \ldots$, nem todos zero, tais que

$$A_1^{\alpha_1} A_2^{\alpha_2} \cdots A_n^{\alpha_n} = \mathbf{1},$$

ou seja,

$$(\alpha_1 \boxtimes A_1) \boxplus (\alpha_2 \boxtimes A_2) \boxplus \cdots \boxplus (\alpha_n \boxtimes A_n) = \mathbf{0},$$

onde $\boxplus$ e $\boxtimes$ são as operações de soma e multiplicação por escalar neste espaço: $A \boxplus B = AB$; e $k \boxtimes A = A^k$.

Exemplo 2.74. As dimensões força, distancia, tempo e massa são dimensionalmente dependentes, como podemos verificar observando suas descrições no sistema MLT:

$$[m] = L$$
$$[s] = T$$
$$[kg] = M$$
$$[Pa] = ML^{-1}T^{-2}$$

A pressão pode ser descrita em termos de massa, tempo e distância. ◀

Exemplo 2.75. As dimensões pressão e área não são dimensionalmente dependentes!

$$[m^2] = L^2$$
$$[Pa] = ML^{-1}T^{-2}$$

Não temos como descrever L^2 em termos de $ML^{-1}T^{-2}$. ◀

Toda dimensão física no sisetma MLT pode ser descrita na forma $M^aL^bT^c$ (ou seja, todo vetor pode ser descrito por suas coordenadas) – e podemos usar este fato para obter fórmulas para descrever fenômenos.

Exemplo 2.76. Suponha que uma partícula cai sobre um fluido viscoso. Sua velocidade para baixo é acelerada pela ação da gravidade, mas depois de um tempo, a aceleração chega a zero.

Para modelar o movimento da partícula, determinaremos uma fórmula que descreva sua velocidade em função do tempo. A velocidade da partícula depende:

- do diâmetro, d;
- da viscosidade, μ;
- da aceleração, g.

Além disso, a velocidade é proporcional à diferença entre a densidade da partícula, ρ_p e a do fluido, ρ_f. Escrevemos, portanto,

$$v = kd^a\mu^b g^c(\rho_p - \rho_f). \tag{2.4}$$

Nesta fórmula, k é uma constante a ser determinada experimentalmente. Os outros fatores são conforme descrevemos, mas ainda não sabemos seus expoentes (ou seja, não sabemos as coordenadas da dimensão física). Mas conhecemos a dimensão física de v, e podemos usá-la: como $[v]$ é um vetor no espaço de dimensões físicas, escrevemos as dimensões da fórmula 2.4:

$$[v] = \left[kd^a\mu^b g^c(\rho_p - \rho_f)\right].$$

Esta fórmula mostra o *mesmo* vetor nos dois lados da igualdade. Suas coordenadas (os expoentes) devem portanto ser as mesmas:

$$\begin{aligned}
[v] &= \left[kd^a\mu^b g^c(\rho_p - \rho_f)\right] \\
M^0LT^{-1} &= \left[kd^a\mu^b g^c(\rho_p - \rho_f)\right] \\
M^0LT^{-1} &= \left[d^a\mu^b g^c(\rho_p - \rho_f)\right] \\
M^0LT^{-1} &= (L)^a\,(ML^{-1}T^{-1})^b\,(L^{-1}T^{-2})^c\,(ML^{-3}) \\
M^0LT^{-1} &= M^{b+1}L^{a-b+c-3}T^{-b-2c}.
\end{aligned}$$

Como os expoentes nos dois lados devem ser iguais, podemos determiná-los resolvendo um sistema linear com três incógnitas e três equações:

$$\begin{cases} b \qquad\quad +1 = 0 \\ a - b + \ c - 3 = 1 \\ -b - 2c \qquad = -1 \end{cases}$$

A solução é $a = 2, b = -1, c = 1$, e podemos escrever os expoentes em nossa fórmula

$$v = kd^2\mu^{-1}g^1(\rho_p - \rho_f),$$

ou

$$\nu = k\frac{d^2 g(\rho_p - \rho_f)}{\mu}. \qquad \blacktriangleleft$$

Exemplo 2.77. Observamos o escoamento laminar de um fluido por um tubo de raio r e comprimento l. A pressão interna no tubo decai com a distância – isto é chamado de *perda de carga*. O volume q é função do raio, da viscosidade do fluido, μ, e da perda de carga, $\Delta p/l$.

$$q = f\left(\frac{\Delta p}{l}, \mu, r\right).$$

Listamos a seguir as dimensões de cada variável.

r	raio	distância	L
q	fluxo	volume por tempo	L^3T^{-1}
μ	viscosidade	força-tempo por área	$ML^{-1}T^{-1}$
$\frac{\Delta p}{l}$	perda de carga	pressão por distância	$ML^{-2}T^{-2}$

As coordenadas das dimensões são iguais em ambos os lados da equação:

$$[q] = \left[\left(\frac{\Delta p}{l}\right)^a (\mu)^b (r)^c\right]$$
$$L^3T^{-1} = (ML^{-2}T^{-2})^a (ML^{-1}T^{-1})^b (L)^c.$$

Chegamos agora ao sistema

$$\begin{cases} a + b = 0 \\ -2a - b + c = 3 \\ -2a - b = -1. \end{cases}$$

Resolvendo, obtemos $a = 1, b = -1, c = 4$, portanto a equação é

$$q = k\frac{\Delta p}{l}(\mu)^{-1}(r)^4$$
$$= k\frac{\Delta p r^4}{l\mu}.$$

Esta é a *equação de Hagen-Poiseuille*. A constante de proporcionalidade k, que pode ser obtida por experimentos, é igual a $\pi/8$. $\blacktriangleleft$

O próximo exemplo mostra que nem sempre obteremos a fórmula exata que procuramos.

Exemplo 2.78. Suponha que uma gota de água cai de uma nuvem imóvel. Determinaremos uma fórmula para sua velocidade. Presumimos, ainda que nos pareça estranho, que a gota é esférica. Seu raio é r, sua densidade é ρ e sua velocidade é v. A viscosidade do ar é μ e a aceleração gravitacional é g.

Se quisermos determinar a velocidade em função das outras variáveis, escrevemos

$$\nu = k r^a g^b \rho^c \mu^d$$
$$[\nu] = \left[r^a\, g^b\, \rho^c\, \mu^d\right]$$
$$LT^{-1} = (L)^a (LT^{-2})^b (ML^{-3})^c (ML^{-1}T^{-1})^d,$$

onde k é uma constante de proporcionalidade. Temos portanto que resolver o sistema

$$\begin{cases} c + d = 0 \\ a + b - 3c - d = -1 \\ -2b - d = 1 \end{cases},$$

que tem quatro incógnitas mas somente três equações. Isso significa que não chegaremos à equação exata da velocidade, mas a uma equação dependendo de um expoente.

Precisamos escolher uma das quatro variáveis para deixar livre. Escolhemos d, e escrevemos a solução como

$$\begin{aligned} a &= -\frac{1+3d}{2} \\ b &= -\frac{1+d}{2} \\ c &= -d, \end{aligned}$$

Substituindo na fórmula,

$$\begin{aligned} v &= k\, r^{-(1+3d)/2} g^{-(1+d)/2} \rho^{-d} \mu^d \\ &= k\, \frac{r^{1/2}}{r^{3d/2}} \frac{g^{1/2}}{g^{d/2}} \frac{\mu^d}{\rho^d} \\ &= k\, \frac{\sqrt{rg}}{\sqrt{r^{3d} g^d}} \frac{\mu^d}{\rho^d} \\ &= k\sqrt{rg} \left(\frac{\mu}{\rho \sqrt{r^3 g}} \right)^d. \end{aligned}$$

Note que se tivéssemos escolhido outra variável livre ao invés de d, chegaríamos a outra fórmula, dando também uma relação válida entre a velocidade da gota e as outras variáveis. ◀

O "Teorema Π de Buckingham" (Teorema 2.79) diz basicamente que se o espaço vetorial onde trabalhamos tem dimensão n, em um conjunto com $k > n$ vetores onde há n vetores LI, podemos descrever todos em função desses n.

Teorema 2.79 (Π, de Buckingham). *Seja Π um espaço de dimensões físicas, cuja dimensão como espaço vetorial é n. Se um experimento físico relaciona grandezas $x_1, x_2, \ldots, x_n, \ldots, x_k$ (onde claramente $k > n$), na forma de uma função*

$$y = f(x_1, x_2, \ldots, x_k),$$

então a relação pode ser reescrita como

$$y = \phi(\pi_{n+1}, \pi_{n+2}, \ldots, \pi_k) x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n},$$

sendo o termo $\phi(\ldots)$ não dimensional (ou seja, tem dimensão $\mathbf{1} = M^0 L^0 T^0$), e

$$\pi_1 = \frac{x_{n+1}}{x_1^{b_{11}} \cdots x_n^{b_{1n}}}$$

$$\pi_2 = \frac{x_{n+2}}{x_1^{b_{21}} \cdots x_n^{b_{2n}}}$$

$$\vdots$$

Demonstração. (Parcial) Claramente, se determinarmos $a_1, a_2, \ldots, a_n$ de forma que $a_1 x_1 a_2 x_2 \ldots a_n x_n$ tenha as mesmas dimensões de y, então *necessariamente* $\phi(\ldots)$ deve ter dimensão $\mathbf{1}$.

A demonstração de que podemos encontrar os π_i na forma dada fica como exercício. ■

Exemplificamos agora o Teorema Π.

Exemplo 2.80. Se uma esfera de diâmetro d se desloca com velocidade v por um fluido com densidade ρ e viscosidade μ, a força contrária ao movimento da esfera é chamada de *força de arrasto*. Como esta força é função da soutras variáveis, temos

$$F_x = f(d, v, \rho, \mu).$$

Sabendo apenas que a relação envolve estas grandezas, poderíamos tentar realizar experimentos, fixando dois parametros de cada vez e variando outros dois. Este procedimento, no entanto, é custoso – e desnecessário se realizarmos a análise dimensional do fenômeno.

A grandeza $f(\ldots)$ tem a mesma dimensão que F_x, e pode ser descrita no sistema MLT com três vetores (dimensões físicas) linearmente independentes (ou "dimensionalmente independentes"). Os vetores que representam as quatro dimensões $[d]$, $[v]$, $[\rho]$, $[\mu]$ são

$$\begin{matrix} d \\ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \end{matrix} \quad \begin{matrix} v \\ \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} \end{matrix} \quad \begin{matrix} \rho \\ \begin{pmatrix} 1 \\ -3 \\ 0 \end{pmatrix} \end{matrix} \quad \begin{matrix} \mu \\ \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix} \end{matrix}$$

Escolhemos d, v, ρ, que são independentes. Sabemos portanto que μ pode ser descrito como combinação linear de d, v, ρ. Usando o Teorema Π de Buckingham, chamamos esta combinação linear de π, e a força de arrasto é descrita como

$$F_x = \phi(\pi)\, d^a v^b \rho^c,$$

onde π tem dimensão $[\pi] = \mathbf{1}$:

$$\pi = \frac{\mu}{d^x v^y \rho^z}.$$

O próximo passo é calcular a, b e c.

$$[F_x] = \left[d^a v^b \rho^c\right]$$
$$MLT^{-2} = (L)^a (LT^{-1})^b (ML^{-3})^c$$

Chegamos ao sistema

$$\begin{cases} c = 1 \\ a + b - 3c = 1 \\ -b = -2 \end{cases}$$

Os valores de a, b e c são portanto

$$a = b = 2, \quad c = 1.$$

Precisamos determinar também x, y, z, que usamos na descrição de π. Novamente, sabendo que a dmiensão de π é $[\pi] = \mathbf{1} = M^0L^0T^0$, calculamos

$$\begin{aligned} M^0L^0T^0 &= [\mu][d^x\nu^y\rho^z] \\ M^0L^0T^0 &= (ML^{-1}T^{-1})\,L^x\,(LT^{-1})^y\,(ML^{-3})^z \end{aligned}$$

Resolvemos o sistema,

$$\begin{cases} z + 1 = 0 \\ x + y - 3z - 1 = 0 \\ -y \quad\quad - 1 = 0 \end{cases}$$

e obtendo os valores

$$x = y = z = -1.$$

Isto nos dá $\pi = \mu/(d\nu\rho)$, e temos agora

$$F_x = \phi\left(\frac{\mu}{d\nu\rho}\right) d^2\nu^2\rho$$

Esta é a *equação do arrasto*, e o que chamamos aqui de $\phi(\mu/(d\nu\rho))$ é o *coeficiente de arrasto.*

Agora, tendo a equação do arrasto, percebemos que precisamos de um único experimento para determinar o coeficiente de arrasto. ◀

Há muito material escrito sobre análise dimensional. No entanto, não é comum descrever o espaço dimensional como fizemos, em termos de espaços vetoriais. Uma boa introdução à Análise Dimensional (ainda sem tratar o espeço dimensional como espaço vetorial) é dada no livro de Gibbings [Gib11].

Esta seção incluiu exemplos envolvendo Mecânica Básica e Mecânica de Fluidos. Para uma introdução à Mecânica Geral, o leitor pode consultar o livro de J. Den Hartog [Har61]. O livro de Robert Brodkey [Bro95] dá uma boa introdução à Mecânica de Fluidos.

★ 2.5.2 Fractais [isomorfismo]

Muitos dos fractais mais conhecidos, em particular o conjunto de Mandelbrot e os conjuntos de Fatou e Julia, são definidos no plano complexo.

Abordaremos o *conjunto de Mandelbrot*.

Considere a seguinte sequencia: começamos com um número complexo inicial z_0. Os outros números da sequência são obtidos elevando o anterior ao quadrado e somando ao número inical z_0, ou seja,

$$\begin{aligned} z_0 &= c \\ z_{n+1} &= z_n^2 + z_0 \end{aligned} \tag{2.5}$$

Por exemplo, se começarmos com $z_0 = 2i$, a sequência será

$$\begin{aligned} z_0 &= 2i \\ z_1 &= (2i)^2 + 2i = -4 + 2i \\ z_2 &= (-4 + 2i)^2 + 2i = 12 - 14i \\ z_3 &= (12 - 14i)^2 + 2i = -52 - 334i \end{aligned}$$

$$\vdots$$

Dependendo do número z_0 escolhido, o limite da sequencia (z_n) quando $n \to \infty$ pode ser infinito (ou seja, a sequencia *diverge*), ou finito. Damos a seguir exemplos de duas destas situações.

i) Se $z_0 = 1$, a sequencia é

$$\begin{aligned} z_0 &= 1 \\ z_1 &= 1^2 + 1 = 2 \\ z_2 &= (2)^2 + 1 = 5 \\ z_3 &= (5)^2 + 1 = 26 \\ &\vdots \end{aligned}$$

ii) Se $z_0 = -2$, temos

$$\begin{aligned} z_0 &= -2 \\ z_1 &= (-2)^2 - 2 = 2 \\ z_2 &= (2)^2 - 2 = 2 \\ z_3 &= (2)^2 - 2 = 2 \\ &\vdots \end{aligned}$$

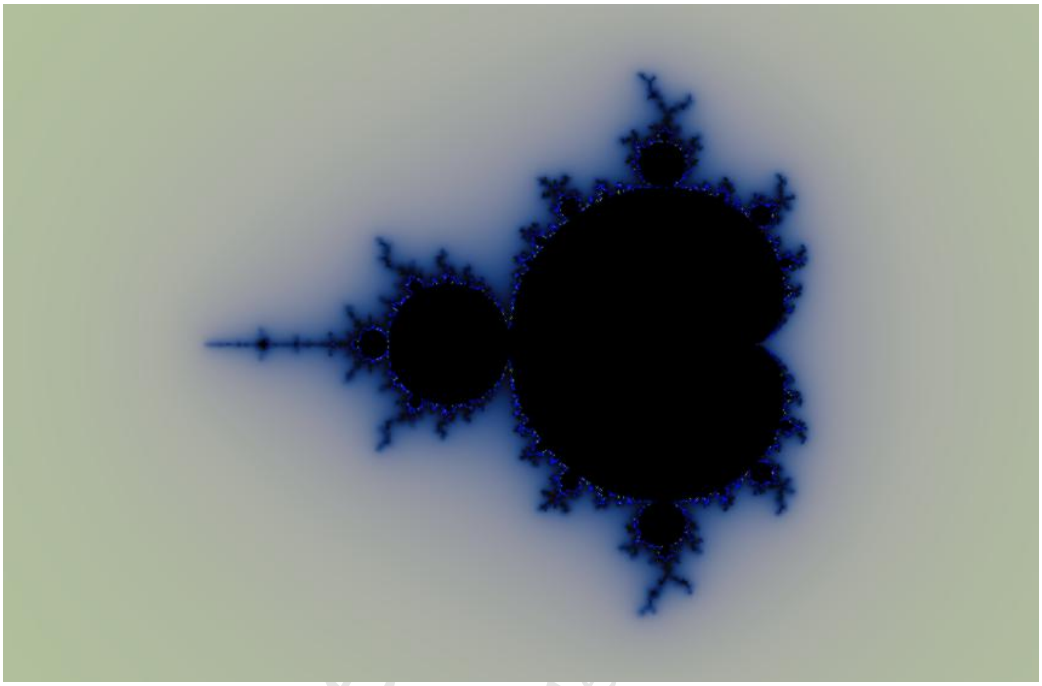
Se para um número $c = a + bi$ a sequência *não diverge*, então z_0 é parte do conjunto de Maldelbrot.

A sequência no caso (i) é divergente (seu limite é $+\infty$), portanto 1 *não* pertence ao conjunto de Mandelbrot.

Já a sequência no caso (ii) é limitada (mais ainda, exceto por z_0 todos os z_i são iguais a dois), logo -2 *pertence* ao conjunto de Maldelbrot.

O ponto importante deste exemplo é: *como conhecemos um isomorfismo entre $\mathbb{C}$ e $\mathbb{R}^2$, podemos plotar o conjunto de Mandelbrot no plano.*

Para plotar o conjunto de Mandelbrot, escolhemos os pontos (x, y) do plano com $-2 \leq x \leq 1$ e $-1 \leq y \leq 1$. Para cada um desses pontos, tomamos $c = x + yi$ e computamos vários valores da sequência z_n descrita na fórmula 2.5. – por exemplo, de z_0 até z_{20}. Se percebemos que a sequência converge, pintamos o ponto de preto. Se não, usamos alguma outra cor para indicar quão rapidamente a sequência diverge. A imagem a seguir, que mostra o conjunto de Mandelbrot, foi construída desta forma.



Exercícios

Ex. 40 — O conjunto

$$A = \{(x, y, z)^T \ : \ x + 2y - 3z = 0\}$$

é subespaço de $\mathbb{R}^3$? Se for, mostre um complemento dele.

Ex. 41 — Considere os subespaços de $\mathbb{R}^5$:

- $A = \{(v, w, x, y, z)^T \ : \ x + y - z = v\}$
- $B = \{(v, w, x, y, z)^T \ : \ v - 2w = x + y + z\}$

Responda o seguinte:

i) Quem são os vetores no subespaço $A \cap B$?

ii) Determine $\dim A$, $\dim B$, $\dim(A \cap B)$.

iii) Mostre um complemento de $A \cap B$.

iv) $\mathbb{R}^5$ é soma de A com B? Se for, é soma direta?

Ex. 42 — O conjunto de soluções para $A\mathbf{x} = \mathbf{0}$ no exemplo 2.54 é um subespaço de $\mathbb{R}^4$. Determine um complemento para ele.

Ex. 43 — A união do subespaço de funções pares com o subespaço de funções ímpares é subespaço?

Ex. 44 — Uma base de um espaço vetorial V pode (ou deve sempre) ser subespaço de V?

Ex. 45 — Se um subespaço de $\mathbb{R}^n$ contém vetores da forma $(\ldots, 0, \ldots)^T$, tendo a i-ésima coordenada igual a zero, é verdade que toda base para este subespaço também terá zero na i-ésima coordeanda?

Ex. 46 — Sejam $A = (1, x, x^2, x^3)$, $B = (-1, 2x^2 - x + 1, x^3 + x^2)$, $C = (\pi, x - \pi, x^2 + \pi^2 - x + \pi, \pi x^3)$ bases para $\mathbb{R}_3[x]$. Escreva as coordenadas dos polinômios a seguir usando A, B e C como base ou, se não for possível, explique o motivo. 1, x, x^2, x^3, $(x + 1)(x - 2)$, $(x^2 + \pi x)(1 - 2x)$

★ **Ex. 47 —** O que significa dois grafos de ciclos disjuntos (exemplo 1.41, página 20) serem linearmente dependentes ou linearmente independentes?

★ **Ex. 48 —** Qual é a dimensão do espaço de sequencias reais? E o das sequências reais constantes? Se algum deles for finito, apresente uma base.

Ex. 49 — É possível obter uma base para $M_{n\times n}$, sem usar nenhum zero nas matrizes da base?

★ **Ex. 50 —** Um grafo finito tem um número finito de ciclos. Quem é a base para o espaço de ciclos de um grafo finito (o espaço de ciclos foi definido no exemplo 1.41 na página 20)?

Ex. 51 — Defina o conjunto P_n como um conjunto de n de vetores en $\mathbb{R}^n$, de forma que o primeiro vetor de P_n tem os n primeiros números primos, o segundo vetor tem os n próximos números primos, e assim por diante. P_n é base para $\mathbb{R}^n$?

★ **Ex. 52 —** Prove que em todo espaço vetorial de dimensão infinita, dado qualquer $k \in \mathbb{N}$, podemos encontrar k vetores linearmente independentes.

Ex. 53 — Prove que são isomorfos os espaços:

- [B], com $B = \{(0, 1, 1)^T, (1, 1, 1)^T\}$ e $\mathbb{R}^2$.
- $\mathbb{R}^5$ e o conjunto de todos os polinômios com grau par e menor ou igual a oito.

Ex. 54 — Mostre que a bijeção g dada no exemplo 2.54 é realmente um isomorfismo.

Ex. 55 — Use as técnicas da seção 2.5.1 para determinar a fórmula da resultante centrípeta em movimento circular. Suponha que você só se lembra que as grandezas físicas envolvidas são massa, velocidade angular e raio do caminho circular.

Ex. 56 — Existe um isomorfismo f entre $\mathbb{C}$ e o espaço das matrizes antissimétricas de ordem dois com as seguintes propriedades: para todos complexos z_1 e z_2,

- $f(z_1) + f(z_2) = f(z_1 + z_2)$;
- $f(z_1) - f(z_2) = f(z_1 - z_2)$;
- $f(z_1)f(z_2) = f(z_1 z_2)$;
- $f(z_2)^{-1} f(z_1) = f(z_1/z_2)$, se $z_2 \neq 0$.

Mostre este isomorfismo;

★ **Ex. 57 —** Mostre o isomorfismo entre $\mathbb{Z}_2^n$ e o espaço de ciclos disjuntos de um grafo.

Capítulo 3

Transformações Lineares

O objeto de estudo neste Capítulo são as *transformações lineares* – certas funções que levam elementos de um espaço vetorial em outro, de grande importância em todas as áreas das Ciências Exatas.

Definição 3.1 (Transformação e operador linear)**.** Sejam U e V dois espaços vetoriais sobre um mesmo corpo. Uma *transformação linear* é uma função $T : V \to U$ tal que para todo escalar c e todos os vetores $\mathbf{v}, \mathbf{w} \in V$,

- $T(\mathbf{v} + \mathbf{w}) = T(\mathbf{v}) + T(\mathbf{w})$;
- $T(c\mathbf{v}) = cT(\mathbf{v})$.

Um *operador linear* é uma transformação linear de um espaço nele mesmo ($T : U \to U$). ♦

Exemplo 3.2. A função $f(x_1, x_2) = x_1 + x_2$ é uma transformação linear de $\mathbb{R}^2$ em $\mathbb{R}$, porque

i) para dois vetores (x_1, x_2) e (y_1, y_2),

$$f[(x_1, x_2) + (y_1, y_2)] = f(x_1 + y_1, x_2 + y_2) = x_1 + y_1 + x_2 + y_2 = f(x_1, x_2) + f(y_1 + y_2);$$

ii) para qualquer constante k e qualquer vetor (x_1, x_2),

$$f(k(x_1, x_2)) = f(kx_1, kx_2) = kx_1 + kx_2 = k(x_1 + x_2) = kf(x_1, x_2).$$

◄

Exemplo 3.3. Em qualquer espaço vetorial podemos definir a função identidade, que denotamos por id e que realiza a transformação $\mathrm{id}(\mathbf{v}) = \mathbf{v}$. Esta função é um operador linear: leva vetores de um espaço vetorial nele mesmo, e para quaisquer vetores $\mathbf{v}$ e $\mathbf{w}$,

- $\mathrm{id}(\mathbf{v} + \mathbf{w}) = \mathrm{id}(\mathbf{v}) + \mathrm{id}(\mathbf{w}) = \mathbf{v} + \mathbf{w}$;
- $\mathrm{id}(c\mathbf{v}) = c\,\mathrm{id}(\mathbf{v}) = c\mathbf{v}$. ◄

Exemplo 3.4. A função que dá a transposta de uma matriz é uma transformação linear de M_{mn} em M_{nm}: claramente, $c(A^T) = (cA)^T$, e $A^T + B^T = (A + B)^T$. ◄

Exemplo 3.5. No espaço vetorial formado por polinômios de grau menor ou igual a n, a derivada é uma transformação linear: (i) $d/dx(p(x) + q(x)) = d/dx(p(x)) + d/dx(q(x))$, e (ii) $k\,[\,d/dx(p(x))\,] = d/dx(kp(x))$. ◀

Exemplo 3.6. A função $f(x_1, x_2) = x_1^2 + x_2$ *não* é uma transformação linear de $\mathbb{R}^2$ em $\mathbb{R}$, porque

$$f(x_1 + y_1, x_2 + y_2) = (x_1 + y_1)^2 + x_2 + y_2$$

que não é, de maneira geral, igual a $x_1^2 + y_1^2 + x_2 + y_2$. ◀

Exemplo 3.7. Seja $T : \mathbb{R} \to \mathbb{R}$, com $T(x) = x + 4$. Esta função *não* é uma transformação linear, porque

$$\begin{aligned} T(x + y) &= (x + y) + 4 \\ &\neq T(x) + T(y) = (x + 4) + (y + 4) = (x + y) + 8, \end{aligned}$$

e portanto $T(x + y) \neq T(x) + T(y)$. ◀

Exemplo 3.8. Considere a transformação $T : \mathbb{R}^2 \to \mathbb{R}^3$, com $T(x, y) = (x + y, y, 1)$:

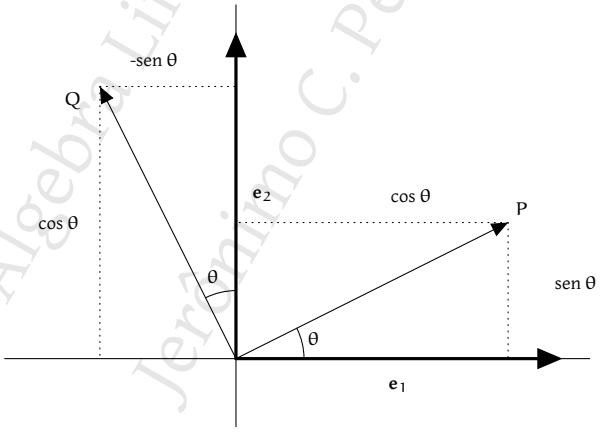
$$\begin{aligned} cT(x, y) &= c(x + y, y, 1) = (cx + cy, cy, c), \\ T(cx, cy) &= (cx + cy, cy, 1). \end{aligned}$$

Como $cT(x, y) \neq T(cx, cy)$, a transformação *não* é linear. ◀

Exemplo 3.9. Em $\mathbb{R}^2$, o operador que rotaciona um ponto por um ângulo θ ao redor da origem e no sentido anti-horário é linear. Não damos aqui uma demonstração formal completa, mas a intuição: primeiro, suponha que multiplicarmos um vetor $\mathbf{w}$ por uma constante c e depois rotacionarmos por um ângulo θ, obteremos um novo vetor. Se rotacionarmos primeiro para multiplicarmos depois, o resultado é o mesmo – portanto $T(c\mathbf{w}) = cT(\mathbf{w})$.

Sejam $\mathbf{u}$ e $\mathbf{v}$ dois vetores. A soma $\mathbf{u} + \mathbf{v}$ resulta em um vetor $\mathbf{w}$, que rotacionado é $\mathbf{w}'$. Se primeiro rotacionarmos $\mathbf{u}$ e $\mathbf{v}$ para depois somarmos, obteremos $\mathbf{w}'$. Assim, $T(\mathbf{u} + \mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v})$.

Construiremos o operador T que rotaciona pontos desta forma, e ao definí-lo, manteremos a linearidade. A figura a seguir mostra o efeito do operador quando rotacionamos os vetores $\mathbf{e}_1$ e $\mathbf{e}_2$ por um ângulo θ.



Suponha que queiramos rotacionar $\mathbf{e}_1$. O novo vetor deverá ser

$$P = T\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\cos\theta\\ \operatorname{sen}\theta\end{pmatrix}.$$

E se rotacionarmos $\mathbf{e}_2$, teremos

$$Q = T\begin{pmatrix}0\\1\end{pmatrix}[r] = \begin{pmatrix}-\operatorname{sen}\theta\\ \cos\theta\end{pmatrix}.$$

O operador T deve então obedecer

$$\begin{aligned} T[(1,0)^T] &= (\cos\theta, \operatorname{sen}\theta)^T \\ T[(0,1)^T] &= (-\operatorname{sen}\theta, \cos\theta)^T. \end{aligned}$$

Como T é linear, então necessariamente

$$\begin{aligned} T[(x,0)^T] &= xT[(1,0)^T] = (x\cos\theta, x\operatorname{sen}\theta)^T \\ T[(0,y)^T] &= yT[(0,1)^T] = (-y\operatorname{sen}\theta, y\cos\theta)^T, \end{aligned}$$

e

$$\begin{aligned} T[(x,y)^T] &= T[(x,0)^T] + T[(0,y)^T] \\ &= (x\cos\theta, x\operatorname{sen}\theta)^T + (-y\operatorname{sen}\theta, y\cos\theta)^T \\ &= (x\cos\theta - y\operatorname{sen}\theta, x\operatorname{sen}\theta + y\cos\theta)^T. \end{aligned}$$

A transformação T é, portanto

$$T\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}x\cos\theta - y\operatorname{sen}\theta\\ x\operatorname{sen}\theta + y\cos\theta\end{pmatrix}$$ ◀

Exemplo 3.10. No exemplo 1.39 mostramos que as variáveis aleatórias reais em um espaço amostral formam um espaço vetorial sobre $\mathbb{R}$. Também sabemos que $\mathbb{R}$ é um espaço vetorial sobre si mesmo.

A esperança de uma variável aleatória discreta X é definida como

$$\mathbb{E}(X) = \sum_x x\Pr(x),$$

desde que o somatório convirja. A linearidade é consequência direta desta definição. Verificamos a soma,

$$\begin{aligned} \mathbb{E}(X+Y) &= \sum_x \sum_y (x+y)\Pr[X=x, Y=y] \\ &= \sum_x x\sum_y \Pr[X=x, Y=y] + \sum_y y\sum_x \Pr[X=x, Y=y] \\ &= \sum_x x\Pr(x) + \sum_y y\Pr(y) \\ &= \mathbb{E}(X) + \mathbb{E}(Y). \end{aligned}$$

Verificamos também a multiplicação por escalar:

$$\mathbb{E}(cX) = \sum_x cx\Pr(x) = c\mathbb{E}(X),$$

ou seja, a esperança de c vezes a variável aleatória X é igual a c multiplicado pela esperança de X. ◀

★ **Exemplo 3.11.** Seja $T : \mathbb{Z}_2^5 \to \mathbb{Z}_2^4$, tal que

$$T[\ (a, b, c, d, e)\ ] = (a \oplus b, b, 0, 0).$$

T é uma transformação linear:

i)

$$\begin{aligned} T[\ (abcde) \oplus (\alpha\beta\gamma\delta\epsilon)\ ] &= T(a \oplus \alpha, b \oplus \beta, c \oplus \gamma, e \oplus \epsilon) \\ &= (a \oplus \alpha \oplus b \oplus \beta, b \oplus \beta, 0, 0) \\ &= (a \oplus b, b, 0, 0) \oplus (\alpha \oplus \beta, \beta, 0, 0) \\ &= T(a, b, c, d, e) \oplus T(\alpha\beta\gamma\delta\epsilon). \end{aligned}$$

ii)

$$\begin{aligned} T[k(a, b, c, d, e)] &= T(ka, kb, kc, kd, ke) \\ &= (ka \oplus kb, kb, 0, 0) \\ &= k(a \oplus b, b, 0, 0) \\ &= kT(a, b, c, d, e). \end{aligned}$$

Agora considere $F : \mathbb{Z}_2^3 \to \mathbb{Z}^3$, com

$$F[\ (a, b, c)\ ] = (ab, c, 1)$$

não é linear, porque $F[(a, b, c) \oplus (\alpha, \beta, \delta)] \neq F[(a, b, c)] \oplus F[(\alpha, \beta, \delta)]$. ◄

Nos exemplos3.7, 3.8 e 3.11, mostramos transformações que levavam vetores a outros com alguns elementos fixos, e que não eram lineares. Há uma maneira muito rápida de determinar que tais transformações não são lineares: o Teorema 3.12 nos informa que para qualquer transformação linear T, deve sempre valer $T(\mathbf{0}) = \mathbf{0}$. Assim, uma transformação que leve a vetores que não podem ser zero não é linear.

Teorema 3.12. *Seja* $T : U \to V$ *uma transformação linear. Então, para todos* $\mathbf{x_1}, \mathbf{x_2} \ldots, \mathbf{x_n} \in U$ *e escalares* k_1, $k_2, \ldots, k_n$,

i) $T(\mathbf{0}) = \mathbf{0}$

ii) $T(k_1\mathbf{x_1} + k_2\mathbf{x_2} + \cdots + k_n\mathbf{x_n}) = k_1T(\mathbf{x_1}) + k_2T(\mathbf{x_2}) + \cdots + k_nT(\mathbf{x_n})$

Demonstração. (i) Como T é transformação linear, $cT(\mathbf{0}) = T(c\mathbf{0})$. Mas

$$\begin{aligned} cT(\mathbf{0}) &= T(c\mathbf{0}), \text{ e} \\ cT(\mathbf{0}) &= T(\mathbf{0}), \end{aligned}$$

o que implica em $c = 1$ ou $T(\mathbf{0}) = \mathbf{0}$. Como c representa *qualquer* escalar, temos necessariamente $T(\mathbf{0}) = \mathbf{0}$.

(ii) Intuitivamente, a afirmativa é verdadeira porque a soma de vetores é associativa e a multiplicação por escalar é distributiva sobre a soma. Formalmente, a demonstração segue facilmente por indução em n, usando a associatividade da soma de vetores e o fato de T ser linear. A base de indução é para um único termo:

$$T(k_1\mathbf{x_1}) = k_1T(\mathbf{x_1}),$$

que é verdadeira pela definição de transformação linear.

A hipótese é de que a afirmação vale para $m-1$. O passo é:

$$\begin{aligned}
T(k_1\mathbf{x_1}+k_2\mathbf{x_2}+\cdots+k_m\mathbf{x_m}) &= T\left[k_1\mathbf{x_1}+(k_2\mathbf{x_2}+\cdots+k_m\mathbf{x_m})\right] && \text{(associatividade de } +\text{)}\\
&= T(k_1\mathbf{x_1})+T(k_2\mathbf{x_2}+\cdots+k_m\mathbf{x_m}) && \text{(T é linear)}\\
&= k_1T(\mathbf{x_1})+T(k_2\mathbf{x_2}+\cdots+k_m\mathbf{x_m}) && \text{(T é linear)}\\
&= k_1T(\mathbf{x_1})+k_2T(\mathbf{x_2})+\cdots+k_mT(\mathbf{x_m}). && \text{(pela hipótese de indução)}
\end{aligned}$$

E concluímos a demonstração. ■

Na seção 2.4 mostramos como obter uma função de mudança de base para espaços vetoriais. Essa função é linear, e a demonstração é pedida no exercício 66.

Teorema 3.13. *Sejam* R *e* S *duas bases para um espaço vetorial* V *de dimensão finita. Então a função que realiza a mudança de base em cada coeficiente é uma transformação linear.*

Exemplo 3.14. A seguir temos duas bases para $\mathbb{R}^3$.

$$\begin{aligned}
\alpha &= \{(1,0,0)^T,(0,1,0)^T,(0,0,1)^T\}\\
\beta &= \{(1/2,0,0)^T,(0,3,0)^T,(0,0,1)^T\}
\end{aligned}$$

A transformação que muda da base α para a base β é

$$T\left[(x,y,z)^T\right] = (2x,y/3,z)^T.$$

Assim, se $\mathbf{x}=(1,1,1)^T$, temos

$$\begin{aligned}
[\mathbf{x}]_\alpha &= (1,1,1)^T,\\
[\mathbf{x}]_\beta &= T([\mathbf{x}]_\alpha) = (2,1/3,1)^T.
\end{aligned}$$

Verificamos que ambos representam o mesmo vetor, expandindo-os como combinação linear de cada uma das bases:

$$\begin{aligned}
[\mathbf{x}]_\alpha = (1,1,1)^T &\Rightarrow \mathbf{x} = 1(0,0,1)^T+1(0,1,0)^T+1(1,0,0)^T = (1,1,1)^T\\
[\mathbf{x}]_\beta = (2,1/3,1)^T &\Rightarrow \mathbf{x} = 2(1/2,0,0)^T+1/3(0,3,0)^T+1(1,1,1)^T = (1,1,1)^T.
\end{aligned}$$

A transformação T é linear: primeiro mostramos que $T[k\mathbf{v}] = kT(\mathbf{v})$.

$$\begin{aligned}
T(k\mathbf{v}) &= T\left[k(x,y,z)^T\right]\\
&= T\left[(kx,ky,kz)^T\right]\\
&= (2kx,ky/3,kz)^T\\
&= k(2x,y/3,z)^T\\
&= kT\left[(x,y,z)^T\right].
\end{aligned}$$

Agora mostramos que $T(\mathbf{v}+\mathbf{w}) = T(\mathbf{v})+T(\mathbf{w})$. Sejam $\mathbf{v}=(x,y,z)^T$ e $\mathbf{w}=(a,b,c)^T$.

$$T(\mathbf{v}+\mathbf{w}) = T\left[(x,y,z)^T+(a,b,c)^T\right]$$

$$
\begin{aligned}
&= T\left[(x+a, y+b, z+c)^T\right] \\
&= (2x+2a, y/3+b/3, z+c)^T \\
&= (2x, y/3, z)^T + (2a, b/3, c)^T \\
&= T\left[(x,y,z)^T\right] + T\left[(a,b,c)^T\right].
\end{aligned}
$$

◀

Da definição de transformação linear, observamos que podemos somar duas transformações T e S, de forma que a transformação $(T+S)$, dada por $(T+S)(\mathbf{x}) = T(\mathbf{x}) + S(\mathbf{x})$ também é linear; e similarmente, também podemos multiplicar uma transformação T por um escalar k, obtendo a transformação kT, dada por $kT(\mathbf{x}) = T(k\mathbf{x})$.

Além da soma e da multiplicação por escalar, também podemos realizar a composição de transformações (que resulta em uma transformação também linear), e em alguns casos, obter a inversa de uma transformação (e quando a inversa existe, ela é linear).

Definição 3.15 (Composição de transformações)**.** Sejam $S : V \to U$ e $T : U \to W$ duas transformações lineares. A composição de T com S é

$$(T \circ S)(\mathbf{v}) = T(S((v))).$$

♦

Exemplo 3.16. Sejam $S : \mathbb{R}^4 \to \mathbb{R}^3$ e $T : \mathbb{R}^3 \to \mathbb{R}^3$, tais que

$$
\begin{aligned}
S[(a,b,c,d)^T] &= (a+b, b+c, c+d)^T \\
T[(x,y,z)^T] &= (-x, -y, x+y+z)^T.
\end{aligned}
$$

Então a composição de S e T é

$$
\begin{aligned}
(T \circ S)(a,b,c,d)^T &= T(S(a,b,c,d)^T) \\
&= T(a+b, b+c, c+d)^T \\
&= (-a-b, -b-c, a+2b+2c+d)^T.
\end{aligned}
$$

Note que a composição é $(T \circ S) : \mathbb{R}^4 \to \mathbb{R}^3$. ◀

Exemplo 3.17. Sabemos que a transposição de matriz quadrada é um operador linear. Outra transformação linear em matrizes quadradas é a multiplicação de uma linha por um escalar. Tomemos então o espaço $\mathcal{M}_{3\times 3}$, com as tranformações:

- transposição,

$$T\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{pmatrix};$$

- multiplicação da terceira linha por 5,

$$M\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 5a_{31} & 5a_{32} & 5a_{33} \end{pmatrix}.$$

A composição $T \circ M$ é

$$T \circ M\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = T\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 5a_{31} & 5a_{32} & 5a_{33} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{21} & 5a_{31} \\ a_{12} & a_{22} & 5a_{32} \\ a_{13} & a_{32} & 5a_{33} \end{pmatrix}.$$

◀

Exemplo 3.18. Em $\mathbb{R}_3[x]$, os dois operadores a seguir são lineares:

- a derivada segunda,
$$\frac{d^2}{dx^2}(a_0 + a_1x + a_2x^2 + a_3x^3) = 2a_2 + 6a_3x$$
- a troca do primeiro com o último coeficiente,
$$T(a_0 + a_1x + a_2x^2 + a_3x^3) = a_3 + a_1x + a_2x^2 + a_0x^3.$$

A composição $d^2/dx^2 \circ T$ é

$$\begin{aligned}\frac{d^2}{dx^2}T(a_0 + a_1x + a_2x^2 + a_3x^3) &= \frac{d^2}{dx^2}(a_3 + a_1x + a_2x^2 + a_0x^3)\\ &= 2a_2 + 6a_0x.\end{aligned}$$ ◀

Exemplo 3.19. Seja T o operador em $\mathbb{R}^2$ que realiza rotação pelo ângulo $\pi/2$, e S o operador que realiza rotação por $-\pi/4$. Nossa intuição diz que a composição das duas deve ser igual à rotação pelo ângulo $\pi/4$. Verificamos[1] então como seria a rotação R por $\pi/4$:

$$R\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}x\cos(\pi/4) - y\,\mathrm{sen}(\pi/4)\\ x\,\mathrm{sen}(\pi/4) + y\cos(\pi/4)\end{pmatrix} = \begin{pmatrix}(x-y)/\sqrt{2}\\(x+y)/\sqrt{2}\end{pmatrix} \qquad \text{(ângulo } \pi/4\text{)}$$

Agora calculamos a composição de T com S:

$$T\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}x\cos(\pi/2) - y\,\mathrm{sen}(\pi/2)\\ x\,\mathrm{sen}(\pi/2) + y\cos(\pi/2)\end{pmatrix} = \begin{pmatrix}-y\\x\end{pmatrix} \qquad \text{(ângulo } \pi/2\text{)}$$

$$S\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}x\cos(-\pi/4) - y\,\mathrm{sen}(-\pi/4)\\ x\,\mathrm{sen}(-\pi/4) + y\cos(-\pi/4)\end{pmatrix} = \begin{pmatrix}(x+y)/\sqrt{2}\\(-x+y)/\sqrt{2}\end{pmatrix}. \qquad \text{(ângulo } -\pi/4\text{)}$$

A composição $T \circ S$ é

$$\begin{aligned}T\left[S\begin{pmatrix}x\\y\end{pmatrix}\right] &= T\begin{pmatrix}(x+y)/\sqrt{2}\\(-x+y)/\sqrt{2}\end{pmatrix}\\ &= \begin{pmatrix}(x-y)/\sqrt{2}\\(x+y)/\sqrt{2}\end{pmatrix},\end{aligned}$$

exatamente igual à rotação por $\pi/4$. ◀

Proposição 3.20. *A composição de transformações lineares é também uma transformação linear.*

[1] Lembrete:

$$\pi/2 = 90^o \qquad \pi/4 = 45^o \qquad -\pi/4 = -45^o$$

$$\begin{array}{lll}\mathrm{sen}(\pi/2) = 1 & \mathrm{sen}(\pi/4) = +1/\sqrt{2} & \mathrm{sen}(-\pi/4) = -1/\sqrt{2}\\ \cos(\pi/2) = 0 & \cos(\pi/4) = +1/\sqrt{2} & \cos(-\pi/4) = +1/\sqrt{2}\end{array}$$

Teorema 3.21. *Sejam*

$$\begin{aligned} Q &: V \to U \\ R &: V \to U \\ S &: W \to V \\ T &: W \to V \end{aligned}$$

transformações lineares. Então

$$\begin{aligned} R \circ (S + T) &= (R \circ S) + (R \circ T) \\ (Q + R) \circ S &= (Q \circ S) + (R \circ S). \end{aligned}$$

Definição 3.22 (Inversa de transformação linear)**.** Seja $T : V \to U$ uma transformação linear. T é invertível se e somente se é bijetora. A inversa de T, denotada T^{-1}, é tal que $T^{-1}(T(\mathbf{v})) = \mathbf{v}$. ♦

Exemplo 3.23. A transformação $T : \mathbb{R}^2 \to \mathbb{R}^2$ com

$$T(x, y)^T = (2x, 3y)^T$$

é invertível, com inversa

$$T^{-1}(a, b)^T = (a/2, b/3)^T.$$ ◀

Exemplo 3.24. Em qualquer espaço vetorial diferente do espaço trivial, fica evidente que a transformação $T(\mathbf{v}) = \mathbf{0}$ não tem inversa. ◀

Exemplo 3.25. A transposta de uma matriz quadrada sempre tem inversa (que é ela mesma, já que $(A^T)^T = A$). Assim, esta é uma transformação invertível. ◀

Exemplo 3.26. O exemplo 3.39 mostra o operador $T(x, y)^T = (x, 2x)^T$ em $\mathbb{R}^2$. Esta transformação não é bijetora:

$$T[(3, 4)^T] = (3, 6)^T = T[(3, 1)^T],$$

portanto não tem inversa. ◀

Exemplo 3.27. Em $\mathbb{R}_n[x]$, a derivada é um operador linear, mas *não* é invertível:

$$\begin{aligned} \frac{d}{dx} a_0 + a_1 x &= a_1 \\ \frac{d}{dx} b_0 + a_1 x &= a_1 \\ \frac{d}{dx} c_0 + a_1 x &= a_1 \\ &\vdots \end{aligned}$$

e portanto não temos um único polinômio tal que $d/dx\ p(x) = a_1$. ◀

Teorema 3.28. *Seja* $T : V \to U$ *uma transformação linear invertível. Então* T^{-1} *é também linear.*

Demonstração. Sejam $\mathbf{v}_1, \mathbf{v}_2 \in V$. Como T é invertível, existem $\mathbf{w}_1, \mathbf{w}_2 \in U$ tais que $T(\mathbf{v}_1) = \mathbf{w}_1$ e $T(\mathbf{v}_2) = \mathbf{w}_2$. Verificamos a multiplicação por escalar:

$$\begin{aligned} T^{-1}(c\mathbf{w}_1) &= T^{-1}(cT(\mathbf{v}_1)) \\ &= T^{-1}(T(c\mathbf{v}_1)) \\ &= c\mathbf{v}_1 \\ &= cT^{-1}(\mathbf{w}_1). \end{aligned}$$

E verificamos também a soma de vetores:

$$\begin{aligned} T^{-1}(\mathbf{w}_1 + \mathbf{w}_2) &= T^{-1}(T(\mathbf{v}_1) + T(\mathbf{v}_2)) \\ &= T^{-1}(T(\mathbf{v}_1 + \mathbf{v}_2)) && \text{(T é linear)} \\ &= \mathbf{v}_1 + \mathbf{v}_2 \\ &= T^{-1}(\mathbf{w}_1) + T^{-1}(\mathbf{w}_2). \end{aligned}$$

■

Exemplo 3.29. A transformação que rotaciona vetores em $\mathbb{R}^2$ por um ângulo θ tem como inversa a rotação por $-\theta$, que também é linear. ◀

Exemplo 3.30. A transformação $T : \mathbb{R}^4 \to \mathbb{R}_3[x]$, com

$$T[(a, b, c, d)^T] = 3ax^3 + 2bx^2 + cx - d$$

é uma bijeção, e sua inversa é

$$T^{-1}(px^3 + qx^2 + rx + s) = \left(\frac{p}{3}, \frac{q}{2}, r, -s\right)^T. \qquad \blacktriangleleft$$

O exercício 64 pede a demonstração da proposição a seguir, que determina a inversa de uma composição.

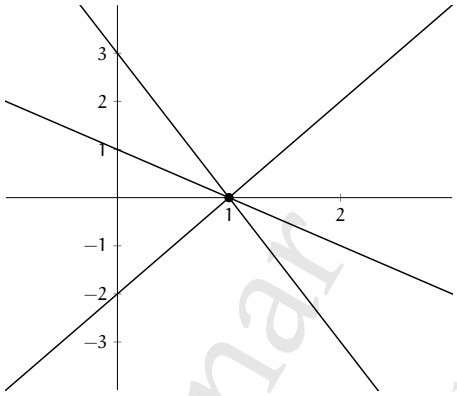
Proposição 3.31. *Se T e S são invertíveis e a composição $S \circ T$ é definida, então*

$$(S \circ T)^{-1} = T^{-1} \circ S^{-1}.$$

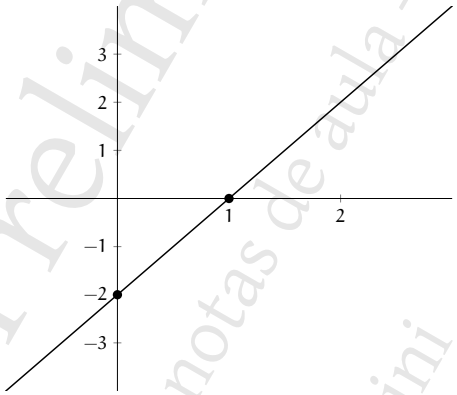
3.1 O efeito em uma base determina completamente uma transformação

No exemplo 3.9 desenvolvemos uma transformação linear que realiza a rotação de vetores no plano. Inicialmente, determinamos o efeito que queríamos na base canônica $\{\mathbf{e}_1, \mathbf{e}_2\}$, e com isso determinamos completamente a transformação. Aquele exemplo ilustra o que o próximo teorema nos garante: *uma transformação linear $T : V \to U$ é completamente caracterizada pelo seu efeito em uma base de V.*

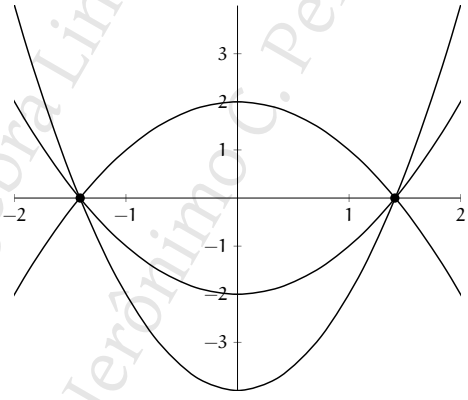
Podemos fazer uma analogia com polinômios: se quisermos determinar as retas $ax + b$ que passam por um ponto dado, teremos infinitas delas. Se tivermos dois pontos, há somente uma reta passando por eles, e sabemos como calcular sua equação. Por exemplo, se tomarmos o ponto $(1, 0)$, há infinitas retas passando por ele. A seguir mostramos tres delas, $2x - 2, -x + 1, -3x + 3$.



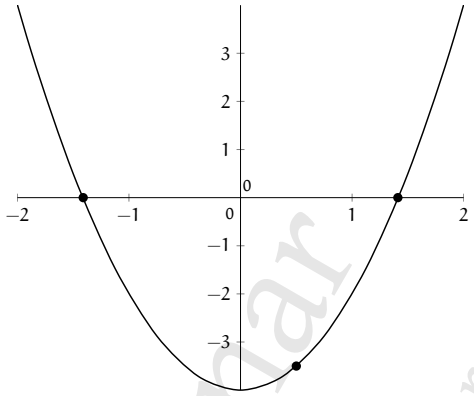
Se fixarmos um segundo ponto, $(0, -2)$, somente uma das retas passará por eles, e sabemos que é a reta $2x - 2$.



Da mesma forma, se tivermos dois pontos no plano, haverá infinitas parábolas $ax^2 + bx + c$ passando por eles. Por exemplo, há infinitas parábolas passasndo por $(-\sqrt{2}, 0)$ e $(+\sqrt{2}, 0)$. Na figura a seguir mostramos tres delas: $x^2 - 2$, $-x^2 + 2$, e $2x^2 - 4$.



Se fixarmos um terceiro ponto, $(1/2, -7/2)$, somente a parábola $2x^2 - 4$ passará por todods eles.



Semelhantemente, com $n+1$ pontos determinamos completamente um polinômio de grau n.

O teorema a seguir nos garante exatamente o mesmo, mas para transformações lineares: conhecendo uma base $\mathbf{v}_1, \ldots, \mathbf{v}_n$ e os valores de $T(\mathbf{v}_i)$ para seus vetores, podemos ter certeza de que há *exatamente uma* transformação $T : V \to U$ que mapeie $v_i \mapsto T(\mathbf{v}_i)$.

Teorema 3.32. *Sejam U e V espaços vetoriais de dimensão finita; $B_V = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ uma base ordenada de V; e $\mathbf{u}_1, \mathbf{u}_2, \ldots \mathbf{u}_n$ vetores em U. Então existe uma única transformação $T : V \to U$ tal que $T(\mathbf{v}_i) = \mathbf{u}_i$.*

Demonstração. Um vetor qualquer $\mathbf{v} \in V$ pode ser descrito como combinação linear dos vetores em B_V:

$$\mathbf{v} = \sum_i a_i \mathbf{v}_i.$$

Com os coeficientes a_i usados para descrever $\mathbf{v}$ podemos determinar a transformação T.

$$\begin{aligned} T(\mathbf{v}) &= T\left(\sum_i a_i \mathbf{v}_i\right) \\ &= \sum_i a_i T(\mathbf{v}_i) && \text{(pelo Teorema 3.12)} \\ &= \sum_i a_i \mathbf{u}_i. && \text{(porque } T(\mathbf{v}_i) = \mathbf{u}_i\text{)} \end{aligned}$$

Temos portanto uma transformação $T : V \to U$ com

$$T(\mathbf{v}) = \sum a_i \mathbf{u}_i,$$

onde os a_i são as coordenadas de $\mathbf{v}$ na base B_V.

Com isto já identificamos completamente a transformação T.

Nos falta, agora, mostrar o que dissemos no enunciado: (i) que de fato T mapeia os $\mathbf{v}_i$ nos $\mathbf{u}_i$; (ii) que T é linear; e (iii) que T é única.

Primeiro verificamos (i), que $T(\mathbf{v}_i)$ é de fato igual a $\mathbf{u}_i$:

$$T(\mathbf{v}_i) = 0\mathbf{u}_1 + 0\mathbf{u}_2 + \ldots + a_i\mathbf{u}_i + \ldots + 0\mathbf{u}_n,$$

e portanto $T(\mathbf{v}_i) = \mathbf{u}_i$.

Assim, obtemos uma transformação T de V em U que mapeia corretamente os vetores $\mathbf{v}_i$ nos vetores $\mathbf{u}_i$.

Agora mostramos (ii), que T é linear. Sejam $\mathbf{v}, \mathbf{w} \in V$ tais que

$$\mathbf{v} = \sum_i a_i \mathbf{v}_i$$
$$\mathbf{w} = \sum_i b_i \mathbf{v}_i.$$

Então

$$\begin{aligned} T(\mathbf{v}+\mathbf{w}) &= T\left[\sum_i (a_i\mathbf{v}_i + b_i\mathbf{v}_i)\right] = T\left(\sum_i (a_i+b_i)\mathbf{v}_i\right) \\ &= \sum_i (a_i+b_i)\mathbf{u}_i = \sum_i a_i\mathbf{u}_i + \sum_i b_i\mathbf{u}_i \\ &= \left(\sum_i a_i\mathbf{v}_i\right) + \left(\sum_i b_i\mathbf{v}_i\right) = T(\mathbf{v}) + T(\mathbf{w}). \end{aligned}$$

e

$$\begin{aligned} T(k\mathbf{v}) &= T\left[k\sum_i (a_i\mathbf{v}_i)\right] = T\left[\sum_i (ka_i\mathbf{v}_i)\right] \\ &= \sum_i ka_i\mathbf{u}_i = k\sum_i a_i\mathbf{u}_i = kT(\mathbf{v}). \end{aligned}$$

Finalmente mostramos (iii) – que T é única. Suponha que $R : V \to U$ seja linear, e que R também mapeie os vetores $\mathbf{v}_i$ nos vetores $\mathbf{u}_i$, ou seja, $R(\mathbf{v}_i) = \mathbf{u}_i$. Seja $\mathbf{v} \in V$, com $\mathbf{v} = \sum a_i\mathbf{v}_i$.

$$R(\mathbf{v}) = \sum a_i R(\mathbf{v}_i) = \sum a_i\mathbf{u}_i = T(\mathbf{v}),$$

e R deve ser igual a T. ■

Podemos determinar completamente uma transformação se soubermos o efeito da transformação na base canônica.

Exemplo 3.33. Suponha que precisemos definir a transformação de $\mathbb{R}^3$ em $\mathbb{R}^2$ tal que

$$T(\mathbf{e}_1) = (4,8)^T$$
$$T(\mathbf{e}_2) = (1,0)^T$$
$$T(\mathbf{e}_3) = (-1,7)^T.$$

Observamos $B = \{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ é base de $\mathbb{R}^3$.

Para todo $\mathbf{v} \in \mathbb{R}^3$, com $\mathbf{v} = (x,y,z)^T$, temos uma representação de $\mathbf{v}$ na base B). Calculamos então $[(x,y,z)]B$.

$$T(\mathbf{v}) = T(x,y,z) = T(x\mathbf{e}_1 + y\mathbf{e}_2 + z\mathbf{e}_3) \qquad \text{(T é linear)}$$

$$\begin{aligned}
&= xT(\mathbf{e}_1) + yT(\mathbf{e}_2) + zT(\mathbf{e}_3)\\
&= x(4,8)^T + y(1,0)^T + z(-1,7)^T\\
&= (4x + y - z, 8x + 7z)^T,
\end{aligned}$$

e com isso determinamos T. ◀

Podemos conseguir o mesmo usando uma base diferente da canônica, como mostra o exemplo a seguir. Lembramos que *qualquer* conjunto de n vetores L.I. é base para um espaço de dimensão n.

Exemplo 3.34. Queremos definir a transformação de $\mathbb{R}^3$ em $\mathbb{R}^2$ tal que

$$\begin{aligned}
T(1,2,0) &= (1,5)^T\\
T(0,-1,0) &= (0,-1)^T\\
T(2,0,1) &= (2,4)^T.
\end{aligned}$$

O conjunto $B = (1,2,0), (0,-1,0), (2,0,1)$ é L.I., e portanto é base de $\mathbb{R}^3$.

Dado $\mathbf{v} \in \mathbb{R}^3$, com $\mathbf{v} = (x,y,z)^T$, determinamos sua representação na base B:

$$(x,y,z) = a_1(1,2,0) + a_2(0,-1,0) + a_3(2,0,1)$$

Para determinar a_1, a_2 e a_3, supomos x, y e z constantes e resolvemos

$$\begin{cases} a_1 + 2a_3 = x\\ 2a_1 - a_2 = y\\ a_3 = z \end{cases}$$

obtendo

$$\begin{aligned}
a_1 &= x - 2z\\
a_2 &= 2x - y - 4z\\
a_3 &= z.
\end{aligned}$$

E portanto, temos

$$\begin{aligned}
T(x,y,z) &= T\left[a_1(1,2,0) + a_2(0,-1,0) + a_3(2,0,1)\right]\\
&= a_1T(1,2,0) + a_2T(0,-1,0) + a_3T(2,0,1) && \text{(pelo Teorema 3.12)}\\
&= a_1(1,5) + a_2(0,-1) + a_3(2,4)\\
&= (x-2z)(1,5) + (2x-y-4z)(0,-1) + z(2,4)\\
&= (x-2z, 5x-10z) + (0,-2x+y+4z) + (2z,4z)\\
&= (x, 3x+y-2z).
\end{aligned}$$ ◀

Exemplo 3.35. Queremos definir uma transformação de $\mathbb{R}_2[x]$ em $M_{2\times 2}$ tal que

$$\begin{aligned}
T(x^2+x) &= \begin{pmatrix} 0 & 2\\ 3 & 1 \end{pmatrix}\\
T(5x^2) &= \begin{pmatrix} -1 & 0\\ 0 & -1 \end{pmatrix}
\end{aligned}$$

$$T(3) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Observamos que $\{ x^2 + x, 5x^2, 3 \}$ é base para $\mathbb{R}_2[x]$ e portanto, tendo o efeito de T sobre uma base, podemos determinar T.

Usamos o seguinte isomorfismo entre estes dois espaços com $\mathbb{R}^3$ e $\mathbb{R}^4$:

$$f(ax^2 + bx + c) = (a, b, c)^T$$
$$g\left[\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right] = (\alpha, \beta, \gamma, \delta)^T$$

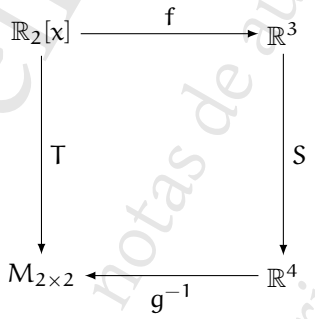
Assim, definimos $S : \mathbb{R}^2 \to \mathbb{R}^4$ como

$$S(\mathbf{v}) = g^{-1} \circ T \circ f = g^{-1}(T(f(\mathbf{v})))$$

e consequentemente,

$$T(\mathbf{w}) = f^{-1}(S^{-1}(g(\mathbf{w})),$$

como fica claro no diagrama a seguir.



Agora, como

$$f(x^2 + x) = (1, 1, 0)^T$$
$$f(5x^2) = (5, 0, 0)^T$$
$$f(3) = (0, 0, 3)^T,$$

$$g\left[\begin{pmatrix} 0 & 2 \\ 3 & 1 \end{pmatrix}\right] = (0, 2, 3, 1)^T$$
$$g\left[\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right] = (-1, 0, 0, -1)^T$$
$$g\left[\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right] = (1, 1, 1, 0)^T,$$

temos os valores de S para tres vetores,

$$S(1, 1, 0)^T = (0, 2, 3, 1)^T$$

$$S(5,0,0)^T = (-1,0,0,-1)^T$$
$$S(0,0,3)^T = (1,1,1,0)^T.$$

Todo vetor em $\mathbb{R}^3$ pode ser representado como combinação linear da base $\{\ (1,1,0)^T, (5,0,0)^T, (0,0,3)^T\ \}$, portanto

$$(p,q,r)^T = a_1(1,1,0)^T + a_2(5,0,0)^T + a_3(0,0,3)^T$$

Resolvemos então

$$\begin{cases} a_1 + 5a_2 = p \\ a_1 = q \\ 3a_3 = r \end{cases}$$

e obtemos

$$\begin{aligned} a_1 &= q \\ a_2 &= (p-q)/5 \\ a_3 &= r/3. \end{aligned}$$

Finalmente, podemos determinar a expressão geral de $S(p,q,r)$.

$$\begin{aligned} S(p,q,r)^T &= S\left[a_1\begin{pmatrix}1\\1\\0\end{pmatrix} + a_2\begin{pmatrix}5\\0\\0\end{pmatrix} + a_3\begin{pmatrix}0\\0\\3\end{pmatrix}\right] \\ &= a_1 S\begin{pmatrix}1\\1\\0\end{pmatrix} + a_2 S\begin{pmatrix}5\\0\\0\end{pmatrix} + a_3 S\begin{pmatrix}0\\0\\3\end{pmatrix} \qquad \text{(pelo Teorema 3.12)} \\ &= a_1\begin{pmatrix}0\\2\\3\\1\end{pmatrix} + a_2\begin{pmatrix}-1\\0\\0\\-1\end{pmatrix} + a_3\begin{pmatrix}1\\1\\1\\0\end{pmatrix} \\ &= q\begin{pmatrix}0\\2\\3\\1\end{pmatrix} + \frac{p-q}{5}\begin{pmatrix}-1\\0\\0\\-1\end{pmatrix} + \frac{r}{3}\begin{pmatrix}1\\1\\1\\0\end{pmatrix} \\ &= \begin{pmatrix}0\\2q\\3q\\q\end{pmatrix} + \begin{pmatrix}(q-p)/5\\0\\0\\(q-p)/5\end{pmatrix} + \begin{pmatrix}r/3\\r/3\\r/3\\0\end{pmatrix} \\ &= \begin{pmatrix}r/3+(q-p)/5\\r/3+2q\\r/3+3q\\q+(q-p)/5\end{pmatrix} \\ &= \begin{pmatrix}r/3+(q-p)/5\\r/3+2q\\r/3+3q\\(6q-p)/5\end{pmatrix} \end{aligned}$$

Expressando a transformação como $T : \mathbb{R}_2[x] \to M_{2\times 2}$,

$$T(px^2 + qx + r) = \begin{pmatrix} r/3 + (q-p)/5 & 2q + r/3 \\ 3q + r/3 & (6q-p)/5 \end{pmatrix}. \quad \blacktriangleleft$$

3.2 Kernel e imagem

O *kernel* de uma transformação linear é análogo ao conceito de raízes de uma função[2].

Definição 3.36 (Kernel de uma transformação)**.** Seja $T : V \to U$ uma transformação linear. Então $\ker(T) = \{\mathbf{v} \in V : T(\mathbf{v}) = \mathbf{0}\}$ é o *kernel*[3] (ou *núcleo*) de T. ♦

Definição 3.37 (Imagem de uma transformação)**.** Seja $T : V \to U$ uma transformação linear. Então $\mathrm{Im}(T) = \{T(\mathbf{v}) : \mathbf{v} \in V\}$ é a *imagem* de T. ♦

Exemplo 3.38. Considere a transformação linear $T : \mathbb{R}^2 \to \mathbb{R}^2$ definida a seguir.

$$T[(x, y)^T] = (x + y, y - x)^T$$

O kernel de T é o conjunto dos vetores com $T(\mathbf{v}) = \mathbf{0}$, ou seja,

$$\ker(T) = \left\{ (x, y)^T : \ x + y = 0 \text{ e } y - x = 0 \right\}.$$

Para $x + y = 0$ e $y - x = 0$ há uma única solução, com $x = y = 0$, e portanto $\ker(T) = \{(0, 0)^T\} = \{\mathbf{0}\}$. ◀

Exemplo 3.39. A transformação $T : \mathbb{R}^2 \to \mathbb{R}^2$ dada por

$$T(x, y)^T = (x, 2x)^T$$

A imagem de T é $\{ (x, 2x) : \ x \in \mathbb{R} \}$.

$T(\mathbf{v})$ resultará em $(0, 0)^T$ para todo vetor $\mathbf{v} = (0, y)^T$, e portanto o kernel de T é

$$\ker(T) = \left\{ (0, y)^T : \ y \in \mathbb{R} \right\} \quad \blacktriangleleft$$

Exemplo 3.40. A operação de rotação em $\mathbb{R}^2$ tem como imagem o próprio $\mathbb{R}^2$, porque todo vetor pode ser resultado da rotação de outro. Além disso, o kernel desta operação é $\{ \mathbf{0} \}$, porque somente a origem $(0, 0)^T$, quando rotacionada, resulta novamente na origem. ◀

Exemplo 3.41. Mencionamos que a derivada é uma transformação linear no espaço das funções deriváveis. O kernel desta transformação é o conjunto de funções que tem a derivada igual a zero – ou seja, o conjunto de todas as funções constantes. ◀

[2] As raízes de uma função f são os pontos x de seu domínio tais que $f(x) = 0$. Por exemplo, se $f(x) = x^2 - 4$, as raízes de f são $+2$ e -2.

[3] Em Álgebra Linear, o *kernel* é o conjunto de elementos que levam em zero. De maneira mais abstrata, pode-se dizer que é o conjunto que leva ao elemento neutro. Para certas funções definidas em grupos, o *kernel* é $\{x \in G : f(x) = 1\}$.

Exemplo 3.42. Considere a transformação $T : \mathbb{R}_2[x] \to C^0$, definida a seguir.

$$T(a_2x^2 + a_1x + a_0) = a_2 \operatorname{sen}^2(x) + a_1 \cos^2(x) + a_0$$

A imagem de T é a de todas as combinações lineares das funções $\operatorname{sen}^2(x)$, $\cos^2(x)$ e $f(x) = 1$.

O kernel de T é composto pelos vetores que levam à função zero, ou seja, nas funções $g(x)$ tais que

$$g(x) = a_2 \operatorname{sen}^2(x) + a_1 \cos^2(x) + a_0 = 0$$

Como isto deve valer para *todo* x, devemos presumir que $\operatorname{sen}^2(x) > 0$ e $\cos^2(x) > 0$, e como seno e cosseno e $f(x) = 1$ são LI, $g(x)$ só é zero quando

$$a_1 = a_2 = -a_0,$$

e portanto o kernel de T é composto dos polinômios da forma

$$p(x) = ax^2 + ax - a. \qquad \blacktriangleleft$$

Exemplo 3.43. Seja f definida em $M_{n\times n}$ da seguinte maneira: a matriz A é transformada em outra matriz B, onde cada elemento b_{ii} da diagonal de B é igual à soma da linha i menos a soma da coluna i, e os elementos de B fora da diagonal são zero. O exercício 69 pede a demonstração de que f é linear.

$$f\begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 4 & 3 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

A imagem de f é o conjunto das matrizes diagonais $n \times n$.

O kernel de f é o conjunto das matrizes onde o somatório de cada i-ésima linha é igual ao da i-ésima coluna. $\blacktriangleleft$

Teorema 3.44. *Seja* $T : V \to U$ *uma transformação linear. Então* $\ker(T)$ *é subespaço de* V *e* $\operatorname{Im}(T)$ *é subespaço de* U*.*

Demonstração. Temos $\ker(T) \subseteq V$ e $\operatorname{Im}(T) \subseteq U$, portanto precisamos demonstrar apenas que $\mathbf{0}$ está em ambos os conjuntos, e que são fechados sob multiplicação por escalar e adição.

(ker, i) *O zero está no núcleo de* T. Claramente é verdade, porque $T(\mathbf{0}) = \mathbf{0}$.

(ker, ii) *A multiplicação por escalar é fechada em* $\ker T$. Mostraremos que um vetor do núcleo de T, quando multiplicado por escalar, continua em $\ker T$.

Suponha que $\mathbf{v} \in \ker T$, ou seja,

$$T(\mathbf{v}) = \mathbf{0}.$$

Se multiplicarmos os dois lados por c, temos

$$\begin{aligned} cT(\mathbf{v}) &= c\mathbf{0} \\ cT(\mathbf{v}) &= \mathbf{0} && \text{(em todo espaço vetorial, } c\mathbf{v} = \mathbf{0}) \\ T(c\mathbf{v}) &= \mathbf{0} && \text{(T é linear)} \end{aligned}$$

Mas a última linha significa que $c\mathbf{v}$ está no núcleo de T.

(ker, iii) *A soma de vetores é fechada em* $\ker T$. Mostraremos que, dados dois vetores no núcleo de T, sua soma também é parte de $\ker T$.

Suponha que $\mathbf{v}, \mathbf{w} \in \ker T$, ou seja,

$$\begin{aligned} T(\mathbf{v}) &= \mathbf{0}, \\ T(\mathbf{w}) &= \mathbf{0}. \end{aligned}$$

Então

$$\begin{aligned} T(\mathbf{v}+\mathbf{w}) &= T(\mathbf{v}) + T(\mathbf{w}) && \text{(porque T é linear)} \\ &= \mathbf{0} + \mathbf{0} \\ &= \mathbf{0}, \end{aligned}$$

o que significa que $\mathbf{v} + \mathbf{w}$ está no núcleo de T.

Agora tratamos da imagem.

(Im, i) *O zero está na imagem de* T. Claramente é verdade, porque $T(\mathbf{0}) = \mathbf{0}$.

(Im, ii) *A multiplicação por escalar é fechada em* Im T. Mostraremos que um vetor da imagem de T, quando multiplicado por escalar, continua na imagem de T.

Seja c um escalar, e suponha que $\mathbf{w} \in \operatorname{Im} T$, ou seja,

$$T(\mathbf{v}) = \mathbf{w}, \quad \text{para algum } \mathbf{v} \in V$$

Como $\mathbf{v} \in V$, e V é espaço vetorial, então $c\mathbf{v} \in V$. Mas isto imediatamente nos permite escrever

$$\begin{aligned} T(c\mathbf{v}) &= cT\mathbf{v} \\ &= c\mathbf{w}. \end{aligned}$$

Assim, se $\mathbf{w} \in \operatorname{Im} T$, então $c\mathbf{w} \in \operatorname{Im} T$.

(Im, iii) *A soma de vetores é fechada em* Im T. Mostraremos que, dados dois vetores na imagem de T, sua soma também é parte de Im T.

Suponha que $\mathbf{w}, \mathbf{z} \in \operatorname{Im} T$, ou seja,

$$\begin{aligned} T(\mathbf{v}) &= \mathbf{w}, \quad \text{para algum } \mathbf{v} \in V \\ T(\mathbf{u}) &= \mathbf{z}, \quad \text{para algum } \mathbf{u} \in V \end{aligned}$$

Então

$$\begin{aligned} T(\mathbf{v}+\mathbf{u}) &= T(\mathbf{v}) + T(\mathbf{u}) \\ &= \mathbf{w} + \mathbf{z} \end{aligned}$$

o que significa que $\mathbf{w} + \mathbf{z}$ é imagem de $\mathbf{u} + \mathbf{v}$ – ou seja, a soma $\mathbf{w} + \mathbf{z}$ está na imagem de T. ■

Exemplo 3.45. A transformação $T : \mathbb{R}^3 \to \mathbb{R}^3$ com $T(x, y, z)^T = (x, x + y + z, 2x)^T$ tem como imagem, evidentemente, os vetores da forma $(x, x + y + z, 2x)^T$ (estes formam um plano). O kernel desta transformação é composto pelos vetores com $x = 0$ e $y + z = 0$ (é uma reta). Os dois (uma reta e um plano, ambos passando pela origem) são espaços vetoriais. Mais rigorosamente, temos:

- Ambos são subconjuntos de $\mathbb{R}^3$.
- $(0, 0, 0)^T \in \ker T$, e $(0, 0, 0)^T \in \operatorname{Im} T$.

- Im T é fechada sob soma:

$$(x, x+y+z, 2x)^T + (x', x'+y'+z', 2x')^T = (x+x', x+x'+y+y'+z+z', 2(x+x')^T.$$

- Im T é fechada sob multiplicação por escalar:

$$c(x, x+y+z, 2x)^T = (cx, cx+cy+cz, 2cx)^T.$$

- ker T é fechado sob soma: se $T(\mathbf{v}) = (0,0,0)^T$, $T(\mathbf{u}) = (0,0,0)^T$,

$$T(\mathbf{u}+\mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v}) = (0,0,0)^T,$$

  e portanto $\mathbf{u}+\mathbf{v} \in \ker T$.

- ker T é fechado sob multiplicação por escalar: se $T(\mathbf{v}) = (0,0,0)^T$,

$$cT(\mathbf{v}) = c(0,0,0)^T = (0,0,0)^T \in \ker T$$ ◀

3.3 Nulidade e posto

Definição 3.46 (Nulidade e posto)**.** Seja T uma transformação linear entre espaços de dimensão finita. A *nulidade* de uma transformação T é a dimensão de $\ker(T)$. O *posto* de T é a dimensão de $\mathrm{Im}(T)$. ♦

Exemplo 3.47. Seja $T : \mathbb{R}^3 \to \mathbb{R}^3$, definida a seguir.

$$T(x, y, z)^T = (x, y, x+y)^T.$$

A imagem desta transformação é um plano, contendo vetores da forma $(x, y, x+y)^T$. Uma base para este plano é

$$B_I = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\}.$$

Como a base da imagem tem dois vetores, o posto de T é dois.

O núcleo de T é composto pelos vetores $\mathbf{v}$ tais que $T(\mathbf{v}) = \mathbf{0}$, ou seja,

$$T \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Ou seja,

$$\begin{aligned} x &= 0 \\ y &= 0 \\ x+y &= 0 \end{aligned}$$

Estes são os vetores da forma $(0,0,z)^T$ – uma reta. Uma base para o núcleo é, portanto,

$$B_N = \left\{ \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}.$$

Como a base do núcleo tem um único vetor, a dimensão do núcleo é um. ◀

Exemplo 3.48. O exemplo 3.9 mostra a transformação que realiza rotação de vetores em $\mathbb{R}^2$. O kernel da transformação contém somente o vetor zero, porque qualquer outro vetor em $\mathbb{R}^2$, quando rotacionado, resulta em vetor diferente de zero. Já $\mathrm{Im}(T)$ é igual a todo $\mathbb{R}^2$, porque todo vetor pode ser obtido como rotação de outro.

Como o kernel de T é $\{\,\mathbf{0}\,\}$, sua nulidade T é zero. O posto de T é dois (a dimensão de $\mathbb{R}^2$). ◀

Exemplo 3.49. O exemplo 3.5 mostra que a derivada em $\mathbb{R}_n[x]$ é transformação linear. A imagem desta transformação é $\mathbb{R}_{n-1}[x]$, e o kernel é o conjunto das funções constantes (que são as que tem derivada zero).

A nulidade da transformação é um (porque a imagem pode ser gerada a partir de um único vetor, a função constante $f(x) = 1$). O posto é n (a dimensão da imagem, $\mathbb{R}_{n-1}[x]$). ◀

Exemplo 3.50. Considere o operador derivada segunda, d^2/dx^2, no espaço $\mathbb{R}_4[x]$. Para um polinômio qualquer deste espaço, temos

$$\frac{d^2}{dx^2}\left(a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0\right) = 12a_4x^2 + 6x_3 + 2a_2.$$

A imagem de d^2/dx^2 é composta, portanto, de polinômios de grau no máximo dois. Uma base para a imagem é

$$B_I = \{1, x, x^2\},$$

e portanto o posto de d^2/dx^2 é tres.

Já o núcleo deste operador é composto pelos polinômios que são transformados no polinômio zero. Estes são, claro, os de grau no máximo um, ou seja, os da forma

$$a_1x + a_0.$$

Uma base para o núcleo é portanto

$$B_N = \{1, x\},$$

e a nulidade de d^2/dx^2 é dois. ◀

Teorema 3.51 (do núcleo e da imagem)**.** *Sejam V e U espaços vetoriais de dimensão finita e $T : V \to U$ uma transformação linear. Então a soma da nulidade com o posto de T é igual à dimensão de V - ou seja,* $\dim \mathrm{Im}(T) + \dim \ker(T) = \dim V$.

Demonstração. Seja $\{\,\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\,\}$ uma base para $\ker(T)$ com k vetores. Podemos completar esta base para formar uma base

$$\{\,\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k, \mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_m\,\}$$

para V. Temos então

$$\dim \ker(T) = k$$
$$\dim V = k + m.$$

Para mostrar que $\dim \mathrm{Im}(T) = m$, mostraremos que o conjunto $\{\,T\mathbf{w}_1, T\mathbf{w}_2, \ldots, T\mathbf{w}_m\,\}$ é uma base para $\mathrm{Im}(T)$.

Todo vetor $\mathbf{v} \in V$ é combinação linear de vetores da base de V, portanto

$$\mathbf{v} = a_1\mathbf{u}_1 + \ldots + a_k\mathbf{u}_k + b_1\mathbf{w}_1 + \ldots + b_m\mathbf{w}_m$$

$$\begin{aligned} T\mathbf{v} &= a_1T(\mathbf{u}_1) + \ldots + a_kT(\mathbf{u}_k) + b_1T(\mathbf{w}_1) + \ldots + b_mT(\mathbf{w}_m) \\ &= b_1T(\mathbf{w}_1) + \ldots + b_mT(\mathbf{w}_m). \qquad (\text{porque } T(\mathbf{u}_i = \mathbf{0})) \end{aligned}$$

As duas últimas linhas acima mostram que todo vetor $T(\mathbf{v})$ é combinação linear dos vetores $T(\mathbf{w}_i)$, e portanto mostramos que os vetores $T(\mathbf{w}_i)$ geram a imagem de T. Para que formem uma base, resta mostrar que são um conjunto L.I[4].

Considere agora uma combinação linear qualquer de vetores $T\mathbf{w}_i$, e suponha que ela seja igual a zero:

$$c_1T(\mathbf{w}_1) + \ldots + c_mT(\mathbf{w}_m) = \mathbf{0}.$$

Mostraremos a seguir que isso implica em todos os c_i serem iguais a zero – e portanto o conjunto dos $T\mathbf{w}_i$ é L.I.

Como T é linear, podemos reescrever a equação na forma a seguir.

$$T(c_1\mathbf{w}_1 + \ldots + c_m\mathbf{w}_m) = \mathbf{0}$$

Ou seja, $\mathbf{w} = c_1\mathbf{w}_1 + \ldots + c_m\mathbf{w}_m \in \ker(T)$.

O kernel de T é gerado pelos $\mathbf{u}_i$, portanto $\mathbf{w}$, estando no kernel, é combinação linear dos $\mathbf{u}_i$:

$$\begin{aligned} \mathbf{w} &= c_1\mathbf{w}_1 + \ldots + c_m\mathbf{w}_m \\ \mathbf{w} &= z_1\mathbf{u}_1 + z_2\mathbf{u}_2 + \ldots + z_k\mathbf{u}_k. \end{aligned}$$

ou seja,

$$(c_1\mathbf{w}_1 + \ldots + c_m\mathbf{w}_m) = (z_1\mathbf{u}_1 + z_2\mathbf{u}_2 + \ldots + z_k\mathbf{u}_k)$$

O que é o mesmo que

$$(c_1\mathbf{w}_1 + \ldots + c_m\mathbf{w}_m) + (-z_1\mathbf{u}_1 - z_2\mathbf{u}_2 - \ldots - z_k\mathbf{u}_k) = \mathbf{0}.$$

No entanto, os $\mathbf{w}_i$ e $\mathbf{u}_i$ formam base para V, e são todos L.I. – e todos os c_i e z_i acima devem necessariamente ser iguais a zero. Desta forma, como os c_i devem ser zero, os vetores $T(\mathbf{w}_i)$ são L.I.

Como mostramos que a imagem de T tem uma base com m vetores, temos $\dim \mathrm{Im}(T) = m$. ■

Exemplo 3.52. O exemplo 3.39 mostra a transformação $T(x, y)^T = (x, 2x)^T$ em $\mathbb{R}^2$, com $\ker(T) = \{(0, y)^T : y \in \mathbb{R}\}$ e $\mathrm{Im}(T) = \{(x, 2x) : \ x \in \mathbb{R}\}$.

A dimensão de $\ker(T)$ é claramente um – uma base para $\ker(T)$ poderia ser, por exemplo, o conjunto $\{(0, 1)^T\}$.

Para $\mathrm{Im}(T)$, a base pode ser $(1, 2)^T$, já que os vetores de $\mathrm{Im}(T)$ são todos múltiplos deste. Assim, $\dim \mathrm{Im}(T) = 1$. Temos então

$$\dim \ker(T) + \dim \mathrm{Im}(T) = \dim \mathbb{R}^2.$$ ◀

Exemplo 3.53. Considere a transformação $T : (x, y, z)^T = (x + y, z)$ de $\mathbb{R}^3$ em $\mathbb{R}^2$.

A imagem de T é $\mathbb{R}^2$. O kernel de T é

$$\ker(T) = \left\{ (a, -a, 0)^T : \ a \in \mathbb{R} \right\},$$

porque para que $x + y$ resulte em zero, y deve ser igual a $-x$.

o kernel de T poderia ser gerado, portanto, pela base $\{(1, -1, 0)^T\}$, e temos a nulidade de T igual a $\dim \ker(T) = 1$, e o posto de T igual a $\dim \mathrm{Im}(T) = 2$, e a soma de ambos é $\dim \mathbb{R}^3 = 3$. ◀

[4] Mostrar a independência linear destes vetores é essencial nesta demonstração, porque estamos mostrando qual é a *dimensão* da imagem. Se houvesse vetores sobrando, estaríamos superestimando a dimensão.

Exemplo 3.54. Já verificamos no exemplo 3.49 que a derivada em $\mathbb{R}_n[x]$ tem imagem igual a $\mathbb{R}_{n-1}[x]$, e seu kernel é o conjunto das funções constantes.

$$\dim \mathbb{R}_n[x] = \dim \mathbb{R}_{n-1}[x] + \dim K,$$

onde K é o conjunto das funções constantes de $\mathbb{R}$ em $\mathbb{R}$. Temos que a dimensão de K deve ser necessariamente um. De fato, podemos escrever qualquer função constante como múltipla de $f(x) = 1$, e portanto $f(x)$, um único vetor, é base para K. ◀

Exemplo 3.55. Em $M_{n\times n}$, a função que dá o *traço* (somatório da diagonal) de uma matriz é $\mathrm{Tr} : M_{n\times n} \to \mathbb{R}$. Sabemos que

$$\dim M_{n\times n} = n^2.$$

E sabemos que $\operatorname{Im}\mathrm{Tr} = \mathbb{R}$, portanto

$$\dim \operatorname{Im}\mathrm{Tr} = 1.$$

Assim, mesmo sem termos determinado o kernel de Tr, sabemos que sua dimensão é necessariamente

$$\dim \ker \mathrm{Tr} = n^2 - 1.$$

E realmente, para que $\mathrm{Tr}(A) = 0$, precisamos que

$$a_{11} + a_{22} + \cdots + a_{nn} = 0,$$

independente dos valores no resto da matriz. Podemos gerar todas estas matrizes (com traço zero) como combinação linear de $n^2 - 1$ vetores: para cada posição i, j na matriz, *exceto na posição* n, n, incluímos a matriz com $a_{ij} = 1$, e definimos a_{nn} de forma que o traço seja zero:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -\mathbf{1} \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \mathbf{0} \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & \mathbf{0} \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & \mathbf{0} \end{pmatrix},$$
$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -\mathbf{1} \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & \mathbf{0} \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & \mathbf{0} \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & \mathbf{0} \end{pmatrix}.$$

Estes oito $(3^2 - 1)$ vetores geram matrizes com traço zero. Não usamos nove vetores porque o último elemento da matriz depende de outros elementos (é zero quando a diagonal é zero, e -1 quando há 1 na diagonal).

Observe que escolhemos a posição n, n arbitrariamente. Poderíamos ter usado a posição $1, 1$ ou $2, 2$ para "compensar" o 1 em outro lugar da diagonal. Teríamos matrizes como

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -\mathbf{1} & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & \mathbf{0} & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \text{etc.}$$ ◀

Os teoremas a seguir tratam de transformações bijetoras, injetoras e sobrejetoras.

Teorema 3.56. *Uma transformação* T *é injetora se e somente se* $\ker(T) = \{\mathbf{0}\}$.

Demonstração. ($\Rightarrow$) Se T é injetora, então há um *único* $\mathbf{x}$ tal que $T(\mathbf{x}) = \mathbf{0}$. Como $\mathbf{0} \in \ker(T)$, então $\mathbf{x}$ deve ser $\mathbf{0}$, e $\ker(T) = \{\mathbf{0}\}$.

($\Leftarrow$) Suponha que $\ker(T) = \{\mathbf{0}\}$, e que há dois vetores $\mathbf{x}, \mathbf{y}$ com $T(\mathbf{x}) = T(\mathbf{y})$. Então $T(\mathbf{x} - \mathbf{y}) = \mathbf{0}$, e $\mathbf{x} - \mathbf{y} \in \ker(T)$. Mas somente $\mathbf{0} \in \ker(T)$, e portanto $\mathbf{x} - \mathbf{y} = \mathbf{0}$, e $\mathbf{x} = \mathbf{y}$ – ou seja, T é injetora. ■

Exemplo 3.57. Seja $T : \mathbb{R}^3 \to \mathbb{R}^3$ uma transformação linear tal que $T\left[(x_1, x_2, x_3)\right]^T = (2x_3, 0, 3x_1)^T$. De imediato observamos que não pode ser injetora, porque seu kernel não contém apenas o vetor zero – todos os vetores da forma $(0, k, 0)^T$ também são levados por T ao zero, e portanto também estão no kernel de T.

Podemos também expor o fato de outra forma: como há mais de um vetor tal que $T(\mathbf{v}) = 0$, há mais de um vetor levando a um único elemento do contradomínio, portanto a transformação não é injetora. ◀

Exemplo 3.58. Seja θ um ângulo. A transformação que rotaciona vetores em $\mathbb{R}^2$ por θ é injetora, porque o único vetor que pode resultar no vetor zero depois de rotacionado é o próprio vetor zero (ou seja,o kernel da transformação contém somente o zero). ◀

Exemplo 3.59. A dimensão da transformação definida pelo traço de matrizes quadradas é um, portanto o traço não é uma transformação injetora. De fato, é fácil construir duas matrizes com o mesmo traço. ◀

Teorema 3.60. *Seja* $T : V \to U$ *uma transformação linear.*

i) *Se* $\dim V < \dim U$, T *não é sobrejetora.*

ii) *Se* $\dim V > \dim U$, T *não é injetora.*

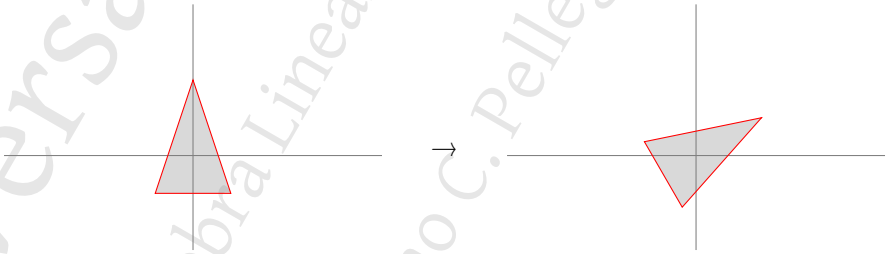
iii) *Se* $\dim V = \dim U$ *e o posto de* T *é* $\dim V$, *então* T *é bijetora.*

3.4 Aplicações

3.4.1 Transformações em imagens

Já verificamos que é possível representar a rotação de um ponto por um ângulo θ como transformação linear. Se tivermos uma imagem a ser mostrada na tela de um computador (ou de cinema), podemos realizar a transformação em cada um dos pontos – o efeito será o de transformar a imagem inteira. A figura a seguir mostra a rotação de todos os pontos de uma imagem por um ângulo de $-\pi/3$. Esta transformação é dada por

$$T\left[\begin{pmatrix} x \\ y \end{pmatrix}\right] = \begin{pmatrix} x\cos(-\pi/3) - y\,\mathrm{sen}\,(-\pi/3) \\ x\,\mathrm{sen}\,(-\pi/3) + y\cos(-\pi/3) \end{pmatrix} = \frac{1}{2}\begin{pmatrix} x + y\sqrt{3} \\ -x\sqrt{3} + y \end{pmatrix}$$

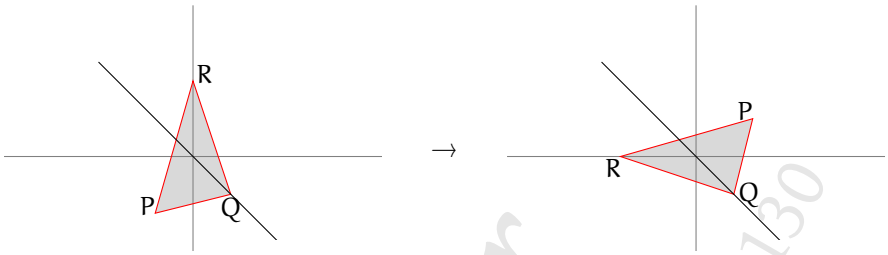


Há diversas outras transformações em $\mathbb{R}^2$ que também são importantes em Computação Gráfica. Listamos algumas delas nesta seção.

A reflexão por qualquer reta que passe pela origem é uma transformação linear. As reflexões pelas retas $y = x$, $y = -x$ e $x = 0$ são realizadas, respectivamente, pelas transformações

$$T_1\left[\begin{pmatrix} x \\ y \end{pmatrix}\right] = \begin{pmatrix} y \\ x \end{pmatrix}, \quad T_2\left[\begin{pmatrix} x \\ y \end{pmatrix}\right] = \begin{pmatrix} -y \\ -x \end{pmatrix}, \quad T_3\left[\begin{pmatrix} x \\ y \end{pmatrix}\right] = \begin{pmatrix} -x \\ y \end{pmatrix}.$$

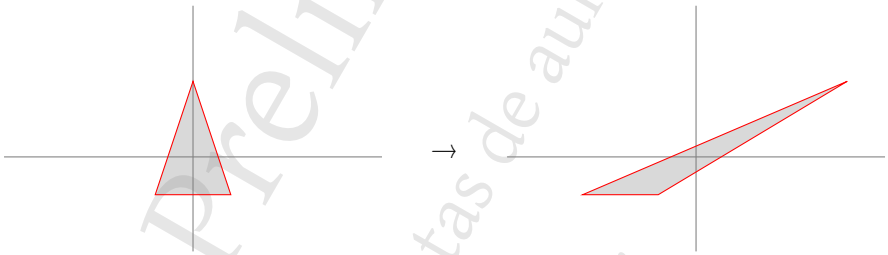
A figura a seguir ilustra a segunda delas (T_2, reflexão pela reta $y = -x$).



O *cisalhamento* também é transformação linear, que consiste em somar um múltiplo de uma das coordenadas do vetor a outra. Por exemplo,

$$T\left[\begin{pmatrix} x \\ y \end{pmatrix}\right] = \begin{pmatrix} x + 2y \\ y \end{pmatrix}$$

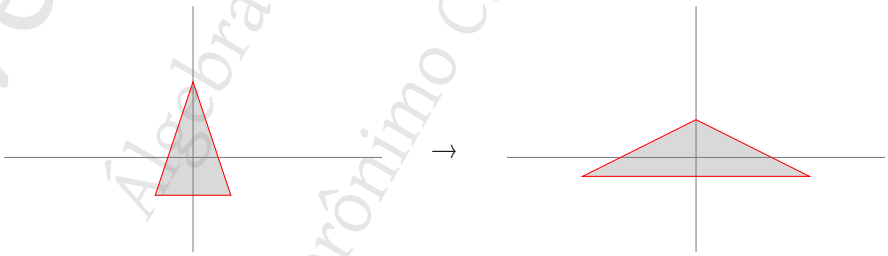
é uma operação de cisalhamento. Geometricamente, o cisalhamento realiza uma deformação como a mostrada na figura a seguir.



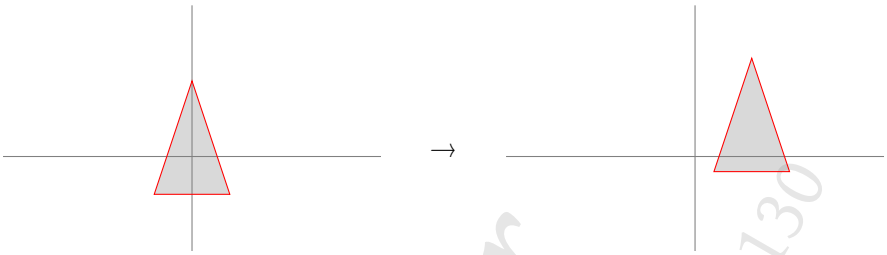
A *mudança de escala* é uma transformação linear. Se quisermos multiplicar a escala no eixo x por a e no eixo y por b, usamos a transformação

$$T\left[\begin{pmatrix} x \\ y \end{pmatrix}\right] = \begin{pmatrix} ax \\ by \end{pmatrix},$$

que é linear. Por exemplo, os pontos da figura abaixo foram modificados usando a transformação $T[(x, y)^T] = (3x, y/2)^T$.



O deslocamento por uma distância fixa é chamado de *translação*. A figura mostra uma translação da imagem do triângulo, para a direita e para cima.



A translação, no entanto, não é uma transformação linear: para deslocar um ponto em um dos eixos por uma distância k, precisaríamos realizar a transformação

$$T\left[\begin{pmatrix} x \\ y \end{pmatrix}\right] = \begin{pmatrix} x+k \\ y \end{pmatrix},$$

que não é linear (claramente, já que $T[(0,0)^T] = (k,0)^T$, levando o vetor zero a algo diferente de zero.

Apesar da translação não ser transformação linear de $\mathbb{R}^2$ em $\mathbb{R}^2$, podemos usar uma coordenada a mais para obter uma transformação *linear de* $\mathbb{R}^3$ *em* $\mathbb{R}^3$.

$$T\left[\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right] = \begin{pmatrix} x+kz \\ y \\ z \end{pmatrix},$$

E representamos todos os pontos como $(x,y,1)^T$. Assim ao invés de somar uma constante k a x, somamos um múltiplo de z (que decidimos que será sempre 1). Esta é a abordagem da Geometria Afim, descrita no Capítulo 13.

Há excelentes livros abordando a Computação Gráfica, como o de Jonas Gomes e Luiz Velho [GV08] e o de Peter Shirley, Michael Ashikhmin e Steve Marschner [SAM09].

Exercícios

Ex. 58 — Em alguns exemplos, afirmamos que certas funções são transformações lineares, mas não o demonstramos. Verifique essas afirmações (troca de coeficientes no exemplo 3.18; multiplicação de linha no exemplo 3.17).

Ex. 59 — Diga se as funções a seguir são transformações lineares.

i) $T : \mathbb{R}^3 \to \mathbb{R}^2$, tal que $T(x,y,z) = (x+y,z)$.

ii) $T : \mathbb{R}^2 \to \mathbb{C}$, com $T(x,y) = (x-y) + (x+y)i$.

iii) No espaço das funções deriváveis de $\mathbb{R}^2$ em $\mathbb{R}$,

$$T[f(x,y)] = \frac{\partial}{\partial x} f(x,y) + \int f(x,y)\ dy.$$

iv) No espaço das funções de $\mathbb{R}^2$ em $\mathbb{R}$,

$$T[f(x,y)] = \left(\frac{\partial}{\partial x} f(x,y)\right)\left(\int f(x,y)\ dy\right).$$

v) $T : M_{n\times n} \to \mathbb{R}$, com $T(A)$ igual ao produtório dos elementos da diagonal de A.

Ex. 60 — Neste Capítulo, para mostrar que uma transformação $T : V \to W$ é linear sempre mostramos primeiro que para todo c escalar e todos $\mathbf{v} \in V, \mathbf{w} \in W$, $T(\mathbf{v}+\mathbf{w}) = T(\mathbf{v})+T(\mathbf{w})$, depois que $T(c\mathbf{v}) = cT(\mathbf{v})$. Mostre que isso é o mesmo que mostrar somente que $T(c\mathbf{v} + d\mathbf{w}) = cT(\mathbf{v}) + dT(\mathbf{w})$.

Ex. 61 — Na demonstração do teorema 3.12 (na página 86) usamos o seguinte argumento: "$cT(\mathbf{0}) = T(\mathbf{0})$, o que implica em $c = 1$ ou $T(\mathbf{0}) = \mathbf{0}$". Demonstre esta afirmação.

Ex. 62 — Construa o operador em $\mathbb{R}^3$ que rotacionan um ponto por um ângulo θ ao redor da origem, mantendo a segunda coordenada fixa (o ponto $(x, y, z)^T$ é mudado para $(x', y, z')^T$). Mostre que este operador é linear.

Ex. 63 — Demonstre o teorema 3.20.

Ex. 64 — Demonstre a proposição 3.31.

Ex. 65 — Demonstre o teorema 3.60.

Ex. 66 — Demonstre o teorema 3.13.

Ex. 67 — O exemplo 3.55 mostra uma base para o espaço das matrizes 3×3 com traço zero. Mostre outra base para este espaço, onde as matrizes não tenham zeros.

Ex. 68 — Seja f uma função de mudança de base (que tem como argumento as coordenadas de um vetor em uma base B em um espaço de dimensão n, e retorna as coordenadas deste vetor em outra base B′). Determine o posto e a nulidade de f.

Ex. 69 — Mostre que a transformação f dada no exemplo 3.43 é linear.

Ex. 70 — Calcule o posto e a nulidade da transformação f, dada no exemplo 3.43.

Ex. 71 — (Difícil) Verificamos que a rotação em $\mathbb{R}^2$ é um operador linear. Em $\mathbb{A}^2$ (onde os pontos tem como coordenadas números algébricos), podemos usar o mesmo operador para rotação?

Ex. 72 — Seja $A = \left(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\right)$ uma matriz com colunas $\mathbf{a}_i$. A operação que transforma A em $\left(\mathbf{0}, \mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{n-1}\right)$ – ou seja, desloca as colunas de A para a direita – é uma transformação linear?

Ex. 73 — Levar uma matriz qualquer para a forma escalonada reduzida é uma transformação linear? Caso seja, determine sua nulidade e posto.

Ex. 74 — A mudança de coordenadas cartesianas para polares (ou a inversa, de polares para catrtesianas) é linear?

Ex. 75 — Sejam f e g transformações lineares tais que $f \circ g$ seja bem definida. Quais são o posto e a nulidade de $f \circ g$, em termos do posto e da nulidade de f e g?

Ex. 76 — Na seção 3.4.1 dissemos que o deslocamento em um eixo por uma distância fixa não é transfor-

mação linear. Mostre que isso vale para deslocamentos em qualquer direção, e não apenas um dos eixos.

Ex. 77 — No exercício 3.10 mostramos que a esperança para variáveis aleatórias discretas é transformação linear. Mostre que para variáveis aleatórias contínuas a esperança também é linear.

Ex. 78 — A mediana é uma transformação linear?

★ **Ex. 79 —** Dê um exemplo de transformação linear no espaço de ciclos de um grafo (descrito no exemplo 1.41). Descreva algebricamente e ilustre com um exemplo particular, desenhando os grafos.

Ex. 80 — No espaço C^1, a derivada é uma transformação linear injetora?

★ **Ex. 81 —** Considere o conjunto de pares de funções reais deriváveis, $C^1 \times C^1 = (f, g) \mid f, g \in C^1$.

i) Verifique que se usarmos as operações $(f, g) + (F, G) = (f + F, g + G)$ e $c(f, g) = (cf, cg)$ o resultado é um espaço vetorial.

ii) Determine a dimensão desse espaço.

iii) Determine a imagem e o kernel da transformação

$$T(f, g) = \left(\frac{d}{dx}(f + g), \frac{d^2}{dx^2} g\right)$$

definida nesse espaço.

Ex. 82 — Um operador linear f em um espaço V é *nilpotente* se existe algum inteiro k tal que $f^k(\mathbf{v}) = \mathbf{0}$, para todo $v \in V$. Mostre como construir um operador nilpotente f em um espaço de dimensão n tal que $f^{n-1}(\mathbf{v}) \neq \mathbf{0}$ para algum $\mathbf{v} \in V$, mas $f^n(\mathbf{v}) = \mathbf{0}$ para todo $\mathbf{v} \in V$. Calcule o posto de f^k para todo $1 \leq k \leq n$.

Ex. 83 — Considere transformações lineares de $\mathbb{R}^n$ em $\mathbb{R}^n$. Diga se tais transformações preservam:

i) retas (se aplicarmos a mesma transformação em todos os pontos de uma reta, o resultado será outra reta?)

ii) planos (idem, para planos)

iii) ângulos (se aplicarmos a mesma transformação em todos os pontos de duas retas, o ângulo entre elas pode mudar?)

iv) proporção entre distâncias em uma mesma reta (se aplicarmos ua mesma transformação linear em uma reta contendo pontos P, Q, R, a razão das distâncias PQ/QR muda?)

Ex. 84 — Sabemos que em $\mathcal{M}_{n\times n}$ o posto do traço é 1, e que sua nulidade é $n^2 - 1$. Determine o posto e a nulidade de $f : \mathcal{M}_{n\times n}$, com

$$f(M) = (\operatorname{Tr} M, \operatorname{Tr}' M),$$

onde $\operatorname{Tr}' M$ é o traço secundário de M (a soma dos elementos da diagonal secundária).

Capítulo 4

Matrizes e Transformações Lineares

Neste Capítulo verificamos que transformações lineares podem ser representadas como matrizes, e analisamos diversas consequências disso.

4.1 Representação de transformações como matrizes

Da mesma forma que a multiplicação de vetores de n elementos por qualquer matriz de n linhas, resultando em outro vetor de n elementos, é uma transformação linear, mostraremos que toda transformação linear de um espaço V em um espaço W, ambos de dimensão finita, pode ser descrita como matriz, de forma que a aplicação da transformação seja também descrita como multiplicação de matrizes.

Estabeleceremos portanto que matrizes $m \times n$ são *equivalentes* a transformações lineares de $\mathbb{R}^n$ em $\mathbb{R}^m$.

4.1.1 De matrizes para transformações

Começamos mostrando que toda matriz representa alguma transformação linear.

Teorema 4.1. *A multiplicação por matriz $m \times n$ é uma transformação linear de $\mathbb{R}^n$ em $\mathbb{R}^m$.*

Demonstração. Se $\mathbf{x} \in \mathbb{R}^n$, e A tem m linhas, então $A\mathbf{x}$ será um vetor com m linhas,

$$\begin{pmatrix} & \leftarrow\ n\ \rightarrow & \\ \uparrow & & \\ m & & \\ \downarrow & & \end{pmatrix} \begin{pmatrix} \uparrow \\ n \\ \downarrow \end{pmatrix} = \begin{pmatrix} \uparrow \\ m \\ \downarrow \end{pmatrix},$$

portanto é uma transformação de $\mathbb{R}^n$ em $\mathbb{R}^m$. Nos falta mostrar que é linear, mas isto é evidente por propriedades de multiplicação de matrizes: (i) $(Ac\mathbf{x}) = cA(\mathbf{x})$ e (ii) $A(\mathbf{x} + \mathbf{y}) = A\mathbf{x} + A\mathbf{y}$. ■

Exemplo 4.2. Temos a seguir uma matriz 3×2.

$$A = \begin{pmatrix} 2 & 0 \\ -3 & 2 \\ 1 & 5 \end{pmatrix}$$

Esta matriz representa uma transformação de um espaço de dimensão dois em um espaço de dimensão três:

$$A\mathbf{x} = \begin{pmatrix} 2 & 0 \\ -3 & 2 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 2x_1 \\ -3x_1 + 2x_2 \\ x_1 + 5x_2 \end{pmatrix}.$$

Note que os vetores $(x_1, x_2)^T$ e $(2x_1, -3x1 + 2x_2, x_1 + 5x_2)^T$ são vetores de *coordenadas*, e que portanto poderiam representar vetores de $\mathbb{R}^n$, $\mathbb{R}_{n-1}[x]$, ou quaisquer outros espaços com as dimensões dadas. ◀

Exemplo 4.3. A matriz

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

representa uma transformação linear de $\mathbb{Z}_2^3$ em $\mathbb{Z}_2^2$, porque a multiplicação de A por um vetor em $\mathbb{Z}_2^3$, usando as operações de $\mathbb{Z}_2$, nos dá

$$A\mathbf{x} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \oplus y \\ y \oplus z \end{pmatrix}.$$

E a função

$$T(x, y, z)^T = (x \oplus y, y \oplus z)^T$$

é linear. ◀

4.1.2 De transformações para matrizes

Já mostramos que toda matriz representa uma transformação linear. Agora mostramos a recíproca: toda transformação linear pode ser representada por uma matriz.

As funções lineares $f : \mathbb{R}^2 \to \mathbb{R}$ são todas da forma

$$f(x, y) = ax + by.$$

De maneira mais geral, as funções lineares $g : \mathbb{R}^n \to \mathbb{R}$ (ou seja, as funções com argumento vetor em $\mathbb{R}^n$ e valor em $\mathbb{R}$) são da forma

$$g(x_1, x_2, \ldots, x_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n.$$

Se $\mathbb{K}$ é um corpo, uma transformação linear de $\mathbb{K}^n$ em $\mathbb{K}$ é unicamente identificada por n coeficientes $a_1, a_2, \ldots, a_n$, de forma que

$$T(\mathbf{x}) = a_1x_1 + a_2x_2 + \cdots + a_nx_n = \sum_{i=1}^{n} a_ix_i$$

Exemplo 4.4. A média $f(x_1, x_2) = (x_1 + x_2)/2$ é linear em $\mathbb{R}^2$, e é representada por

$$a_1 = 1/2$$
$$a_2 = 1/2,$$

porque

$$a_1x_1 + a_2x_2 = \frac{x_1 + x_2}{2} = f(x_1, x_2).$$ ◀

Considere uma transformação T agindo em um vetor $\mathbf{x}$, que denotamos $T(\mathbf{x})$. Se representarmos T por um vetor linha e $\mathbf{x}$ por vetor coluna, o produto $T\mathbf{x}$ é exatamente o valor de $T(\mathbf{x})$:

$$T\mathbf{x} = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = a_1x_1 + a_2x_2 + \cdots + a_nx_n = T(\mathbf{x}).$$

Exemplo 4.5. A função $F : \mathbb{R}^3 \to \mathbb{R}$, tal que $f(x, y, z) = 2x - z$, é representada por

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

porque

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

★ **Exemplo 4.6.** A transformação $T : \mathbb{Z}_2^4 \to \mathbb{Z}_2$, dada por $T(abcd) = a \oplus b \oplus c$ é representada por

$$\begin{pmatrix} 1 & 1 & 0 & 1 \end{pmatrix},$$

porque

$$\begin{pmatrix} 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = a \oplus b \oplus d.$$

Observamos que como o corpo usado é $\mathbb{Z}_2$, as operações usadas na multiplicação de matrizes são as desse corpo. ◀

Lema 4.7. *Sejam U e V espaços vetoriais de dimensão finita, e seja $\{\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e}_n\}$ base canônica para $\mathbf{u}$. Seja também $T : U \to V$ linear. Se $T(\mathbf{u}) = \mathbf{v}$, então a i-ésima coordenada de $\mathbf{v}$ é combinação linear das coordenadas de $\mathbf{u}$. Em outras palavras, se*

$$\mathbf{u} = \sum_{j=1}^{n} u_j\mathbf{e_j}$$

então existem coeficientes q_{ij} tais que

$$v_i = \sum_{j=1}^{n} q_{ij}u_j$$

Demonstração. O vetor $\mathbf{u}$ é combinação linear da base:

$$\mathbf{u} = \sum_{j=1}^{n} u_j \mathbf{e}_j,$$

e como T é linear, temos

$$\begin{aligned} \mathbf{v} &= T(\mathbf{u}) \\ &= T\Big(\sum_{j=1}^{n} u_j \mathbf{e}_j\Big) \\ &= \sum_{j=1}^{n} u_j T(\mathbf{e}_j) \end{aligned} \tag{4.1}$$

Seja t_{ij} a i-ésima coordenada de $T(\mathbf{e}_j)$:

$$t_{ij} = \Big[T(\mathbf{e}_j)\Big]_i. \tag{4.2}$$

De 4.1 e 4.2, concluímos que

$$v_i = \sum_{j=1}^{m} u_j q_{ij}$$ ■

Exemplo 4.8. Seja $T : \mathbb{R}^3 \to \mathbb{R}^2$, com

$$T\left[\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right] = \begin{pmatrix} x - y \\ 2x + z \end{pmatrix}.$$

As coordenadas do vetor resultante ($x - y$ e $2x + z$) são evidentemente funções lineares de x, y e z. ◄

Teorema 4.9. *Sejam U e V espaços vetoriais de dimensão finita com bases canônicas A e B. Então toda transformação linear $T : U \to V$ pode ser representada na forma de uma matriz M, de forma que $T(\mathbf{u}) = \mathbf{v}$ se e somente se $M[\mathbf{u}]_A = [\mathbf{v}]_B$.*

Demonstração. Usando o Lema 4.7 para cada coordenada de $\mathbf{v}$, chegamos à fórmula de multiplicação de matriz por vetor. A i-ésima posição da multiplicação $M\mathbf{u}$ é exatamente

$$(M\mathbf{u})_i = \sum_{j=1}^{m} u_j m_{ij}.$$ ■

As figuras a seguir ilustram o conceito: cada coordenada de $\mathbf{y}$ é combinação linear dos coeficientes de $\mathbf{x}$:

$$A\mathbf{x} = \mathbf{y}$$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_i \\ \vdots \\ y_m \end{pmatrix}$$

Assim, cada coordenada pode ser representada como a multiplicação de um vetor linha pelo vetor coluna $\mathbf{x}$. Posicionado os vetores uns sobre os outros:

$$\begin{aligned} (a_{11} \quad a_{12} \quad \cdots \quad a_{1n})\,\mathbf{x} &= y_1 \\ (a_{21} \quad a_{22} \quad \cdots \quad a_{2n})\,\mathbf{x} &= y_2 \\ &\vdots \\ (a_{m1} \quad a_{m2} \quad \cdots \quad a_{mn})\,\mathbf{x} &= y_m \end{aligned}$$

chegamos a uma matriz:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \mathbf{x} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}.$$

Exemplo 4.10. A transformação $T : \mathbb{R}^3 \to \mathbb{R}^2$, dada por

$$T\left[(a, b, c)^T\right] = (a + b, b - c)^T$$

é também descrita pela matriz

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix}.$$

Aplicamos a transformação em um vetor $\mathbf{v}$ multiplicando a matriz por $\mathbf{v}$:

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} a + b \\ b - c \end{pmatrix}$$ ◀

Exemplo 4.11. No exemplo 3.9 mostramos que a transformação linear que realiza a rotação de vetores em $\mathbb{R}^2$ é

$$R \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \cos\theta - y \operatorname{sen}\theta \\ x \operatorname{sen}\theta + y \cos\theta \end{pmatrix}.$$

Esta transformação pode ser representada como uma matriz:

$$R = \begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{pmatrix}.$$

A multiplicação por R resulta na rotação do vetor pelo ângulo θ:

$$R\mathbf{v} = \begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \cos\theta - y \operatorname{sen}\theta \\ x \operatorname{sen}\theta + y \cos\theta \end{pmatrix}.$$ ◀

Exemplo 4.12. Seja $T : \mathbb{R}^4 \to \mathbb{R}^3$, com

$$T\left[(a, b, c, d)^T\right] = (a + b + c, 3d, -2a)^T.$$

A matriz que representa T é

$$M_T = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 3 \\ -2 & 0 & 0 & 0 \end{pmatrix}.$$

É fácil verificar que $M_T(a, b, c, d)^T = (a + b + c, 3d, -2a)$. ◀

Exemplo 4.13. Como qualquer espaço vetorial de dimensão finita com dimensão n é isomorfo a $\mathbb{R}^n$, dada uma transfomração $t : V \to W$, podemos usar este isomorfismo para associar:

- A transformação $t : V \to W$ com outra, $r : \mathbb{R}^n \to \mathbb{R}^m$
- Uma matriz T com a transformação t

Por exemplo, considere o operador d^2/dx^2 no espaço $\mathbb{R}_4[x]$. Usamos o isomorfismo entre $\mathbb{R}_4[x]$ e $\mathbb{R}^5$,

$$f(a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0) = (a_4, a_3, a_2, a_1, a_0)^T.$$

A derivada segunda é

$$\frac{d^2}{dx^2}(a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0) = 12a_4x^2 + 6a_3x + 2a_2$$

Como transformação de $\mathbb{R}^5$ em $\mathbb{R}^3$, esta transformação é

$$T(a_4, a_3, a_2, a_1, a_0)^T = (12a_4, 6a_3, 2a_2)^T$$

A matriz que realiza a transformação *de* $\mathbb{R}^5$ *em* $\mathbb{R}^3$ é

$$T = \begin{pmatrix} 12 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \end{pmatrix}.$$ ◀

★ **Exemplo 4.14.** Em $\mathbb{Z}_2^2$, considere a transformação

$$T(a, b) = (b, a \oplus b).$$

Esta transformação pode ser representada como matriz, de forma que

$$T(a, b) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \oplus b \end{pmatrix}.$$

Note que realizamos multiplicação de matrizes usando as operações de $\mathbb{Z}_2$ ($\wedge$ e $\oplus$) onde normalmente usaríamos $\cdot$ e $+$. ◀

4.2 Propriedades da multiplicação de matrizes

Nesta seção exploramos propriedades de multiplicação de matrizes que serão usadas no decorrer do capítulo.

4.2.1 Matrizes por blocos

Primeiro abordamos a multiplicação de matrizes por blocos.

Definição 4.15 (Partição de matriz por blocos)**.** A *partição de uma matriz por blocos* é uma partição das linhas e colunas da matriz de forma a definir *blocos* (submatrizes). ♦

Exemplo 4.16. Considere a matriz

$$A = \left(\begin{array}{ccc:cc:c} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & a_{26} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & a_{36} \\ \hdashline a_{41} & a_{42} & a_{43} & a_{44} & a_{45} & a_{46} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} & a_{56} \end{array}\right).$$

As linhas pontilhadas mostram uma possível maneira de particionar a matriz, com duas partições de linhas (uma com as linhas de 1 a 3, e outra com as linhas 4 e 5); e três partições de colunas (uma com as duas primeiras, outra com as três seguintes, e outra com a última coluna).

Podemos ver esta matriz como uma matriz de blocos

$$A = \left(\begin{array}{c:c:c} A_{11} & A_{12} & A_{13} \\ \hdashline A_{21} & A_{22} & A_{23} \end{array}\right)$$

onde

$$A_{11} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix} \quad A_{12} = \begin{pmatrix} a_{13} & a_{14} & a_{15} \\ a_{23} & a_{24} & a_{25} \\ a_{33} & a_{34} & a_{35} \end{pmatrix} \quad A_{13} = \begin{pmatrix} a_{16} \\ a_{26} \\ a_{36} \end{pmatrix}$$
$$A_{21} = \begin{pmatrix} a_{41} & a_{42} \\ a_{51} & a_{52} \end{pmatrix} \quad A_{22} = \begin{pmatrix} a_{43} & a_{44} & a_{45} \\ a_{53} & a_{54} & a_{55} \end{pmatrix} \quad A_{23} = \begin{pmatrix} a_{46} \\ a_{56} \end{pmatrix}.$$

◀

Exemplo 4.17. A matriz A a seguir está particionada. Há três partições de linhas e três de colunas.

$$A = \left(\begin{array}{cc:cc:c} 1 & -1 & 8 & 9 & 4 \\ 2 & 0 & -3 & 1 & -7 \\ \hdashline 3 & -3 & 5 & 1 & 2 \\ 0 & 2 & 1 & 0 & 0 \\ \hdashline 9 & 8 & 6 & -1 & -7 \end{array}\right) = \left(\begin{array}{c:c:c} A_{11} & A_{12} & A_{13} \\ \hdashline A_{21} & A_{22} & A_{23} \\ \hdashline A_{31} & A_{32} & A_{33} \end{array}\right),$$

onde A_{ij} é o bloco na i-ésima partição das linhas e j-ésima partição das colunas:

$$A_{11} = \begin{pmatrix} 1 & -1 \end{pmatrix} \quad A_{12} = \begin{pmatrix} 8 & 9 \end{pmatrix} \quad A_{13} = \begin{pmatrix} 4 \end{pmatrix}$$
$$A_{21} = \begin{pmatrix} 2 & 0 \end{pmatrix} \quad A_{22} = \begin{pmatrix} -3 & 1 \end{pmatrix} \quad A_{23} = \begin{pmatrix} -7 \end{pmatrix}$$
$$A_{31} = \begin{pmatrix} 3 & -3 \\ 0 & 2 \\ 9 & 8 \end{pmatrix} \quad A_{32} = \begin{pmatrix} 5 & 1 \\ 1 & 0 \\ 6 & -1 \end{pmatrix} \quad A_{33} = \begin{pmatrix} 2 \\ 0 \\ -7 \end{pmatrix}$$

As partições, como se pode notar no exemplo, não precisam ser de mesmo tamanho. ◀

Teorema 4.18. *Considere duas matrizes* A *e* B *compatíveis para multiplicação:* A *é* $m \times r$, B *é* $r \times n$.

Suponha que r colunas de A *sejam particionadas da mesma forma que as* r linhas de B *- ou seja, o mesmo número* s *de partições, e a* i*-ésima partição das colunas de* A *é do mesmo tamanho que a* i*-ésima partição das linhas de* B.

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1s} \\ A_{21} & A_{22} & & A_{2s} \\ \vdots & & \ddots & \\ A_{p1} & A_{p2} & & A_{ps} \end{pmatrix}, B = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1q} \\ A_{21} & A_{22} & & A_{2q} \\ \vdots & & \ddots & \\ A_{s1} & A_{s2} & & A_{sq} \end{pmatrix}.$$

Então podemos particionar o produto $C = AB$ *com as mesmas partições das linhas de* A *e das colunas de* B*:*

$$\begin{pmatrix} C_{11} & C_{12} & \cdots & C_{1q} \\ C_{21} & C_{22} & & C_{2q} \\ \vdots & & \ddots & \\ C_{p1} & C_{p2} & & C_{pq} \end{pmatrix}.$$

O bloco C_{ij} *pode ser calculado usando o método usual de multiplicação de matrizes, exceto que ao invés de elementos em linhas e colunas, multiplicam-se blocos em partições de linhas e partições de colunas:*

$$C_{ij} = \sum_{k=1}^{p} A_{ik} B_{kj}$$

Exemplo 4.19.

$$A = \left(\begin{array}{cc:c:c} 1 & 0 & 1 & 0 \\ 2 & 1 & -2 & -1 \\ \hdashline 3 & -3 & -3 & 1 \\ -3 & 3 & -3 & 5 \end{array}\right) \quad B = \left(\begin{array}{c:ccc:cc} 2 & 3 & 1 & 2 & 0 & 1 \\ -2 & 1 & 4 & 10 & 1 & 0 \\ \hdashline 0 & -3 & 0 & -1 & 1 & -1 \\ 0 & 8 & 2 & 1 & 4 & 3 \end{array}\right)$$

A matriz C particionada será

$$C = \left(\begin{array}{c:c:c} C_{11} & C_{12} & C_{13} \\ \hdashline C_{21} & C_{22} & C_{23} \end{array}\right)$$

O bloco C_{22} é

$$\begin{aligned} C_{22} &= A_{21}B_{12} + A_{22}B_{22} + A_{23}B_{32} \\ &= \begin{pmatrix} 3 & -3 \\ -3 & 3 \end{pmatrix} \begin{pmatrix} 3 & 1 & 2 \\ 1 & 4 & 10 \end{pmatrix} + \begin{pmatrix} -3 \\ -3 \end{pmatrix} \begin{pmatrix} -3 & 0 & -1 \end{pmatrix} + \begin{pmatrix} 1 \\ 5 \end{pmatrix} \begin{pmatrix} 8 & 2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 6 & -9 & -24 \\ -6 & 9 & 24 \end{pmatrix} + \begin{pmatrix} 9 & 0 & 3 \\ 9 & 0 & 3 \end{pmatrix} + \begin{pmatrix} 8 & 2 & 1 \\ 40 & 10 & 5 \end{pmatrix} = \begin{pmatrix} 23 & -7 & -20 \\ 43 & 19 & 32 \end{pmatrix} \end{aligned}$$

◀

Definição 4.20 (Matriz diagonal de blocos)**.** Uma matriz particionada em blocos é *diagonal por blocos* se somente os blocos da posição (i, i) são diferentes de zero. ♦

Exemplo 4.21. Sejam

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 5 & 5 & 5 \\ 5 & 0 & 5 \\ 5 & 5 & 5 \end{pmatrix}.$$

Então

$$\operatorname{diag}(A, \mathcal{I}_2, B) = \left(\begin{array}{cc:c:ccc} 1 & 1 & & & & \\ 2 & 2 & & & & \\ \hdashline & & 1 & & & \\ & & & 1 & & \\ \hdashline & & & & 5 & 5 & 5 \\ & & & & 5 & 0 & 5 \\ & & & & 5 & 5 & 5 \end{array}\right),$$

onde as entradas ausentes são zero. ◀

Exemplo 4.22. A seguinte matriz,

$$\left(\begin{array}{cc:cc:ccc} 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 & 1 & 0 & 4 \\ 5 & 0 & 2 & 0 & 1 & 0 & 4 \end{array}\right),$$

não é diagonal por blocos, porque todos os blocos na última linha tem elementos diferentes de zero. ◀

O exercício 89 pede a demonstração da proposição 4.23.

Proposição 4.23. $\operatorname{diag}(A_1, A_2, \ldots, A_k)^{-1} = \operatorname{diag}(A_1^{-1}, A_2^{-1}, \ldots, A_k^{-1})$.

Exemplo 4.24. Seja

$$A = \left(\begin{array}{cc:c:cc} 1 & 1 & & & \\ 2 & 0 & & & \\ \hdashline & & 2 & & \\ \hdashline & & & 2 & 1 \\ & & & 0 & 2 \end{array}\right) = \left(\begin{array}{c:c:c} A_{11} & 0 & 0 \\ \hdashline 0 & A_{22} & 0 \\ \hdashline 0 & 0 & A_{33} \end{array}\right),$$

com

$$A_{11} = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}, \quad A_{22} = (2), \quad A_{33} = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}.$$

As inversas dos blocos são

$$A_{11}^{-1} = \begin{pmatrix} 0 & 1/2 \\ 1 & -1/2 \end{pmatrix}, \quad A_{22}^{-1} = (1/2), \quad A_{33}^{-1} = \begin{pmatrix} 1/2 & -1/4 \\ 0 & 1/2 \end{pmatrix}.$$

Assim,

$$A^{-1} = \left(\begin{array}{c:c:c} A_{11}^{-1} & 0 & 0 \\ \hdashline 0 & A_{22}^{-1} & 0 \\ \hdashline 0 & 0 & A_{33}^{-1} \end{array}\right) = \left(\begin{array}{cc:c:cc} 0 & 1/1 & & & \\ 1 & -1/2 & & & \\ \hdashline & & 1/2 & & \\ \hdashline & & & 1/2 & -1/4 \\ & & & 0 & 1/2 \end{array}\right). \quad ◀$$

É usual darmos nomes aos blocos de uma matriz. Por exemplo, dadas matrizes conhecidas A e B,

$$\begin{pmatrix} A & B \\ B^{-1} & 0 \end{pmatrix}$$

é uma matriz composta por quatro blocos. O bloco $(2,2)$ é zero, o bloco $(1,1)$ é igual a A e os blocos $(1,2)$ e $(2,1)$ são B e B^{-1}.

Muitas vezes a notação por blocos nos permite representar famílias de matrizes: a notação determina a forma de um conjunto infinito de matrizes. Por exemplo,

$$\begin{pmatrix} \mathcal{I} & 0 \\ 0 & 0 \end{pmatrix}$$

é uma matriz cuja diagonal é da forma $(1, 1, 1, \ldots, 1, 0, 0, 0, \ldots, 0)$ – ou seja, uns seguidos de zeros, que também podemos denotar por $\text{diag}(\mathcal{I}, 0)$. Observe que $\text{diag}(\mathcal{I}, 0)$ pode ser de qualquer ordem, e o tamanho dos blocos $\mathcal{I}$ e 0 não foi especificado.

Exemplo 4.25. A notação $\text{diag}(\mathcal{I}, 0, \mathcal{I})$ indica matrizes como

$$\left(\begin{array}{c|c|c} 1 & 0 & 0 \\ \hline 0 & 0 & 0 \\ \hline 0 & 0 & 1 \end{array}\right), \quad \left(\begin{array}{c|c|c|c} 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \quad \left(\begin{array}{c|c|c|c|c} 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}\right), \quad \left(\begin{array}{c|c|c|c|c} 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}\right),$$

e todas as matrizes diagonais onde a diagonal é composta de uma sequência de uns seguida de uma sequência de zeros e outra sequência de uns. ◀

A matriz a seguir,

$$\left(\begin{array}{c|c|c} 1 & \mathbf{v}^T & 0 \\ \hline \mathbf{w} & B & 0 \end{array}\right), \tag{4.3}$$

tem a primeira linha igual a $(1, v_1, v_2, \ldots, v_n, 0)^T$, a primeira coluna igual a $(1, w_1, w_2, \ldots, w_m)$. Se retirarmos da matriz a primeira coluna e a primeira linha, sobra a matriz B.

Também é comum não usar as barras que dividem as partições. A matriz 4.3 pode também ser representada da seguinte forma:

$$\begin{pmatrix} 1 & \mathbf{v}^T & 0 \\ \mathbf{w} & B & 0 \end{pmatrix}.$$

4.2.2 Multiplicação por vetor é combinação linear

A multiplicação de matriz por vetor pode ser vista como combinação linear das linhas ou colunas da matriz. Isto nos dá uma interpretação mais útil da operação de multiplicação.

Multiplicando à direita da matriz: combinação de colunas

Em algumas situações representaremos uma matriz como uma sequência de vetores coluna:

$$\begin{aligned} M &= \begin{pmatrix} \mathbf{c}^1 & \mathbf{c}^2 & \cdots & \mathbf{c}^n \end{pmatrix} \\ &= \begin{pmatrix} c_1^1 & c_1^2 & \ldots & c_1^m \\ c_2^1 & c_2^2 & & c_2^m \\ \vdots & & \ddots & \\ c_n^1 & c_n^2 & & c_n^m \end{pmatrix}. \end{aligned}$$

Observamos que ao multiplicar uma matriz por um vetor coluna, temos

$$\begin{pmatrix} c_1^1 & c_1^2 & \dots & c_1^m \\ c_2^1 & c_2^2 & & c_2^m \\ \vdots & & \ddots & \\ c_n^1 & c_n^2 & & c_n^m \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix} = \begin{pmatrix} a_1c_1^1 + a_2c_1^2 + \ldots + a_mc_1^m \\ a_1c_2^1 + a_2c_2^2 + \ldots + a_mc_2^m \\ \vdots \\ a_1c_n^1 + a_2c_n^2 + \ldots + a_mc_n^m \end{pmatrix}$$
$$= \begin{pmatrix} a_1c_1^1 \\ a_1c_2^1 \\ \vdots \\ a_1c_n^1 \end{pmatrix} + \begin{pmatrix} a_2c_1^2 \\ a_2c_2^2 \\ \vdots \\ a_2c_n^2 \end{pmatrix} + \cdots + \begin{pmatrix} a_mc_1^m \\ a_mc_2^m \\ \vdots \\ a_mc_n^m \end{pmatrix}$$
$$= a_1\mathbf{c}^1 + a_2\mathbf{c}^2 + \cdots a_m\mathbf{c}^m,$$

ou seja, a multiplicação da matriz $(\mathbf{c}^1, \mathbf{c}^2, \ldots, \mathbf{c}^n)$ pelo vetor $(a_1, a_2, \ldots, a_n)^T$ é combinação linear das colunas da matriz, com os coeficientes a_i.

Exemplo 4.26. Pode-se calcular o produto a seguir como combinação linear das colunas da matriz.

$$\begin{pmatrix} 1 & 2 & 3 & 1 \\ -2 & 0 & -2 & -5 \\ 8 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ -a \\ d \end{pmatrix} = a \begin{pmatrix} 1 \\ -2 \\ 8 \end{pmatrix} + b \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} - a \begin{pmatrix} 3 \\ -2 \\ 0 \end{pmatrix} + d \begin{pmatrix} 1 \\ -5 \\ 0 \end{pmatrix}$$
$$= \begin{pmatrix} a + 2b - 3a + d \\ -2a + 2a - 5d \\ 8a + b \end{pmatrix} = \begin{pmatrix} -2a + 2b + d \\ -5d \\ 8a + b \end{pmatrix} \quad \blacktriangleleft$$

Esta propriedade pode ser usada na demonstração de Lema 4.27, que é pedida no Exercício 93.

Lema 4.27. *Se a soma de cada linha (ou de cada coluna) de uma matriz é zero, então as linhas (colunas) da matriz são LD.*

Multiplicação à esquerda: combinação de linhas

Da mesma forma que a multiplicação M**v** é combinação linear das *colunas* de M, a multiplicação **w**M é combinação das *linhas* de M.

Exemplo 4.28. Sejam

$$M = \begin{pmatrix} 1 & 2 & -3 \\ 4 & 3 & -8 \\ 0 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix}, \quad \mathbf{w} = (2, 0, -1, 3).$$

Então

$$\begin{aligned} \mathbf{w}M = \quad & 2(1, \ 2, -3) \\ & -1(0, \ 0, \ 2) \\ & +3(2, \ 1, \ 0) \\ = \quad & (8, \ 7, -8). \end{aligned} \quad \blacktriangleleft$$

A justificativa é análoga à do caso anterior, para multiplicação à direita de M.

4.2.3 Matrizes triangulares

Matrizes triangulares tem propriedades bastante úteis. A seguir apresentamos algumas delas.

Proposição 4.29. *O produto de duas matrizes triangulares inferiores também é triangular inferior, e o produto de duas matrizes triangulares superiores também é triangular superior.*

Demonstração. Segue trivialmente da definição de multiplicação de matrizes. ■

Exemplo 4.30.

$$\begin{pmatrix} 1 & -1 & 0 & -1 \\ 0 & 2 & 1 & 5 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix} \begin{pmatrix} -1 & 0 & 1 & 1 \\ 0 & 2 & 5 & 3 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -2 & -4 & -3 \\ 0 & 4 & 10 & 14 \\ 0 & 0 & 0 & 9 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$ ◀

Proposição 4.31. *A inversa de uma matriz triangular inferior também é triangular inferior, e a inversa de uma matriz triangular superior também é triangular superior.*

Exemplo 4.32. A inversa de

$$A = \begin{pmatrix} 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

é

$$A^{-1} = \begin{pmatrix} 1 & -2 & 2 & -1 \\ 0 & 1 & -2 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$ ◀

Proposição 4.33. *Se A é uma matriz triangular, então as entradas da diagonal de A^{-1} são os inversos das mesmas posições em A.*

Exemplo 4.34. A inversa de

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -3 & 0 & 0 \\ 3 & 6 & 4 & 0 \\ 4 & -2 & 0 & 5 \end{pmatrix}$$

é

$$A^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2/3 & -1/3 & 0 & 0 \\ -7/4 & 1/2 & 1/4 & 0 \\ -8/15 & -2/15 & 0 & 1/5 \end{pmatrix}.$$

Observe que os elementos da diagonal de A^{-1} são $1, -1/3, 1/4, 1/5$ – exatamente os inversos dos elementos da diagonal de A, $1, -3, 4, 5$. ◀

4.3 Propriedades de matrizes de transformações

Das propriedades de matrizes derivamos também os seguintes fatos – dadas matrizes A, B, um vetor $\mathbf{v}$ e um escalar λ,

- $(A+B)\mathbf{v} = A\mathbf{v} + B\mathbf{v}$,
- $(\lambda A)\mathbf{v} = \lambda(A\mathbf{v}) = A(\lambda\mathbf{v})$,
- $(AB)\mathbf{v} = A(B\mathbf{v})$,

quando os produtos forem bem definidos.

Proposição 4.35. *Sejam T e S matrizes representando transformações lineares t e s. A composição $t \circ s$, se existir, é representada pela matriz TS, e a soma $t+s$, se for bem definida, é dada pela matriz $T+S$. A inversa da transformação t é representada pela matriz T^{-1}.*

Exemplo 4.36. Considere as transformações $s : \mathbb{R}^2 \to \mathbb{R}^3$, e $t : \mathbb{R}^3 \to \mathbb{R}^4$, tais que

$$\begin{aligned} s(a,b)^T &= (a, a+b, 2b)^T \\ t(x,y,z)^T &= (x+y, x-y, x+z, x-z)^T. \end{aligned}$$

Sem ainda escrever suas matrizes, calculamos a composta

$$\begin{aligned} t \circ s &= t(s(a,b)^T) \\ &= t(a, a+b, 2b)^T \\ &= (2a+b, -b, a+2b, a-2b)^T \end{aligned} \tag{4.4}$$

As matrizes das transformações são

$$T = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & -1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 2 \end{pmatrix}$$

A matriz da composta é

$$TS = \begin{pmatrix} 2 & 1 \\ 0 & -1 \\ 1 & 2 \\ 1 & -2 \end{pmatrix}$$

Ao aplicarmos a matriz da composta ao vetor $(a,b)^T$, obtemos

$$\begin{pmatrix} 2 & 1 \\ 0 & -1 \\ 1 & 2 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 2a+b \\ -b \\ a+2b \\ a-2b \end{pmatrix},$$

claramente correto, pois é exatamente da mesma forma que havíamos calculado em 4.4, antes de escrever as matrizes. ◀

Teorema 4.37. *A imagem da transformação linear representada por uma matriz A é o conjunto de todas as combinações lineares das colunas de A.*

Demonstração. Cada elemento da imagem de A é o resultado da multiplicação de A por um vetor $\mathbf{x}$ – ou seja, a combinação linear das colunas de A, onde os coeficientes são os elementos de $\mathbf{x}$. Se considerarmos todos os valores possíveis em $\mathbf{x}$, temos todas as combinações lineares das colunas de A. ■

Exemplo 4.38. A transformação com a matriz

$$T = \begin{pmatrix} 1 & 2 \\ 2 & 2 \\ 1 & 3 \end{pmatrix}$$

é

$$T(x, y) = (x + 2y, 2x + 2y, x + 3y),$$

e tem como imagem um plano em $\mathbb{R}^3$. Este plano é composto pelas combinações lineares

$$x \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} + y \begin{pmatrix} 2 \\ 2 \\ 3 \end{pmatrix}. \qquad \blacktriangleleft$$

Definição 4.39 (Posto de matriz)**.** O *posto* de uma matriz é o posto da transformação linear representada por ela. ♦

Segue imediatamente da definição 4.39 e do teorema 4.37 o seguinte corolário.

Corolário 4.40. *O posto de uma matriz A é igual à quantidade de colunas linearmente independentes em A.*

A imagem de uma transformação linear é o *espaço-coluna* de sua matriz, e portanto a dimensão da imagem (e o posto da transformação) é igual à quantidade de colunas independentes na matriz.

Definição 4.41 (Espaço-linha, espaço-coluna, posto de linhas e colunas)**.** O *espaço-linha* de uma matriz é o espaço vetorial gerado pelas linhas da matriz; o *espaço-coluna* é o espaço vetorial gerado pelas colunas da matriz.

O *posto de linhas* de uma matriz é a dimensão de seu espaço-linha – ou seja, a quantidade de linhas linearmente independentes na matriz

O *posto de colunas* de uma matriz é definido de forma similar: é a dimensão de seu espaço-coluna, ou a quantidade de colunas linearmente independentes na matriz. ♦

Uma matriz $m \times n$ tem o espaço-linha gerado por m vetores-linha, e o espaço-coluna gerado por n vetores-coluna. As dimensões destes espaços não são, no entanto, necessariamente iguais a m e n, uma vez que as linhas e colunas da matriz podem não ser L.I., e neste caso não formam base para aqueles espaços.

Muitas vezes dizemos que uma matriz quadrada de ordem n e com posto de colunas igual a n é "base" para $\mathbb{R}^n$, porque $\mathbb{R}^n$ é seu espaço-coluna, e portanto a matriz, quando vista como uma sequência de colunas, é uma base ordenada de $\mathbb{R}^n$.

Exemplo 4.42. As matrizes

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & -1 & -1 \end{pmatrix}$$

são bases para $\mathbb{R}^2$ e $\mathbb{R}^3$, porque qualquer vetor de $\mathbb{R}^2$ pode ser escrito como combinação linear das colunas de A, e qualquer vetor de $\mathbb{R}^3$ é combinação linear das colunas de B. ◀

O lema e o teorema a seguir relacionam o posto de linhas com o posto de colunas.

Lema 4.43. *Qualquer matriz* A $m \times n$ *com posto de colunas* r *pode ser decomposta em duas matrizes,* C $m \times r$ *e* L $r \times n$*, de forma que* $A = CL$*, de forma que o espaço coluna de* A *é gerado pelas* r *colunas de* C*, e o espaço linha de* A *é gerado pelas* r *linhas de* L*.*

Demonstração. Seja A, $m \times n$, com posto r. Como o posto de A é igual ao posto de colunas de A, podemos tomar r colunas LI de A. Pomos estas colunas lado a lado para formar uma nova matriz C, $m \times r$.

Dadas A e C, existe uma única matriz L, $r \times n$, tal que

$$A = CL.$$

Já sabemos que C gera as mesmas colunas que A. Resta observar que L gera as mesmas linhas que A. Mas no produto CL, *as linhas geradas são combinações lineares das linhas de* L*, com os coeficientes dados pelas colunas de* C. Por exemplo, se

$$A = \begin{pmatrix} 1 & 6 & -11 \\ 2 & 0 & 2 \\ 5 & -1 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 6 \\ 2 & 0 \\ 5 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -2 \end{pmatrix}$$

Neste exemplo, a primeira linha de A, $(1, 6, 4)$, é gerada pelas linhas de L, com coeficientes na primeira linha de C; o mesmo vale para as outras linhas:

$$\begin{aligned} 1(1,0,1) + 6(0,1,-2) &= (1,0,1) + (0,6,-12) \\ &= (1,6,-11). \end{aligned} \qquad \text{(linha 1 de } A\text{)}$$

$$2(1,0,1) + 0(0,1,-2) = (2,0,2). \qquad \text{(linha 2 de } A\text{)}$$

$$\begin{aligned} 5(1,0,1) - 1(0,1,-2) &= (5,0,5) + (0,-1,2) \\ &= (5,-1,7). \end{aligned} \qquad \text{(linha 3 de } A\text{)}$$

A demonstração está portanto terminada. ■

Exemplo 4.44. Seja

$$A = \begin{pmatrix} 2 & 1 & 3 & 1 \\ 3 & 0 & 3 & 0 \\ 1 & -2 & -1 & 0 \\ 1 & 3 & 4 & -1 \end{pmatrix}$$

A pode ser decomposta em

$$A = \overbrace{\begin{pmatrix} 2 & 1 & 1 \\ 3 & 0 & 0 \\ 1 & -2 & 0 \\ 1 & 3 & -1 \end{pmatrix}}^{C} \overbrace{\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}^{L}.$$

A matriz C claramente tem tres colunas LI, e gera as mesmas colunas que A (porque suas colunas são idênticas às únicas tres colunas LI de A).

A matriz L tem tres linhas LI, e gera as mesmas linhas que A: A primeira linha de C é $(2, 1, 1)$, indicando que a primeira linha de A é a combinação linear da linhas de L com coeficientes 2, 1 e 1:

$$(2,\ 1,\ 1)\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix} = (2,\ 1,\ 3,\ 1).$$

O mesmo vale para as outras linhas de A. ◀

Teorema 4.45. *Para toda matriz, o posto de linhas é igual ao posto de colunas.*

Demonstração. Seja A uma matriz $m \times n$. Se $A = 0$, as duas quantidades (de linhas e de colunas L.I.) são zero.

Suponha que o posto de colunas de A é r. Podemos portanto escolher r colunas LI de A. Tomamos estas r colunas LI e as pomos lado a lado para formar outra matriz C, e escolhemos uma matris L como determina o lema 4.43, resultando em uma decomposição

$$A = CL.$$

Sabemos que C gera as colunas de A (e portanto o espaço coluna de A); sabemos também que L gera as linhas de A (e seu espaço-linha).

Isso significa que o posto de linhas de A não é maior que a quantidade de linhas em L, que é igual a r. (Não provamos ainda que o posto de linhas é *exatamente* r, porque não provamos que as r linhas são LI.) Assim,

$$\text{posto\_linhas}(A) \leq \text{posto\_colunas}(A)$$

Se repetirmos o mesmo raciocínio para A^T obteremos

$$\text{posto\_colunas}(A) \leq \text{posto\_linhas}(A)$$

e consequentemente,

$$\text{posto\_linhas}(A) = \text{posto\_colunas}(A).$$ ■

Exemplo 4.46. A transformação de $\mathbb{R}^4$ em $\mathbb{R}^3$, exibida no exemplo 4.12, é

$$T\left[(a, b, c, d)^T\right] = (a + b + c, 3d, -2a)^T.$$

A matriz que representa T é

$$M_T = \begin{pmatrix} 1 & 1 & 1 & 0\\ 0 & 0 & 0 & 3\\ -2 & 0 & 0 & 0\end{pmatrix}.$$

A imagem da transformação é composta pelos vetores da forma $(a + b + c, 3d, -2a)^T$ – e na verdade qualquer vetor de $\mathbb{R}^3$ é desta forma. Assim, o posto da transformação é três. Observamos também que a matriz de T tem três linhas LI, e também tem três colunas LI.

A decomposição que mencionamos na demonstração do Teorema 4.45 é

$$M_T = LC,$$

com

$$L = \begin{pmatrix} 1 & 1 & 0\\ 0 & 0 & 3\\ -2 & 0 & 0\end{pmatrix}.\quad C = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}.$$ ◀

Teorema 4.47. *Se uma matriz M de ordem n tem posto estritamente menor que n, então M é singular.*

Demonstração. M representa um operador linear em um espaço V com $\dim V = n$. Se o posto da transfomação for menor que n, a dimensão da imagem de M será menor que n. Pelo Teorema 3.60, M não é bijetora, e portanto não tem inversa. ■

4.3.1 Mudança de base

Uma vez que a mudança de base é uma transformação linear, como descrito na seção 2.4, ela pode ser descrita como matriz. Usamos a notação $[\mathrm{id}]_{R\to S}$ para enfatizar que esta matriz não modifica os vetores, mudando apenas a base em que são descritos. Esta matriz representa a função identidade (que é uma transformação linear), mas levando de uma base a outra:

$$[\mathrm{id}]_{R\to S}[\mathbf{x}]_R = [\mathbf{x}]_S.$$

Teorema 4.48. *Sejam R e S duas bases para um espaço vetorial V com dimensão n:*

$$R = (\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_n)$$
$$S = (\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_n).$$

A matriz de mudança de base $[\mathrm{id}]_{R\to S}$ é $n \times n$ cujas colunas são os vetores da base R escritos na base S:

$$[\mathrm{id}]_{R\to S} = \begin{pmatrix} [\mathbf{r}_1]_S & [\mathbf{r}_2]_S & \cdots & [\mathbf{r}_n]_S \end{pmatrix},$$

de forma que para todo $\mathbf{v} \in V$,

$$[\mathbf{v}]_S = [\mathrm{id}]_{R\to S}[\mathbf{v}]_R.$$

Demonstração. Primeiro observamos que se uma matriz como esta existir ela deve levar vetores $\mathbf{r}_i$ da base R nos vetores $\mathbf{s}_i$ da base S.

Sabemos que $[\mathbf{r}_i]_R = \mathbf{e}_i$. Assim, se aplicarmos a matriz a algum vetor $\mathbf{r}_i \in R$, obtemos

$$[\mathrm{id}]_{R\to S}[\mathbf{r}_i]_R = [\mathrm{id}]_{R\to S}\mathbf{e}_i,$$

que é a í-ésima coluna de $[\mathrm{id}]_{R\to S}$ – ou seja, $[\mathbf{r}_i]_S$, como queríamos.

Seja então $\mathbf{v} \in V$ um vetor qualquer. Sua representação na base R é $(a_1, a_2, \ldots, a_n)^T$ – ou seja,

$$\mathbf{v} = a_1\mathbf{r}_1 + \cdots + a_n\mathbf{r}_n.$$

Aplicamos $[\mathrm{id}]_{R\to S}$ em $[\mathbf{v}]_R$:

$$\begin{aligned}[\mathrm{id}]_{R\to S}[\mathbf{v}]_R &= \begin{pmatrix} [\mathbf{r}_1]_S & [\mathbf{r}_2]_S & \cdots & [\mathbf{r}_n]_S \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \cdots \\ a_n \end{pmatrix} \\ &= a_1[\mathbf{r}_1]_S + a_2[\mathbf{r}_2]_S + \cdots + a_n[\mathbf{r}_n]_S \\ &= [\mathbf{v}]_S.\end{aligned}$$

■

Exemplo 4.49. Considere as seguintes bases para $\mathbb{R}^3$:

$$\mathrm{B} = \{\, (1,0,0)^\mathsf{T}, (0,1,0)^\mathsf{T}, (0,0,1)^\mathsf{T} \,\}$$
$$\mathrm{C} = \{\, (1,0,0)^\mathsf{T}, (0,2,0)^\mathsf{T}, (0,0,3)^\mathsf{T} \,\}$$

O vetor $(2,4,12)^\mathsf{T}$ de $\mathbb{R}^3$ na base canônica tem coordenadas $[(2,4,12)^\mathsf{T}]_\mathrm{B}$. Já na base C o vetor tem coordenadas $[(2,2,4)^\mathsf{T}]_\mathrm{C}$:

$$2(1,0,0)^\mathsf{T} + 2(0,2,0)^\mathsf{T} + 4(0,0,3)^\mathsf{T} = (2,4,12)^\mathsf{T}.$$

Para obtermos a matriz que muda vetores da base C para a base B, listamos os vetores de C na base B:

$$[\mathrm{id}]_{\mathrm{C}\to\mathrm{B}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Verificamos que a matriz realmente transforma o vetor mencionado anteriormente, $(2,2,4)^\mathsf{T}$ na base C, em $(2,4,12)^\mathsf{T}$, que é sua representação na base B:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \\ 12 \end{pmatrix}.$$ ◀

Teorema 4.50. *Uma matriz de mudança de base sempre tem inversa. Se* $[\mathrm{id}]_{\mathrm{B}\to\mathrm{D}}$ *é a matriz de mudança da base* B *para a base* D*, então* $([\mathrm{id}]_{\mathrm{B}\to\mathrm{D}})^{-1}$ *(a inversa de* P*) é a matriz de mudança de base de* D *para* B*,* $[\mathrm{id}]_{\mathrm{D}\to\mathrm{B}}$*.*

Demonstração 1. Matrizes de mudança de base são quadradas, portanto representam transformações entre espaços de mesma dimensão. Além disso, são construídas com colunas da base do espaço, por isso todas as colunas são LI, e elas sempre tem posto completo. Pelo Teorema 3.60, representam transformações bijetoras, e consequentemente tem inversa – *por isso* $([\mathrm{id}]_{\mathrm{B}\to\mathrm{C}})^{-1}$ *sempre existe!*

Sejam B, C duas bases de um espaço V e $\mathbf{v}$ um vetor $\mathbf{v} \in V$. Então

$$\begin{aligned} [\mathrm{id}]_{\mathrm{B}\to\mathrm{C}}[\mathbf{v}]_\mathrm{B} &= [\mathbf{v}]_\mathrm{C} \\ ([\mathrm{id}]_{\mathrm{B}\to\mathrm{C}})^{-1}[\mathrm{id}]_{\mathrm{B}\to\mathrm{C}}[\mathbf{v}]_\mathrm{B} &= ([\mathrm{id}]_{\mathrm{B}\to\mathrm{C}})^{-1}[\mathbf{v}]_\mathrm{C} \\ \mathcal{I}[\mathbf{v}]_\mathrm{B} &= ([\mathrm{id}]_{\mathrm{B}\to\mathrm{C}})^{-1}[\mathbf{v}]_\mathrm{C}, \end{aligned}$$

e de acordo com a última linha, $([\mathrm{id}]_{\mathrm{B}\to\mathrm{C}})^{-1}$ realiza a mudança de base de C para B. ■

Demonstração 2. Suponha que exista uma transformação $[\mathrm{T}]_{\alpha\to\beta}$ que transforma a representação de vetores da base α para a base β. Sabemos que é possível mudar de qualquer base para outra, e portanto deve necessariamente haver outra transformação $[\mathrm{S}]_{\beta\to\alpha}$ que leve da base β para a base α. Seja então $[\mathrm{id}]_{\mathrm{B}\to\mathrm{D}}$ a matriz de mudança da base B para a base D. Seja $[\mathbf{v}]_\mathrm{B}$ um vetor representado na base B. A representação de $\mathbf{v}$ na base D é $[\mathrm{id}]_{\mathrm{B}\to\mathrm{D}}[\mathbf{v}]_\mathrm{B}$. A representação de $\mathbf{v}$ na base B é

$$([\mathrm{id}]_{\mathrm{B}\to\mathrm{D}})^{-1}([\mathrm{id}]_{\mathrm{B}\to\mathrm{D}}[\mathbf{v}]_\mathrm{B}) = ([\mathrm{id}]_{\mathrm{B}\to\mathrm{D}})^{-1}([\mathrm{id}]_{\mathrm{B}\to\mathrm{D}})[\mathbf{v}]_\mathrm{B} = [\mathbf{v}]_\mathrm{B},$$

e portanto $([\mathrm{id}]_{\mathrm{B}\to\mathrm{D}})^{-1}$ é a matriz de mudança de base de D para B. ■

Exemplo 4.51. Temos a seguir duas bases de $\mathbb{R}^2$:

$$\mathrm{B} = \left((1,0)^\mathsf{T}, (1,1)^\mathsf{T}\right)$$

$$D = \left((1,2)^T, (2,3)^T\right)$$

Para obter a matriz $[\mathrm{id}]_{B\to D}$ escrevemos os vetores de B na base D. Precisamos então determinar os valores de a, b, x, y tais que

$$(1,0)^T = a(1,2)^T + b(2,3)^T$$
$$(1,1)^T = x(1,2)^T + y(2,3)^T$$

Resolvemos os sistemas,

$$\begin{cases} a & +2b & = 1 \\ 2a & +3b & = 0 \end{cases} \qquad \begin{cases} x & +2y & = 1 \\ 2x & +3y & = 1 \end{cases}$$

e obtemos

$$\begin{array}{ll} a = -3 & x = -1 \\ b = +2 & y = +1 \end{array}$$

A matriz de mudança de base $[\mathrm{id}]_{B\to D}$ e sua inversa, $[\mathrm{id}]_{D\to B}$ são, portanto,

$$[\mathrm{id}]_{B\to D} = \begin{pmatrix} -3 & -1 \\ 2 & 1 \end{pmatrix}, \quad [\mathrm{id}]_{D\to B} = \begin{pmatrix} -1 & -1 \\ 2 & 3 \end{pmatrix}.$$

Escolhemos um vetor qualquer na base B, $[\mathbf{v}]_B = (-5,7)^T$. O vetor de $\mathbb{R}^2$ com estas coordenadas é

$$\mathbf{v} = -5(1,0)^T + 7(1,1)^T = (2,7)^T.$$

para obter suas coordenadas na base D,

$$[\mathbf{v}]_D = [\mathrm{id}]_{B\to D}[\mathbf{v}]_B = \begin{pmatrix} -3 & -1 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} -5 \\ 7 \end{pmatrix} = \begin{pmatrix} 8 \\ -3 \end{pmatrix}$$

Agora verificamos que estas coordenadas, na base D, nos dão o mesmo vetor:

$$\mathbf{v} = 8(1,2)^T - 3(2,3)^T = (2,7)^T.$$

Observamos também a mudança inversa no mesmo vetor, dada por $[\mathrm{id}]_{D\to B}$: dadas as coordenadas $(8,-3)^T$,

$$[\mathbf{v}]_B = [\mathrm{id}]_{D\to B}[\mathbf{v}]_D = \begin{pmatrix} -1 & -1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 8 \\ -3 \end{pmatrix} = \begin{pmatrix} -5 \\ 7 \end{pmatrix},$$

as coordeandas do mesmo vetor na base B, que havíamos escolhido inicialmente. ◀

Exemplo 4.52. Considere as seguintes bases para $\mathbb{R}^3$:

$$B = \left((1,0,0)^T, (0,1,0)^T, (0,0,1)^T\right)$$
$$D = \left((2,3,0)^T, (4,0,5)^T, (0,6,7)^T\right)$$

$$(2,3,0) = 2(1,0,0)^T + 3(0,1,0)^T + 0(1,0,0)^T$$
$$(4,0,5) = 4(1,0,0)^T + 0(0,1,0)^T + 5(0,0,1)^T$$

$$(0,6,7) = 0(1,0,0)^T + 6(0,1,0)^T + 7(0,0,1)^T$$

$$[\mathrm{id}]_{B\to D} = \begin{pmatrix} 2 & 4 & 0 \\ 3 & 0 & 6 \\ 0 & 5 & 7 \end{pmatrix}$$

Verificamos que a transformação de cada vetor da base B resulta em outro da base D:

$$[\mathrm{id}]_{B\to D}(1,0,0)^T = \begin{pmatrix} 2 & 4 & 0 \\ 3 & 0 & 6 \\ 0 & 5 & 7 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 0 \end{pmatrix}$$
$$[\mathrm{id}]_{B\to D}(0,1,0)^T = \begin{pmatrix} 2 & 4 & 0 \\ 3 & 0 & 6 \\ 0 & 5 & 7 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 0 \\ 5 \end{pmatrix}$$
$$[\mathrm{id}]_{B\to D}(0,0,1)^T = \begin{pmatrix} 2 & 4 & 0 \\ 3 & 0 & 6 \\ 0 & 5 & 7 \end{pmatrix}\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 6 \\ 7 \end{pmatrix}$$

Agora transformamos um vetor qualquer da base B para a base D:

$$[\mathrm{id}]_{B\to D}(8,-1,2)^T = \begin{pmatrix} 2 & 4 & 0 \\ 3 & 0 & 6 \\ 0 & 5 & 7 \end{pmatrix}\begin{pmatrix} 8 \\ -1 \\ 2 \end{pmatrix} = \begin{pmatrix} 12 \\ 36 \\ 9 \end{pmatrix}.$$

A inversa de P é

$$[\mathrm{id}]_{D\to B} = ([\mathrm{id}]_{B\to D})^{-1} = \begin{pmatrix} \frac{5}{24} & \frac{7}{36} & -\frac{1}{6} \\ \frac{7}{48} & -\frac{7}{72} & \frac{1}{12} \\ -\frac{5}{48} & \frac{5}{72} & \frac{1}{12} \end{pmatrix},$$

e $[\mathrm{id}]_{D\to B}(12,36,9)^T = (8,-1,2)^T$. ◀

Agora obervamos que, assim como uma matriz de mudança de base sempre tem inversa, *toda matriz invertível representa uma mudança de base.*

Proposição 4.53. *Seja* M *uma matriz não singular de ordem* n*. Se fixarmos uma base* $B = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ *de tamanho* n*, então* M *representa simultaneamente:*

i) a mudança de base de B *para alguma base* C *(*$M = [\mathrm{id}]_{B\to C}$*);*

ii) a mudança de base de alguma outra base A *para* B *(*$M = [\mathrm{id}]_{A\to B}$*),*

conforme ilustrado no diagrama a seguir.

$$[\mathbf{v}]_A \xrightarrow{M} [\mathbf{v}]_B \xrightarrow{M} [\mathbf{v}]_C$$

O Exercício 119 pede a demonstração da Proposição 4.53.

Exemplo 4.54. Uma matriz de rotação por θ,

$$R_\theta = \begin{pmatrix} \cos(\theta) & -\operatorname{sen}(\theta) \\ \operatorname{sen}(\theta) & \cos(\theta) \end{pmatrix}$$

sempre tem inversa,

$$(R_\theta)^{-1} = R_{-\theta} = \begin{pmatrix} \cos(-\theta) & -\operatorname{sen}(-\theta) \\ \operatorname{sen}(-\theta) & \cos(-\theta) \end{pmatrix}.$$

A matriz R_θ realiza uma mudança de base. Para sabermos qual é a base para a qual ela leva, calculamos:

$$\begin{pmatrix} \cos(\theta) & -\operatorname{sen}(\theta) \\ \operatorname{sen}(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos(\theta) \\ \operatorname{sen}(\theta) \end{pmatrix}, \qquad \begin{pmatrix} \cos(\theta) & -\operatorname{sen}(\theta) \\ \operatorname{sen}(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\operatorname{sen}(\theta) \\ \cos(\theta) \end{pmatrix}.$$

Assim, a matriz leva as coordenadas de vetores de $\mathbb{R}^2$ na base canônica em coordenadas dos dois vetores da nova base,

$$\left(\begin{pmatrix} \cos(\theta) \\ \operatorname{sen}(\theta) \end{pmatrix}, \begin{pmatrix} -\operatorname{sen}(\theta) \\ \cos(\theta) \end{pmatrix} \right)$$

Note que a fórmula mostra um *par ordenado com duas matrizes-coluna*, e *não* uma matriz-linha contendo duas matrizes.

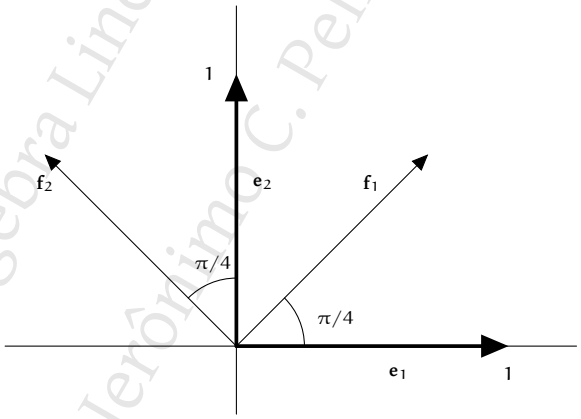
Seja $B = \{\mathbf{e}_1, \mathbf{e}_2\}$ a base canônica para $\mathbb{R}^2$. Escolhemos agora $\theta = \pi/4$. A matriz $R_{\pi/4}$ e sua inversa, $R_{(-\pi/4)}$ são[1]

$$R_{\pi/4} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \qquad R_{(-\pi/4)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

Isto significa que se aplicarmos uma rotação por $\pi/4$ nos vetores da base canônica, a nova base será

$$\begin{aligned} F &= \left(\mathbf{f}_1 = R_{\pi/4}\mathbf{e}_1,\ \ \mathbf{f}_2 = R_{\pi/4}\mathbf{e}_2\right) \\ &= \left(\mathbf{f}_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \mathbf{f}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \end{pmatrix}\right). \end{aligned}$$

A figura a seguir mostra as bases B e F. Note que *a rotação leva os dois vetores* $\mathbf{e_1}$ *e* $\mathbf{e_2}$ *em outros dois vetores LI (a mesma rotação em dois vetores não poderia torná-los colineares).*



[1] Lembrete: $\operatorname{sen}(\pi/4) = \cos(\pi/4) = \cos(-\pi/4) = 1/\sqrt{2}$. $\operatorname{sen}(-\pi/4) = -1/\sqrt{2}$. Veja também a nota de rodapé 1 na página 89.

Escrevemos os vetores $\mathbf{e}_1$ e $\mathbf{e}_2$ na base F:

$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} - \frac{1}{\sqrt{2}} \begin{pmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$\mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

Assim, temos

$$[\mathbf{e}_1]_F = \frac{1}{\sqrt{2}}(1,-1)^T,$$

$$[\mathbf{e}_2]_F = \frac{1}{\sqrt{2}}(1,1)^T.$$

Vemos que a matriz que muda da base canônica B para a base F é, portanto, a matriz de rotação $R_{-\pi/4}$:

$$[\mathrm{id}]_{B\to F} = \begin{pmatrix} [\mathbf{e}_1]_F & [\mathbf{e}_2]_F \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = R_{-\pi/4}.$$

Como a base foi rotacionada por $\pi/4$, as coordenadas dos vetores são rotacionadas por $-\pi/4$, para compensar a mudança na base, de outra forma os vetores também sofreriam a mesma rotação feita na base. Por isso os vetores em $\mathbb{R}^n$ são chamados de *contravariantes.*

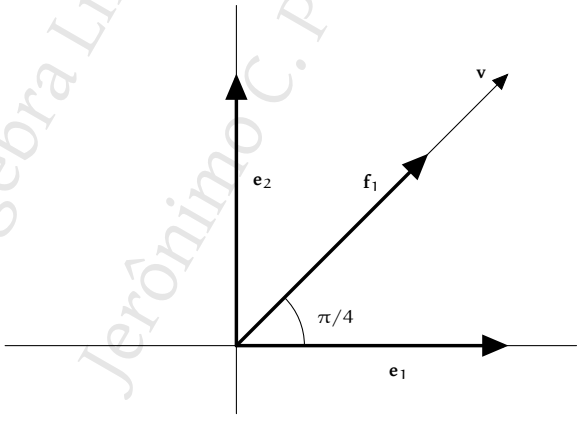
Considere agora o vetor $[\mathbf{v}]_B = (2,2)^T$ em $\mathbb{R}^2$, aqui descrito na base canônica. Na nova base, suas coordenadas são

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 2\sqrt{2} \\ 0 \end{pmatrix}.$$

Vemos que o mesmo vetor que tem as coordenadas $(2,2)^T$ na base canônica tem as coordenadas $(2\sqrt{2},0)$ na nova base:

$$2\sqrt{2}\left[\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right] + 0\left[\frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 1 \end{pmatrix}\right] = \begin{pmatrix} 2 \\ 2 \end{pmatrix}.$$

Realmente, usando os vetores $\mathbf{f}_1$ e $\mathbf{f}_2$, precisamos apenas de $2\sqrt{2}$ vezes $\mathbf{f}_1$ (observe que $\mathbf{v}$ tem o comprimento da diagonal de um quadrado de lado 2):



Fica claro então que, fixada uma base B, uma transformação invertível sempre realiza uma mudança de base, e que para identificar a nova base, basta aplicar a transformação nos vetores de B. ◀

4.3.2 Similaridade

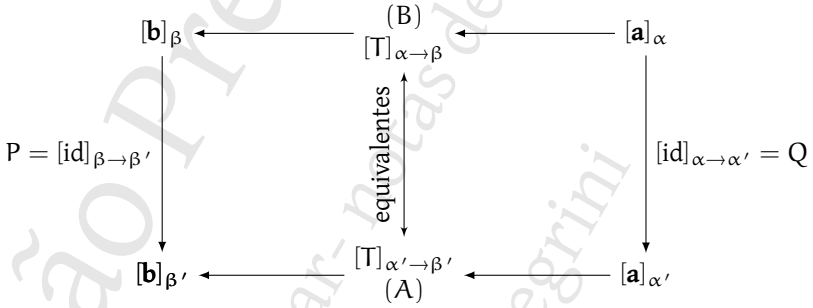
Da mesma forma que a descrição de vetores por coordenadas em $\mathbb{R}^n$ depende da escolha de uma base, a representação de transformações lineares como matrizes depende, também, das bases usadas para representar os vetores do domínio e do contradomínio.

Sejam V e W dois espaços vetoriais, tais que

$$\begin{aligned} V &\text{ tem bases } \alpha, \alpha' \\ W &\text{ tem bases } \beta, \beta', \end{aligned}$$

e $T : V \to W$ uma transformação linear. A matriz que representa T agindo em vetores na base α e resultando em vetores na base β é $[T]_{\alpha\to\beta}$.

Quaisquer vetores $\mathbf{a} \in V$ e $\mathbf{b} \in W$ tem representações $[\mathbf{a}]_\alpha$, $[\mathbf{a}]_{\alpha'}$, $[\mathbf{b}]_\beta$ e $[\mathbf{b}]_{\beta'}$. Deve existir também uma matriz que realize a mesma transformação da base α' para a base β'. A próxima figura ilustra este conceito. A matriz P muda da base β para β'; a matriz Q muda de α para α'; e as matrizes A e B realizam a mesma transformação, mas usando bases diferentes.



Se conhecemos $B = [T]_{\alpha\to\beta}$, podemos determinar $A = [T]_{\alpha'\to\beta'}$ observando que

$$\begin{aligned} [T]_{\alpha'\to\beta'}\ [\mathbf{a}]_{\alpha'} &= [T(\mathbf{a})]_{\beta'} \\ &= [\mathrm{id}]_{\beta\to\beta'}\ [T(\mathbf{a})]_\beta \\ &= [\mathrm{id}]_{\beta\to\beta'}\ [T]_{\alpha\to\beta}\ [\mathbf{a}]_\alpha \\ &= [\mathrm{id}]_{\beta\to\beta'}\ [T]_{\alpha\to\beta}\ [\mathrm{id}]_{\alpha'\to\alpha}\ [\mathbf{a}]_{\alpha'}, \end{aligned}$$

ou seja,

$$[T]_{\alpha'\to\beta'} = \underbrace{[\mathrm{id}]_{\beta\to\beta'}}_{(\mathrm{iii})}\ \underbrace{[T]_{\alpha\to\beta}}_{(\mathrm{ii})}\ \underbrace{[\mathrm{id}]_{\alpha'\to\alpha}}_{(\mathrm{i})},$$

ou

$$A = \underbrace{P}_{(\mathrm{iii})}\ \underbrace{B}_{(\mathrm{ii})}\ \underbrace{Q^{-1}}_{(\mathrm{i})}.$$

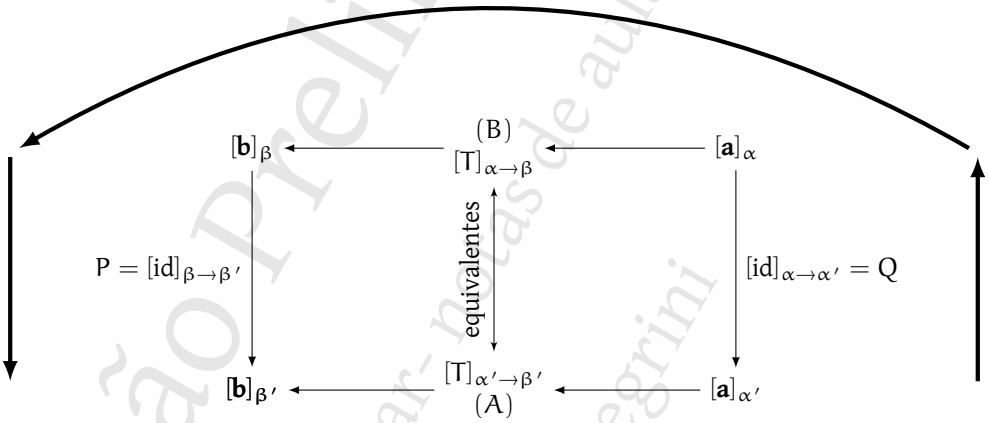
Note que o lado direito da expressão é mais facilmente lido da direita para a esquerda, porque a transformação será aplicada a um vetor que ficará à direita. Lemos a expressão da seguinte maneira: (i) mude o vetor $\mathbf{x}$ da base α' para α; (ii) aplique a transfomração T, e depois (iii) leve da base β para β'.

Dizemos que as matrizes $[T]_{\alpha'\to\beta'}$ e $[T]_{\alpha\to\beta}$, que representam a mesma transformação em bases diferentes, são *equivalentes* (como mostra também a figura anterior).

Definição 4.55 (Matrizes equivalentes)**.** Duas matrizes A e B são *equivalentes* se e somente se existem matrizes invertíveis P e Q tais que

$$A = PBQ^{-1}. \qquad \blacklozenge$$

Na definição 4.55, P e Q são matrizes de mudança de base. Estritamente falando, P e Q^{-1} são invertíveis, portanto poderíamos também ter escrito "se existem matrizes invertíveis R e S tais que $A = SBR$". Usamos "Q^{-1}" para deixar claro que uma das mudanças é *de alguma outra base para* a base em que B opera, e outra mudança é *a partir* da base em que B opera *para alguma outra*. A figura a seguir deve deixar isto claro: partindo de $[\mathbf{a}]_{\alpha'}$, primeiro aplicamos Q^{-1}, depois B e em seguida P, para chegarmos a $[\mathbf{b}]_{\beta'}$, e temos portanto $A = PBQ^{-1}$.



Exemplo 4.56. Seja $T : \mathbb{R}^3 \to \mathbb{R}^2$, dada por

$$T\left[\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right] = \begin{pmatrix} x+y \\ 2z \end{pmatrix}.$$

Temos as seguintes bases para $\mathbb{R}^3$ e $\mathbb{R}^2$:

$$\alpha = \{ (1,0,0)^T, (0,1,0)^T, (0,0,1)^T \} \quad \beta = \{ (1,0)^T, (0,1)^T \}$$
$$\alpha' = \{ (1,0,0)^T, (0,2,0)^T, (0,0,3)^T \} \; \beta' = \{ (5,0)^T, (0,-2)^T \}$$

Seja

$$\mathbf{v} = \begin{pmatrix} 2 \\ 1 \\ -3 \end{pmatrix}.$$

Claramente, $[\mathbf{v}]_\alpha = (2,1,-3)^T$, ou seja, $\mathbf{v}$ na base α é ele mesmo. Além disso,

$$[\mathbf{v}]_{\alpha'} = \begin{pmatrix} 2 \\ 1/2 \\ -1 \end{pmatrix},$$

já que $2(1,0,0)^T + 1/2(0,2,0)^T - (0,0,3)^T = (2,1,-3)^T$.

Agora calculamos a matriz de mudança de base de α para α':

$$\begin{aligned}[\mathrm{id}]_{\alpha\to\alpha'} &= \begin{pmatrix} [\alpha_1]_{\alpha'} & [\alpha_2]_{\alpha'} & [\alpha_3]_{\alpha'} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1/3 \end{pmatrix}.\end{aligned}$$

Similarmente, obtemos

$$[\mathrm{id}]_{\alpha'\to\alpha} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \quad [\mathrm{id}]_{\beta\to\beta'} = \begin{pmatrix} 1/5 & 0 \\ 0 & -1/2 \end{pmatrix}, \quad [\mathrm{id}]_{\beta'\to\beta} = \begin{pmatrix} 5 & 0 \\ 0 & -2 \end{pmatrix}.$$

A transformação T pode ser representada como matriz, levando vetores na base α na base β:

$$[T]_{\alpha\to\beta} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Calculamos agora a matriz de T para as bases α' e β':

$$\begin{aligned}[T]_{\alpha'\to\beta'} &= [\mathrm{id}]_{\beta\to\beta'}[T]_{\alpha\to\beta}[\mathrm{id}]_{\alpha'\to\alpha} \\ &= \begin{pmatrix} 1/5 & 0 \\ 0 & -1/2 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1/5 & 1/5 & 0 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1/5 & 2/5 & 0 \\ 0 & 0 & -3 \end{pmatrix}.\end{aligned}$$

De fato,

$$[T]_{\alpha'\to\beta'}[\mathbf{v}]_{\alpha'} = \begin{pmatrix} 1/5 & 2/5 & 0 \\ 0 & 0 & -3 \end{pmatrix} \begin{pmatrix} 2 \\ 1/2 \\ -1 \end{pmatrix} = \begin{pmatrix} 3/5 \\ 3 \end{pmatrix}.$$

Verificamos que

$$T[(2,1,-3)^T = (3,-6)^T,$$

e

$$3/5(5,0)^T + 3(0,-2)^T = (3,-6)^T. \qquad \blacktriangleleft$$

Se considerarmos um *operador* linear $T : V \to V$ e duas bases α e α' para o espaço V, temos

$$[T]_{\alpha'\to\alpha'} = [\mathrm{id}]_{\alpha\to\alpha'}\,[T]_{\alpha\to\alpha}\,[\mathrm{id}]_{\alpha'\to\alpha},$$

ou

$$A = SBS^{-1}.$$

Dizemos que as matrizes $[T]_{\alpha'\to\alpha'}$ e $[T]_{\alpha\to\alpha}$ são *similares*. Isto é conceitualmente o mesmo que dizer que as duas matrizes são semelhantes, exceto que temos o domínio igual ao contradomínio (e portanto temos $P = Q$ na definição 4.55).

Definição 4.57 (Matrizes similares)**.** Duas matrizes A e B são similares se e somente se existe uma matriz S tal que

$$A = SBS^{-1}. \qquad \blacklozenge$$

Damos a seguir um exemplo simples, sem a interpretação das matrizes como operadores de mudança de base, e um outro, mais extenso, onde tratamos das matrizes S e S^{-1} como matrizes de mudança de base.

Exemplo 4.58. Sejam

$$S = \begin{pmatrix} 1 & 4 & 0 \\ 0 & 0 & 1 \\ 0 & -2 & 0 \end{pmatrix}, \quad S^{-1} = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & -1/2 \\ 0 & 1 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 7 & 12 & 14 \\ 0 & 1 & 2 \\ -4 & -6 & -8 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 0 & 0 \\ 2 & 0 & 3 \\ 0 & -4 & 1 \end{pmatrix}.$$

As matrizes A e B são similares, porque $A = SBS^{-1}$. ◀

Exemplo 4.59. A seguir temos duas bases para $\mathbb{R}^2$:

$$C = \big((1,0)^T, (0,1)^T\big),$$
$$D = \big((0,1)^T, (2,2)^T\big).$$

Definimos uma transformação $T : \mathbb{R}^2 \to \mathbb{R}^2$ como

$$T(x,y)^T = (x + y, 2x - 2y)^T.$$

Para vetores na base canônica C, a matriz de T é

$$A = [T]_{C\to C} = \begin{pmatrix} 1 & 1 \\ 2 & -2 \end{pmatrix}.$$

$$[(1,0)^T]_D = (-1, 1/2)^T \qquad (\text{porque } (1,0) = -\mathbf{1}(0,1)^T + \mathbf{1/2}(2,2)^T)$$
$$[(0,1)^T]_D = (1,0)^T \qquad (\text{porque } (0,1) = \mathbf{1}(0,1)^T + \mathbf{0}(2,2)^T)$$

As matrizes de mudança são, portanto:

$$S = [\mathrm{id}]_{C\to D} = \begin{pmatrix} -1 & 1 \\ 1/2 & 0 \end{pmatrix}, \quad S^{-1} = [\mathrm{id}]_{D\to C} = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}.$$

A matriz que realiza a transformação na base D é

$$B = [T]_{D\to D} = [\mathrm{id}]_{C\to D}[T]_{C\to C}[\mathrm{id}]_{D\to C}$$

$$= SAS^{-1},$$

e portanto as matrizes $A = [T]_{C\to C}$ e $B = [T]_{D\to D}$ são similares. A matriz B é

$$B = [T]_{D\to D} = \begin{pmatrix} -3 & -4 \\ 1/2 & 2 \end{pmatrix}$$

Para finalizar este exemplo, tomamos as coordenadas um vetor qualquer em $\mathbb{R}^2$ na base canônica, $\mathbf{v} = (3,5)^T$. Calculamos $\mathbf{w} = T(\mathbf{v})$ nas duas bases. Temos

$$[T]_{C\to C}([\mathbf{v}]_C) = \begin{pmatrix} 1 & 1 \\ 2 & -2 \end{pmatrix}\begin{pmatrix} 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 8 \\ -4 \end{pmatrix} = [\mathbf{w}]_C.$$

Para aplicar T na base D, primeiro obtemos as coordenadas $[\mathbf{v}]_D$:

$$[\mathbf{v}]_D = [\mathrm{id}]_{C\to D}[\mathbf{v}]_C = \begin{pmatrix} -1 & 1 \\ 1/2 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 2 \\ 3/2 \end{pmatrix}.$$

Agora aplicamos $[T]_{D\to D}$:

$$[T]_{D\to D}([\mathbf{v}]_D) = \begin{pmatrix} -3 & -4 \\ 1/2 & 2 \end{pmatrix}\begin{pmatrix} 2 \\ 3/2 \end{pmatrix}. = \begin{pmatrix} -12 \\ 4 \end{pmatrix} = [\mathbf{w}]_D.$$

Agora verificamos que este é de fato o mesmo vetor $\mathbf{w}$ na base D:

$$-12\begin{pmatrix} 0 \\ 1 \end{pmatrix} + 4\begin{pmatrix} 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 8 \\ -4 \end{pmatrix}. \qquad \blacktriangleleft$$

A proposição a seguir segue trivialmente do fato de matrizes similares representarem a mesma transformação.

Proposição 4.60. *Matrizes equivalentes (ou similares) tem o mesmo posto.*

Teorema 4.61. *Similaridade é uma relação e equivalência.*

Demonstração. Demonstramos a reflexividade, simetria e transitividade a seguir.

(i, reflexividade) A é similar a A, trivialmente: $\mathcal{I}A\mathcal{I}^{-1} = A$

(ii, simetria) Suponha que A é similar a B. Então

$$\begin{aligned} A &= SBS^{-1} \\ AS &= SBS^{-1}S \\ AS &= SB \\ S^{-1}AS &= B \end{aligned}$$

(iii, transitividade) Suponha que A é similar a B e B é similar a C:

$$\begin{aligned} A &= SBS^{-1} \\ B &= RCR^{-1}. \end{aligned}$$

Então

$$\begin{aligned} A &= SBS^{-1} \\ &= SRCR^{-1}S^{-1} \\ &= (SR)C(SR)^{-1}. \end{aligned}$$

■

Exemplo 4.62. Sejam

$$A = \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix}, \quad P = \begin{pmatrix} -2 & 0 \\ 0 & 1/3 \end{pmatrix}, \quad P^{-1} = \begin{pmatrix} -1/2 & 0 \\ 0 & -3 \end{pmatrix}.$$

Exemplificamos primeiro a simetria. Suponha que B é similar a A, com

$$B = PAP^{-1}.$$

Então

$$B = \begin{pmatrix} -2 & 0 \\ 0 & 1/3 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} -1/2 & 0 \\ 0 & -3 \end{pmatrix} = \begin{pmatrix} 1 & -18 \\ -1/3 & -1 \end{pmatrix}.$$

Como temos $B = PAP^{-1}$, temos também $A = P^{-1}BP$:

$$P^{-1}BP = \begin{pmatrix} -1/2 & 0 \\ 0 & -3 \end{pmatrix} \begin{pmatrix} 1 & -18 \\ -1/3 & -1 \end{pmatrix} \begin{pmatrix} -2 & 0 \\ 0 & 1/3 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix} = A.$$

Agora ilustramos a transitividade. Suponha que

$$R = \begin{pmatrix} -1 & 0 \\ 0 & 4 \end{pmatrix}, \quad R^{-1} = \begin{pmatrix} -1 & 0 \\ 0 & 1/4 \end{pmatrix},$$

e C é similar a B, com $C = RBR^{-1}$:

$$C = \begin{pmatrix} -1 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 1 & -18 \\ -1/3 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1/4 \end{pmatrix} = \begin{pmatrix} 1 & 9/2 \\ 4/3 & -1 \end{pmatrix}.$$

Temos C similar a B e B similar a A. Devemos ter, portanto, C similar a A.

$$\begin{aligned} C &= RBR^{-1} \\ &= R(PAP^{-1})R^{-1} \\ &= (RP)A(P^{-1}R^{-1}) \\ &= \begin{pmatrix} -1 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} -2 & 0 \\ 0 & 1/3 \end{pmatrix} A \begin{pmatrix} -1/2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1/4 \end{pmatrix} \\ &= \underbrace{\begin{pmatrix} 2 & 0 \\ 0 & 4/3 \end{pmatrix}}_{RP} A \underbrace{\begin{pmatrix} 1/2 & 0 \\ 0 & 3/4 \end{pmatrix}}_{P^{-1}R^{-1}=(RP)^{-1}}. \end{aligned}$$

Claramente, RP e $P^{-1}R^{-1}$ são inversas, e portanto C é similar a A. ◀

4.4 Espaços de transformações

Uma transformação de um espaço de n dimensões em outro, de m dimensões, sempre será representada por uma matriz $m \times n$. Já verificamos que dados m e n, o conjunto de todas as matrizes $m \times n$ é um espaço vetorial. Podemos dizer então que o espaço $M_{m\times n}$ é o espaço das transformações de dimensão n para dimensão m.

Exemplo 4.63. Uma matriz 3×2 representa uma transformação de $\mathbb{R}^2$ em $\mathbb{R}^3$. Mas sabemos também que as matrizes 3×2, com as operações de soma de matriz e multiplicação por escalar, é um espaço vetorial ($\mathcal{M}_{3\times 2}$). Esse espaço é, portanto, isomorfo ao espaço de todas as transformações lineares de $\mathbb{R}^3$ em $\mathbb{R}^2$. ◀

★ **Exemplo 4.64.** É particularmente importante o *espaço dual* de um espaço vetorial.

Definição 4.65 (Espaço dual)**.** Seja V um espaço vetorial sobre um corpo F. O conjunto de todas as transformações lineares de V em F é o *espaço dual* de V, denotado por V^*. ♦

Suponha por exemplo que $V = \mathbb{R}^3$. Então V^* é o conjunto das transformações de $\mathbb{R}^3$ em $\mathbb{R}$, que podem ser representadas por vetores-linha com 3 elementos (e portanto tem a mesma dimensão que $\mathbb{R}^3$: $\dim V^* = 3$).

A matriz (vetor-linha) $(2, 0, 3)$ pertence a $(\mathbb{R}^3)^*$, porque representa uma transformação de $\mathbb{R}^3$ em $\mathbb{R}$. ◀

4.5 Matrizes elementares

As operações elementares utilizadas na solução de sistemas lineares pelo método de eliminação de Gauss [2] são transformações lineares, e suas matrizes são chamadas de *matrizes elementares*. Uma matriz elementar é obtida aplicando uma operação elementar em $\mathcal{I}$.

Definição 4.66. Uma *matriz elementar* é uma matriz obtida submetendo $\mathcal{I}$ a uma das seguintes *operações elementares*:

- Multiplicação de uma linha i por uma constante k, denotada E_{kLi};
- Permutação de duas linhas i e j, representada por $E_{i,j}$;
- Soma de um múltiplo de uma linha a outra linha, denotada $E_{i+(kLj)}$. ♦

Exemplo 4.67. A operação de multiplicação da segunda linha por 5 é uma operação elementar. Seu efeito na matriz identidade 4×4 é mostrado a seguir.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Temos então

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 & -1 \\ 2 & 3 & 1 & 4 \\ 9 & 5 & -6 & 7 \\ -1 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 & -1 \\ 10 & 15 & 5 & 20 \\ 9 & 5 & -6 & 7 \\ -1 & 3 & 1 & 2 \end{pmatrix}. \quad ◀$$

Exemplo 4.68. Permutar a segunda e terceira linhas é uma operação elementar. O efeito na identidade 3×3 é mostrado a seguir.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

[2] O método de eliminação de Gauss é descrito na seção α.1.2 do Apêndice α.

Por exemplo,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & -1 & 2 \\ 0 & 1 & 1 \\ 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 2 & -1 & 2 \\ 3 & 4 & 5 \\ 0 & 1 & 1 \end{pmatrix}. \qquad \blacktriangleleft$$

Exemplo 4.69. Somar 4 vezes a primeira linha à terceira é uma operação elementar. O efeito na identidade 3×3 é mostrado a seguir.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}$$

Exemplificando,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 9 & 1 & -1 \\ 2 & 6 & 12 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 9 & 1 & -1 \\ 6 & 14 & 24 \end{pmatrix}. \qquad \blacktriangleleft$$

O teorema a seguir esclarece a *atuação* de matrizes elementares sobre outras matrizes.

Teorema 4.70. *Seja A uma matriz quadrada. Então, com relação à multiplicação de matrizes elementares* à esquerda *de A:*

i) $E_{ij}A$ *resulta na matriz A com as* linhas i *e* j *trocadas;*

ii) $E_{kLi}A$ *resulta na matriz A com a* i*-ésima* linha *multiplicada por* k*;*

iii) $E_{i+kLj}A$ *resulta na matriz A após a soma de* k *vezes a* j-ésima linha *sobre a* i-ésima*.*

Já com relação à multiplicação de matrizes elementares à direita *de A, temos:*

i) AE_{ij} *resulta na matriz A com as* colunas i *e* j *trocadas;*

ii) AE_{iLk} *resulta na matriz A com a* j*-ésima* coluna *multiplicada por* k*;*

iii) AE_{i+kLj} *resulta na matriz A após a soma de* k *vezes a* i-ésima coluna *sobre a* j-ésima*.*

No Teorema 4.70, observe que os itens (iii) das duas situações não diferem apenas na atuação de linhas e colunas, mas nos índices também: Denotarmos a k-ésima linha e a k-ésima coluna por L_k e C_k. A mesma matriz elementar $E_{i(\alpha,j)}$ soma:

- α vezes a j-ésima linha à i-ésima;
- α vezes a i-ésima coluna à j-ésima.

Note a troca de índices:

$$L_i = L_i + \alpha L_j$$
$$C_j = C_j + \alpha C_i$$

Exemplo 4.71. Temos a seguir três matrizes elementares de ordem 3:

$$E_{2,3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad E_{3L1} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad E_{2+(5L3)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 5 \\ 0 & 0 & 1 \end{pmatrix}.$$

Escolhemos também uma matriz quadrada para observar a atuação das matrizes acima:

$$A = \begin{pmatrix} 1 & -1 & 0 \\ 4 & 2 & 2 \\ -5 & 7 & 3 \end{pmatrix}.$$

A seguir temos a *atuação das matrizes* E_k *à esquerda de* A:

$$E_{2,3}A = \begin{pmatrix} 1 & -1 & 0 \\ -5 & 7 & 3 \\ 4 & 2 & 2 \end{pmatrix}, \quad E_{3L1}A = \begin{pmatrix} 3 & -3 & 0 \\ 4 & 2 & 2 \\ -5 & 7 & 3 \end{pmatrix}, \quad E_{2+5L3}A = \begin{pmatrix} 1 & -1 & 0 \\ -21 & 37 & 17 \\ -5 & 7 & 3 \end{pmatrix}.$$

Agora verificamos a *atuação das matrizes* E_k *à direita de* A:

$$AE_{2,3} = \begin{pmatrix} 1 & 0 & -1 \\ 4 & 2 & 2 \\ -5 & 3 & 7 \end{pmatrix}, \quad AE_{3L1} = \begin{pmatrix} 3 & -1 & 0 \\ 12 & 2 & 2 \\ -15 & 7 & 3 \end{pmatrix}, \quad AE_{2+5L3} = \begin{pmatrix} 1 & -1 & -5 \\ 4 & 2 & 12 \\ -5 & 7 & 38 \end{pmatrix}. \quad \blacktriangleleft$$

Definição 4.72 (Matrizes equivalentes por linhas)**.** Duas matrizes A e B são *equivalentes por linhas* se uma pode ser obtida da outra por operações elementares em linhas. Ou, equivalentemente, se

$$A = E_k E_{k-1} \cdots E_1 B,$$

onde cada E_k é uma matriz elementar. ♦

Exemplo 4.73. Sejam

$$A = \begin{pmatrix} 2 & 1 \\ -6 & 9 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 1 \\ 0 & 4 \end{pmatrix}, \quad C = \begin{pmatrix} -2 & 3 \\ 2 & 1 \end{pmatrix}.$$

A e B são equivalentes por linha, porque

$$A = \begin{pmatrix} 2 & 1 \\ -6 & 9 \end{pmatrix} \xrightarrow{L_2 \div 3} \begin{pmatrix} 2 & 1 \\ -2 & 3 \end{pmatrix} \xrightarrow{L_2 + L_1} \begin{pmatrix} 2 & 1 \\ 0 & 4 \end{pmatrix} = B$$

A e C também são equivalentes por linhas, porque

$$A = \begin{pmatrix} 2 & 1 \\ -6 & 9 \end{pmatrix} \xrightarrow{L_2 \div 3} \begin{pmatrix} 2 & 1 \\ -2 & 3 \end{pmatrix} \xrightarrow{L_1 \leftrightarrow L_2} \begin{pmatrix} -2 & 3 \\ 2 & 1 \end{pmatrix} = C \quad \blacktriangleleft$$

Teorema 4.74. *Equivalência por linhas é uma relação de equivalência.*

Demonstração. Precisamos mostrar reflexividade, simetria e transitividade.

(i) (Reflexividade) Trivial (A é equivalente a A – a sequência vazia de operações elementares transforma A em A).

(ii) (Simetria) Se A é equivalente por linhas a B, há uma sequência de matrizes elementares $E_1, E_2, \ldots, E_k$ tal que $B = E_1 E_2 \ldots E_k A$. Como toda matriz elementar tem inversa, temos $A = E_k^{-1} E_{k-1}^{-1} \ldots E_1^{-1} B$.

(iii) (Transitividade) Se A é equivalente por linhas a B e B é equivalente por linhas a C, então

$$\begin{aligned} A &= E_k E_{k-1} \ldots E_1 B \\ B &= E'_m E'_{m-1} \ldots E'_1 C. \end{aligned}$$

Mas então

$$\begin{aligned} A &= (E_k E_{k-1} \ldots E_1) B \\ &= (E_k E_{k-1} \ldots E_1)(E'_m E'_{m-1} \ldots E'_1) C \end{aligned} \quad \blacksquare$$

4.6 Sistemas de equações lineares

Podemos representar um sistema de equações lineares em forma matricial. O sistema a seguir tem m equações e n variáveis.

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ \vdots \qquad\qquad & \quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m \end{aligned}$$

Este sistema é descrito por uma matriz A, onde cada entrada a_{ij} é o coeficiente da j-ésima variável na i-ésima linha; um vetor coluna $\mathbf{x}$, com cada uma das variáveis, e um vetor coluna $\mathbf{b}$ com os valores do lado direito das equações:

$$A\mathbf{x} = \mathbf{b}.$$

E desta forma resolver o sistema é o mesmo que encontrar o vetor $\mathbf{x}$ que satisfaça esta equação.

Exemplo 4.75. O sistema

$$\begin{cases} x_1 & -2x_2 & +3x_3 & & = 4 \\ & 5x_2 & -x_3 & +3x_4 & = 2 \\ x_1 & +x_2 & +x_3 & +x_4 & = 10 \end{cases}$$

é descrito como

$$\begin{pmatrix} 1 & -2 & 3 & 0 \\ 0 & 5 & -1 & 3 \\ 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 4 \\ 2 \\ 10 \end{pmatrix}. \qquad \blacktriangleleft$$

É claramente possível também representar sistemas de inequações como $A\mathbf{x} \leq \mathbf{b}$ ou $A\mathbf{x} \geq \mathbf{b}$.

Definição 4.76 (Sistema linear homogêneo)**.** Um sistema de equações lineares é *homogêneo* se é da forma $A\mathbf{x} = \mathbf{0}$ (ou seja, se os termos independentes de todas as equações são iguais a zero). ⧫

Exemplo 4.77. O sistema a seguir é homogêneo.

$$\begin{pmatrix} 3 & 4 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \qquad \blacktriangleleft$$

Todo sistema linear homogêneo admite pelo menos uma solução, com todas as variáveis iguais a zero. Esta solução é chamada de *solução trivial* para o sistema. O sistema dado como exemplo admite a solução trivial $x_1 = x_2 = 0$. É importante ressaltar que isto significa que um sistema homogêneo sempre é possível (ou "compatível"), mas ele pode ter infinitas soluções (quando é indeterminado) ou somente uma (quando é determinado).

O Teorema 4.78 reafirma o que dissemos no exemplo 1.58, no Capítulo 1. Damos aqui uma demonstração diferente, usando notação matricial.

Teorema 4.78. *O conjunto de soluções para qualquer sistema homogêneo de equações lineares é um espaço vetorial.*

Demonstração. As soluções são claramente um subconjunto de $\mathbb{R}^n$ (ou K^n para algum corpo K), portanto somente precisamos provar que é subespaço de $\mathbb{R}^n$.

i) O vetor zero pertence ao conjunto, porque $\mathbf{0}$ é solução.

ii) A multiplicação de uma solução por escalar resulta em outra solução:

$$c(A\mathbf{x}) = c \cdot 0$$
$$A(c\mathbf{x}) = 0$$

E portanto $c\mathbf{x}$ é solução.

iii) A soma de duas soluções também resulta em outra.

$$A\mathbf{x} = A\mathbf{y} = 0$$
$$A\mathbf{x} + A\mathbf{y} = 0$$
$$A(\mathbf{x} + \mathbf{y}) = 0$$

E portanto $\mathbf{x} + \mathbf{y}$ é solução. ■

Antes de enunciar o próximo Teorema, relembramos a classificação de sistemas lineares[3], que um sistema pode ser *impossível*, *possível e indeterminado* (com infinitas soluções) ou *possível e determinado* (com somente uma solução.

Teorema 4.79. *Um sistema linear $A\mathbf{x} = \mathbf{b}$ é determinado se e somente se A tem inversa.*

Demonstração. Temos

$$A\mathbf{x} = \mathbf{b}$$
$$A^{-1}A\mathbf{x} = A^{-1}\mathbf{b}$$
$$\mathbf{x} = A^{-1}\mathbf{b}.$$

($\Rightarrow$) Como a inversa é única, sua existência garante que existe uma única solução para o sistema.
($\Leftarrow$) A existência de uma solução única também nos permite determinar A^{-1}. Se o sistema não tem solução, a inversa não pode existir. Se o sistema é indeterminado, há mais de um $\mathbf{x}$ que o satisfaz, e portanto A não pode ter uma única inversa. Não podendo haver uma única inversa, concluímos que a inversa não existe. ■

Exemplo 4.80. O sistema

$$\begin{cases} x_1 & & -x_3 = 3 \\ x_1 & +3x_2 & -x_3 = -6 \\ x_1 & & -2x_3 = -1 \end{cases}$$

pode ser reescrito na forma matricial como

$$\begin{pmatrix} 1 & 0 & -1 \\ 1 & 3 & -1 \\ 1 & 0 & -2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 3 \\ -6 \\ -1 \end{pmatrix}.$$

A inversa da matriz de coeficientes A é

$$A^{-1} = \begin{pmatrix} 2 & 0 & -1 \\ -1/3 & 1/3 & 0 \\ 1 & 0 & -1 \end{pmatrix},$$

[3] Esta classificação é dada na Definição α.4, no Apêndice α.

e a solução para o sistema é

$$\begin{aligned}\mathbf{x} &= A^{-1}\mathbf{b} \\ &= \begin{pmatrix} 2 & 0 & -1 \\ -1/3 & 1/3 & 0 \\ 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 3 \\ -6 \\ -1 \end{pmatrix} \\ &= \begin{pmatrix} 7 \\ -3 \\ 4 \end{pmatrix}\end{aligned}$$

◀

Exemplo 4.81. Mudando um único coeficiente no sistema linear do exemplo 4.80, obtemos

$$\begin{cases} x_1 & & -x_3 &=& 3 \\ x_1 & +3x_2 & -x_3 &=& -6 \\ x_1 & & -\mathbf{x_3} &=& -1 \end{cases}$$

que podemos descrever na forma matricial como

$$\begin{pmatrix} 1 & 0 & -1 \\ 1 & 3 & -1 \\ 1 & 0 & -\mathbf{1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 3 \\ -6 \\ -1 \end{pmatrix}.$$

A matriz de coeficientes não tem inversa, e o sistema não tem solução única (na verdade não tem solução nenhuma).

Mesmo que troquemos o vetor $\mathbf{b}$ *para qualquer outro vetor não-nulo, continuaremos sem solução única.* Observe que se mudarmos $\mathbf{b}$ para

$$\mathbf{b} = \begin{pmatrix} 3 \\ -6 \\ 3 \end{pmatrix},$$

a primeira e a terceira linhas do sistema passam a ser iguais: $A\mathbf{x} = \mathbf{b}$ seria o mesmo que

$$\begin{pmatrix} 1 & 0 & -1 \\ 1 & 3 & -1 \\ 1 & 0 & -\mathbf{1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 3 \\ -6 \\ 3 \end{pmatrix},$$

e teríamos então infinitas soluções da forma

$$x_1 = x_3 + 3, \quad x_2 = -3,$$

mas não teríamos uma única solução. ◀

Uma matriz está na forma escalonada se representa um sistema linear escalonado.

Definição 4.82 (Matriz escalonada por linhas e por colunas)**.** Seja A uma matriz. Se as condições (i) e (ii) abaixo valem para todas as linhas adjacentes i e j (com $i + 1 = j$), então dizemos que A está na forma *escalonada por linhas*.

i) Se j não é nula, i também não é;

ii) A quantidade de zeros à esquerda do primeiro elemento não-nulo em i é estritamente menor que a quantidade de zeros à esquerda do primeiro elemento não-nulo em j.

O *pivô* de uma linha é o primeiro (mais à esquerda) elemento não-nulo.

Se todo pivô da matriz for igual a um e as colunas dos pivôs não tiverem outras entradas não-nulas, a matriz está na forma escalonada *reduzida* por linhas.

Uma matriz está na forma *escalonada (reduzida) por colunas* se sua transposta está na forma escalonada (reduzida) por linhas. ♦

Exemplo 4.83. Todas as matrizes mostradas a seguir estão na forma escalonada.

$$A = \begin{pmatrix} 3 & 6 & 9 \\ 0 & 2 & 4 \\ 0 & 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & -1 & 2 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix} \quad C = \begin{pmatrix} 13 & 11 & 7 \\ 0 & 5 & 3 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \quad D = \begin{pmatrix} 0 & 3 & 5 & 7 \\ 0 & 0 & 0 & 9 \end{pmatrix}$$ ◀

Exemplo 4.84. Todas as matrizes mostradas as seguir estão na forma escalonada *reduzida* por linhas.

$$A = \begin{pmatrix} 1 & 5 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \end{pmatrix} \quad C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 8 \\ 0 & 0 & 1 & 9 \end{pmatrix}$$ ◀

Observe que se A é a matriz aumentada de um sistema linear, a forma escalonada reduzida por linhas identifica claramente a solução. Por exemplo, na matriz B do Exemplo 4.84, temos $x_1 = 2$, $x_2 = 3$, e a linha adicional não faz diferença. Já na matriz C, temos $x_1 = 0$, $x_2 = 8$ e $x_3 = 9$.

Claramente, a forma escalonada por colunas é obtida usando as mesmas operações que resultam na forma escalonada por linhas, exceto que as operações são realizadas na transposta (ou seja, são realizadas nas colunas e não nas linhas).

Exemplo 4.85. Todas as matrizes mostradas as seguir estão na forma escalonada por colunas.

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 3 & 4 & 0 \\ 0 & 9 & 1 \end{pmatrix} \quad B = \begin{pmatrix} -5 & 0 & 0 \\ 0 & 4 & 0 \\ 2 & 0 & 0 \end{pmatrix} \quad C = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ -4 & 5 & 9 & 0 \end{pmatrix}$$ ◀

Exemplo 4.86. Todas as matrizes mostradas as seguir estão na forma escalonada *reduzida* por colunas.

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 3 & 9 \end{pmatrix}$$ ◀

4.6.1 Eliminação de Gauss

Nesta seção revemos o método da eliminação de Gauss para resolução de sistemas de equações lineares usando matrizes elementares.

Definição 4.87 (Matriz aumentada)**.** Seja $A\mathbf{x} = \mathbf{b}$ um sistema de equações lineares com m equações e n variáveis. Então a *matriz aumentada* deste sistema é a matriz $m \times n + 1$ que tem as colunas de A seguidas da única coluna de $\mathbf{b}$,

$$\left(A \;\vdots\; \mathbf{b} \right).$$ ♦

Exemplo 4.88. O sistema linear

$$\begin{cases} 2x_1 + 3x_2 - x_3 = 2 \\ 3x_1 - x_2 = 1 \\ -x_1 - x_2 + 8x_3 = 4 \end{cases}$$

é descrito em forma matricial como

$$\begin{pmatrix} 2 & 3 & -1 \\ 3 & -1 & 0 \\ -1 & -1 & 8 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 4 \end{pmatrix}.$$

A matriz aumentada do sistema é

$$\left(\begin{array}{ccc|c} 2 & 3 & -1 & 2 \\ 3 & -1 & 0 & 1 \\ -1 & -1 & 8 & 4 \end{array}\right)$$ ◀

A solução de sistemas triangulares (na forma escalonada) pode ser feita na forma matricial da mesma maneira que quando é usada a representação sem matrizes. O processo de eliminação de Gauss consiste na aplicação sucessiva de operações elementares sobre o sistema linear. Quando representamos o sistema como matriz aumentada, cada aplicação de operação elementar é uma multiplicação. O processo de eliminação de Gauss consiste em multiplicar sucessivamente a matriz aumentada por matrizes elementares.

Lembramos aqui que normalmente não realizamos operações elementares sem ordem definida. Em cada fase do algoritmo, transformamos em zero a parte inferior de uma das colunas da matriz, processando as colunas da esquerda para a direita. A seguir temos um exemplo para um sistema com 3 variáveis e 4 equações (que resulta em uma matriz quadrada de ordem 4). Os pivôs estão marcados com fundo cinza. Para simplificar a exposição, não ilustramos trocas de linhas.

$$\overbrace{\left(\begin{array}{cccc} \cellcolor{gray!20}a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array}\right) \to \left(\begin{array}{cccc} \cellcolor{gray!20}a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ 0 & a_{42} & a_{43} & a_{44} \end{array}\right) \to \left(\begin{array}{cccc} \cellcolor{gray!20}a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ 0 & a_{32} & a_{33} & a_{34} \\ 0 & a_{42} & a_{43} & a_{44} \end{array}\right) \to \left(\begin{array}{cccc} \cellcolor{gray!20}a_{11} & a_{12} & a_{13} & a_{14} \\ 0 & a_{22} & a_{23} & a_{24} \\ 0 & a_{32} & a_{33} & a_{34} \\ 0 & a_{42} & a_{43} & a_{44} \end{array}\right)}^{\text{FASE 1}}$$

$$\to \overbrace{\left(\begin{array}{cccc} a_{11} & \cellcolor{gray!20}a_{12} & a_{13} & a_{14} \\ 0 & a_{22} & a_{23} & a_{24} \\ 0 & a_{32} & a_{33} & a_{34} \\ 0 & 0 & a_{43} & a_{44} \end{array}\right) \to \left(\begin{array}{cccc} a_{11} & \cellcolor{gray!20}a_{12} & a_{13} & a_{14} \\ 0 & a_{22} & a_{23} & a_{24} \\ 0 & 0 & a_{33} & a_{34} \\ 0 & 0 & a_{43} & a_{44} \end{array}\right)}^{\text{FASE 2}} \to \overbrace{\left(\begin{array}{cccc} a_{11} & a_{12} & \cellcolor{gray!20}a_{13} & a_{14} \\ 0 & a_{22} & a_{23} & a_{24} \\ 0 & 0 & a_{33} & a_{34} \\ 0 & 0 & 0 & a_{44} \end{array}\right)}^{\text{FASE 3}}$$

Exemplo 4.89. Considere o sistema a seguir.

$$\begin{cases} 2x_1 - x_2 + 4x_3 = 9 \\ x_1 - x_2 = 4 \\ -x_1 + 4x_2 - x_3 = 1 \end{cases}$$

Este sistema pode ser representado por

$$\left(\begin{array}{ccc|c} 2 & -1 & 4 & 9 \\ 1 & -1 & 0 & 4 \\ -1 & 4 & -1 & 1 \end{array}\right).$$

Aplicamos operações elementares até chegar a uma matriz triangular superior:

$$\left(\begin{array}{ccc|c} 2 & -1 & 4 & 9 \\ 1 & -1 & 0 & 4 \\ -1 & 4 & -1 & 1 \end{array}\right) \xrightarrow{E_{3+1/2L1}} \left(\begin{array}{ccc|c} 2 & -1 & 4 & 9 \\ 1 & -1 & 0 & 4 \\ 0 & 7/2 & 1 & 11/2 \end{array}\right) \xrightarrow{E_{2-1/2L1}} \left(\begin{array}{ccc|c} 2 & -1 & 4 & 9 \\ 0 & -1/2 & -2 & -1/2 \\ 0 & 7/2 & 1 & 11/2 \end{array}\right) \xrightarrow{E_{3+7L2}}$$

$$\left(\begin{array}{ccc|c} 2 & -1 & 4 & 9 \\ 0 & -1/2 & -2 & -1/2 \\ 0 & 0 & -13 & 2 \end{array}\right) \xrightarrow{E_{1/2L1}, E_{-2L2}, E_{-1/13L3}} \left(\begin{array}{ccc|c} 1 & -1/2 & 2 & 9/2 \\ 0 & 1 & 4 & 1 \\ 0 & 0 & 1 & -2/13 \end{array}\right)$$

E substituindo as variáveis obtemos o resultado

$$\begin{aligned} x_1 &= 73/13, \\ x_2 &= 21/13, \\ x_3 &= -2/13. \end{aligned}$$

Cada uma das operações é uma multiplicação por matriz elementar. Por exemplo, a primeira operação é

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1/2 & 0 & 1 \end{pmatrix} \left(\begin{array}{ccc|c} 2 & -1 & 4 & 9 \\ 1 & -1 & 0 & 4 \\ -1 & 4 & -1 & 1 \end{array}\right) = \left(\begin{array}{ccc|c} 2 & -1 & 4 & 9 \\ 1 & -1 & 0 & 4 \\ 0 & 7/2 & 1 & 11/2 \end{array}\right).$$

O Exercício 111 pede as outras matrizes usadas. ◀

Cálculo da inversa

Podemos calcular a inversa de uma matriz usando operações elementares.

Método 4.90. Escreva a matriz lado a lado com a identidade.

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \dots & \dots & 1 \end{pmatrix}.$$

Realize operações elementares na matriz do lado esquerdo até transformá-la na identidade. Cada operação que realizar no lado esquerdo, realize também na matriz do lado direito.

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \dots & \dots & 1 \end{pmatrix}$$

$$\downarrow$$
$$E_1$$
$$E_2$$
$$\vdots$$
$$E_k$$
$$\downarrow$$

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \dots & \dots & 1 \end{pmatrix} \qquad \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & & b_{2n} \\ \vdots & & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix}$$

Ao terminar, a matriz à direita será $B = A^{-1}$. ●

Exemplo 4.91. Inverteremos a matriz

$$A = \begin{pmatrix} 2 & -1 & 4 \\ 0 & 1 & 0 \\ 0 & -5 & 6 \end{pmatrix}.$$

Começamos escrevendo $\mathcal{I}$ ao lado de A:

$$\begin{pmatrix} 2 & -1 & 4 \\ 0 & 1 & 0 \\ 0 & -5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Somamos 5 vezes L_2 em L_3, depois dividimos L_3 por 6:

$$\begin{pmatrix} 2 & -1 & 4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 5/6 & 1/6 \end{pmatrix}$$

Somamos L_2 a L_1:

$$\begin{pmatrix} 2 & 0 & 4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 5/6 & 1/6 \end{pmatrix}$$

Somamos $-4L_3$ a L_1:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -7/3 & -2/3 \\ 0 & 1 & 0 \\ 0 & 5/6 & 1/6 \end{pmatrix}$$

Finalmente, dividimos L_1 por 2:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1/2 & -7/6 & -1/3 \\ 0 & 1 & 0 \\ 0 & 5/6 & 1/6 \end{pmatrix}$$

A matriz à direita é a inversa de A:

$$\begin{pmatrix} 2 & -1 & 4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1/2 & -7/6 & -1/3 \\ 0 & 1 & 0 \\ 0 & 5/6 & 1/6 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$ ◀

Este método pode ser útil se quisermos resolver mais de um sistema com os mesmos coeficientes. O exercício 109 pede a demonstração do teorema a seguir, que enuncia a corretude do método.

Teorema 4.92. *O método 4.90 sempre produzirá a inversa de qualquer matriz não singular.*

4.6.2 Decomposição LU

Definição 4.93 (Decomposição LU)**.** Seja A uma matriz quadrada. Se existem L e U tais que U é triangular superior, L é triangular inferior, e $A = LU$, então LU é a *decomposição LU* de A.

Se a diagonal de L só contém uns, esta é a *decomposição de Doolitle*. Se a diagonal de U só contém uns, é a *decomposição de Crout* ♦

Exemplo 4.94. Seja

$$A = \begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix}$$

Temos

$$A = \begin{pmatrix} 1 & 0 \\ 1/2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 0 & 7/2 \end{pmatrix}. \qquad \blacktriangleleft$$

Teorema 4.95. *Seja A uma matriz quadrada tal que*

$$E_k E_{k-1} \dots E_1 A = U,$$

onde as matrizes E_i são elementares que não realizam trocas de linhas, e U é diagonal superior (ou seja, A pode ser escalonada sem trocas de linhas). Então A admite fatoração LU.

Demonstração. Suponha que A necessite de k passos para ser escalonada. Realizamos o escalonamento de A, mas descrevendo-a inicialmente como

$$A = \mathcal{I}A.$$

Observe que a matriz identidade, $\mathcal{I}$, é triangular inferior. Aplicaremos operações elementares em A até transformá-la em U, escalonada, e consequentemente triangular superior. A aplicação destas operações modificará a matriz identidade, à esquerda, mas ela será mantida triangular inferior durante todo o processo.

$$\begin{aligned} A &= \mathcal{I}A \\ &= X^{(1)}A^{(1)} && (E_1 A = A^{(1)}) \\ &= X^{(2)}A^{(2)} && (E_2 E_1 A = A^{(2)}) \\ &\vdots \\ &= X^{(k)}A^{(k)} \\ &= X^{(k)}U. \end{aligned}$$

Se realizarmos operações elementares somente em $A^{(i)}$, para que a multiplicação $X^{(i)}A^{(i)}$ continue sendo igual a A, teremos que multiplicar $X^{(i)}$ pela matriz elementar inversa – e multiplicaremos *à direita* de $X^{(i)}$:

$$\begin{aligned} &\left(X^{(i)}E^{-1}\right)\left(EA^{(i)}\right) \\ &= X^{(i)}\big(\underbrace{E^{-1}E}_{=\mathcal{I}}\big)A^{(i)} \\ &= X^{(i)}\mathcal{I}A^{(i)} = A. \end{aligned}$$

Olhamos para o efeito das duas operações elementares. Suponha que pivô atual é o da j-ésima coluna Y_{jj}, e que pretendemos modificar a i-ésima linha, com $i > j$ (ou seja, uma linha abaixo do pivô).

- E realizará uma modificação na *linha* i, mas somente os elementos *depois* (abaixo) da posição j serão modificados (os anteriores eram zero).
- E^{-1} realizará uma modificação na *coluna* i, mas somente os elementos *antes* (à esquerda) da posição j serão modificados (os da direita eram zero).

Assim, a aplicação das duas operações não desfaz a parte escalonada por linhas de $X^{(i)}$, e nem a parte escalonada por colunas de $A^{(i)}$. O resultado será

$$A = LU,$$

onde $L = X^{(k)}$, triangular inferior,e $U = A^{(k)}$, triangular superior. ■

A demonstração do teorema 4.95 nos dá um método para encontrar a decomposição LU de uma matriz.

Método 4.96 (Decomposição LU)**.** Descreva A como $\mathcal{I}A$.

$$A = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & 0 \\ 0 & \cdots & & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & a_{2n} \\ \vdots & & \ddots & \cdots \\ a_{n1} & \cdots & & a_{nn} \end{pmatrix}$$

Use o método da eliminação de Gauss transformar a matriz da direita em triangular superior, escalonando-a, mas sempre que aplicar a operação elementar nas linhas da matriz à direita, aplique sua inversa nas colunas da matriz à esquerda. Quando a matriz à direita estiver escalonada, a da esquerda será triangular inferior. ●

Exemplo 4.97. Obteremos a decomposição LU da matriz

$$\begin{pmatrix} 2 & 3 & -1 \\ 2 & 1 & 5 \\ 4 & 0 & 7 \end{pmatrix}.$$

Durante o processo, mostraremos tanto L como U. Denotamos por U_i a i-ésima linha de U. Começamos com $A = \mathcal{I}A$.

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & -1 \\ 2 & 1 & 5 \\ 4 & 0 & 7 \end{pmatrix} \xrightarrow{U_2 \leftarrow U_2 - U_1} = \overbrace{\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}^{L} \overbrace{\begin{pmatrix} 2 & 3 & -1 \\ 0 & -2 & 6 \\ 4 & 0 & 7 \end{pmatrix}}^{U}$$

$$\xrightarrow{U_3 \leftarrow U_3 - 2U_1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & -1 \\ 0 & -2 & 6 \\ 0 & -6 & 9 \end{pmatrix} \xrightarrow{U_3 \leftarrow U_3 - 3U_2} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & -1 \\ 0 & -2 & 6 \\ 0 & 0 & -9 \end{pmatrix} \quad ◀$$

Se uma matriz A precisa de permutação de linhas para ser escalonada, não admite decomposição LU. Podemos, no entanto, decompô-la de forma parecida com a decomposição LU.

Teorema 4.98. *Toda matriz quadrada A pode ser decomposta em $A = PLU$, onde P é uma matriz de permutação; L é triangular inferior; e U é triangular superior.*

Demonstração. Se aplicarmos o método de decomposição LU que descrevemos, mas permitirmos trocas de linhas, também trocaremos as *colunas* da matriz da esquerda, e por isso ela pode não terminar o processo como triangular inferior.

No entanto, estas trocas podem ser representadas por uma matriz de de permutação P. Ao invés de manter duas matrizes, iniciando com $\mathcal{I}a$, mantemos três matrizes, começando com $\mathcal{I}\mathcal{I}A$:

$$A = \mathcal{I}\mathcal{I}A$$

$$
\begin{aligned}
&= P^{(1)}X^{(1)}A^{(1)} && (E_1A = A^{(1)})\\
&= P^{(2)}X^{(2)}A^{(2)} && (E_2E_1A = A^{(2)})\\
&\vdots\\
&= P^{(k)}X^{(k)}A^{(k)}\\
&= P^{(k)}X^{(k)}U.
\end{aligned}
$$

Quando uma operação de troca de linha for aplicada em $A^{(i)}$, as colunas de $X^{(i)}$ ficarão na ordem errada. Aplicamos uma troca de linhas em $X^{(i)}$ e sua inversa nas colunas de $P^{(i)}$:

$$P^{(i)}E^{-1}EX^{(i)}.$$

Desta forma mantemos X como triangular inferior. Durante todo o processo P será matriz de permutação, e ao final teremos

$$A = PLU. \qquad \blacksquare$$

Exemplo 4.99. Considere a matriz

$$\begin{pmatrix} 0 & 4 & 1 & 4\\ 1 & 2 & 1 & 1/2\\ 12 & 24 & 6 & 1\\ 2 & -8 & 5 & 7/6 \end{pmatrix}$$

Esta matriz não pode ser escalonada sem troca de linhas. O processo para deixá-la na forma triangular deverá necessariamente trocar as duas primeiras linhas de ordem, já que não é possível dividir pelo elemento $a_{11} = 0$.

Começamos com $A = \mathit{II}A$.

$$
\begin{aligned}
A &= \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix}\begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix}\begin{pmatrix} 0&4&1&4\\1&2&1&1/12\\12&24&6&1\\2&-8&5&7/6 \end{pmatrix}\\
&= \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix}\overbrace{\begin{pmatrix} 0&0&1&0\\0&1&0&0\\1&0&0&0\\0&0&0&1 \end{pmatrix}}^{C_1\leftrightarrow C_3}\overbrace{\begin{pmatrix} 12&24&6&1\\1&2&1&1/12\\0&4&1&4\\2&-8&5&7/6 \end{pmatrix}}^{L_1\leftrightarrow L_3}\\
&= \overbrace{\begin{pmatrix} 0&0&1&0\\0&1&0&0\\1&0&0&0\\0&0&0&1 \end{pmatrix}}^{C_1\leftrightarrow c_3}\overbrace{\begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix}}^{L_1\leftrightarrow L_3}\begin{pmatrix} 12&24&6&1\\1&2&1&1/12\\0&4&1&4\\2&-8&5&7/6 \end{pmatrix}\\
&= \begin{pmatrix} 0&0&1&0\\0&1&0&0\\1&0&0&0\\0&0&0&1 \end{pmatrix}\overbrace{\begin{pmatrix} 1&0&0&0\\1/12&1&0&0\\0&0&1&0\\1/6&0&0&1 \end{pmatrix}}^{\substack{C_1=C_1+C_2/12\\C_1=C_1+C_4/6}}\overbrace{\begin{pmatrix} 12&24&6&1\\0&0&1/2&0\\0&4&1&4\\0&-12&4&1 \end{pmatrix}}^{\substack{L_2=L_2-L_1/12\\L_4=L_4-L_1/6}}
\end{aligned}
$$

$$
\begin{aligned}
&= \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \overbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1/12 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1/6 & 0 & 0 & 1 \end{pmatrix}}^{C_2 \leftrightarrow C_3} \overbrace{\begin{pmatrix} 12 & 24 & 6 & 1 \\ 0 & 4 & 1 & 4 \\ 0 & 0 & 1/2 & 0 \\ 0 & -12 & 4 & 1 \end{pmatrix}}^{L_2 \leftrightarrow L_3} \\
&= \overbrace{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}^{C_2 \leftrightarrow C_3} \overbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1/12 & 0 & 1 & 0 \\ 1/6 & 0 & 0 & 1 \end{pmatrix}}^{L_2 \leftrightarrow L_3} \begin{pmatrix} 12 & 24 & 6 & 1 \\ 0 & 4 & 1 & 4 \\ 0 & 0 & 1/2 & 0 \\ 0 & -12 & 4 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \overbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1/12 & 0 & 1 & 0 \\ 1/6 & -3 & 0 & 1 \end{pmatrix}}^{C_2 = CL_2 - 3C_4} \overbrace{\begin{pmatrix} 12 & 24 & 6 & 1 \\ 0 & 4 & 1 & 4 \\ 0 & 0 & 1/2 & 0 \\ 0 & 0 & 7 & 13 \end{pmatrix}}^{L_4 = L_4 + 3L_2} \\
&= \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \overbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1/12 & 0 & 1 & 0 \\ 1/6 & -3 & 14 & 1 \end{pmatrix}}^{C_3 = C_3 + 14C_4} \overbrace{\begin{pmatrix} 12 & 24 & 6 & 1 \\ 0 & 4 & 1 & 4 \\ 0 & 0 & 1/2 & 0 \\ 0 & 0 & 0 & 13 \end{pmatrix}}^{L_4 = L_4 - 14L_3}.
\end{aligned}
$$

Temos finalmente $A = PLU$, onde P é matriz de permutação, L é triangular inferior e U é triangular superior. ◀

Teorema 4.100. *Se uma matriz admite decomposição LU, também pode ser decomposta em* LDU*, onde* L *é triangular estritamente inferior,* U *é triangular estritamente superior, e* D *é uma matriz diagonal.*

Resolução de múltiplos sistemas lineares via decomposição LU

Passamos agora ao uso da decomposição LU na solução de sistemas lineares.

Método 4.101 (Resolução de sistemas lineares por decomposição LU)**.** Suponha que queiramos resolver o sistema $A\mathbf{x} = \mathbf{b}$. Se A tem fatoração LU, podemos usar o método a seguir.

- Decomponha A em LU. Agora temos $LU\mathbf{x} = \mathbf{b}$
- Seja $\mathbf{y} = U\mathbf{x}$. Resolvemos $L\mathbf{y} = \mathbf{b}$
- Como L é triangular, o sistema é resolvido facilmente e obtemos $\mathbf{y}$.
- Finalmente resolvemos $U\mathbf{x} = \mathbf{y}$, que também é fácil porque U é triangular, e obtemos $\mathbf{x}$. ●

Suponha que queiramos resolver diversos sistemas com a mesma matriz A, mas com diferentes vetores constantes $\mathbf{b}_1, \mathbf{b}_2$, etc. Podemos calcular a fatoração LU de A (que é a parte mais demorada do processo) e posteriormente resolver $LU\mathbf{x} = \mathbf{b}_i$ facilmente. Por esse motivo o método LU é normalmente preferível à eliminação de Gauss.

Exemplo 4.102. Suponha que queiramos resolver os sistemas

$$\text{(i)} \quad A\mathbf{x} = \mathbf{b},$$

$$(ii)\ A\mathbf{x}' = \mathbf{c},$$
$$(iii)\ A\mathbf{x}'' = \mathbf{d},$$

onde

$$A = \begin{pmatrix} 1 & 2 & -1 \\ 2 & 6 & -3 \\ -2 & 2 & 4 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} 1 \\ 1 \\ 10 \end{pmatrix}, \quad \mathbf{c} = \begin{pmatrix} 0 \\ 0 \\ 15 \end{pmatrix}, \quad \mathbf{d} = \begin{pmatrix} 4 \\ 2 \\ -20 \end{pmatrix}.$$

Primeiro calculamos a decomposição LU de A:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ -2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & -1 \\ 0 & 2 & -1 \\ 0 & 0 & 5 \end{pmatrix}.$$

Esta decomposição, que requer muito trabalho, é feita *uma única vez.* Agora resolvemos os tres sistemas por simples substituição.

(i) Resolvemos $A\mathbf{x} = \mathbf{b}$, ou $LU\mathbf{x} = \mathbf{b}$. Seja $\mathbf{w} = U\mathbf{x}$. Resolvemos $L\mathbf{w} = \mathbf{b}$ facilmente, porque L é triangular:

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ -2 & 3 & 1 \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 10 \end{pmatrix}$$

Temos

$$w_1 = 1, \ \ w_2 = -1, \ \ w_3 = 15.$$

Agora resolvemos $U\mathbf{x} = \mathbf{w}$, também facilmente, porque U é triangular:

$$\begin{pmatrix} 1 & 2 & -1 \\ 0 & 2 & -1 \\ 0 & 0 & 5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 15 \end{pmatrix}$$

Obtemos

$$x_1 = 2, \ \ x_2 = 1, \ \ x_3 = 3.$$

(ii) resolvemos $A\mathbf{x}' = \mathbf{c}$, ou $LU\mathbf{x}' = \mathbf{c}$. Seja $\mathbf{y} = U\mathbf{x}'$. Resolvemos $L\mathbf{y} = \mathbf{c}$ facilmente, porque L é triangular:

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ -2 & 3 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 15 \end{pmatrix}$$

Temos evidentemente

$$y_1 = 0, \ \ y_2 = 0, \ \ y_3 = 15.$$

Agora resolvemos $U\mathbf{x}' = \mathbf{y}$, também facilmente, porque U é triangular:

$$\begin{pmatrix} 1 & 2 & -1 \\ 0 & 2 & -1 \\ 0 & 0 & 5 \end{pmatrix} \begin{pmatrix} x_1' \\ x_2' \\ x_3' \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 15 \end{pmatrix}$$

Obtemos

$$x_1' = 0, \ \ x_2' = 3/2, \ \ x_3' = 3.$$

(iii) Novamente, resolvemos $A\mathbf{x}'' = \mathbf{c}$, ou $LU\mathbf{x}'' = \mathbf{c}$. Seja $\mathbf{z} = U\mathbf{x}''$. Resolvemos $L\mathbf{z} = \mathbf{c}$ facilmente, porque L é triangular:

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ -2 & 3 & 1 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \begin{pmatrix} 4 \\ 2 \\ -20 \end{pmatrix}$$

Temos

$$z_1 = 4, \quad z_2 = -6, \quad z_3 = 6.$$

Agora resolvemos $U\mathbf{x}'' = \mathbf{z}$, também facilmente, porque U é triangular:

$$\begin{pmatrix} 1 & 2 & -1 \\ 0 & 2 & -1 \\ 0 & 0 & 5 \end{pmatrix} \begin{pmatrix} x_1'' \\ x_2'' \\ x_3'' \end{pmatrix} = \begin{pmatrix} 4 \\ -6 \\ 6 \end{pmatrix}$$

Obtemos

$$x_1'' = 10, \quad x_2'' = -12/5, \quad x_3'' = 6/5. \qquad \blacktriangleleft$$

Como já vimos, a matriz A pode não admitir decomposição LU. Neste caso calculamos a decomposição PLU de A e usamos o método abaixo.

Método 4.103 (Resolução de sistemas lineares por decomposição PLU)**.** Suponha que queiramos resolver o sistema $A\mathbf{x} = \mathbf{b}$. Se A *não* tem fatoração LU, podemos usar o método a seguir.

- Decomponha A em $PA = LU$. Agora temos $PLU = P\mathbf{b}$.
- Permute os elementos de $\mathbf{b}$ – ou seja, calcule $\mathbf{d} = P\mathbf{b}$
- Seja $\mathbf{y} = U\mathbf{x}$. Resolvemos $L\mathbf{y} = \mathbf{d}$
- Como L é triangular, o sistema é resolvido facilmente e obtemos $\mathbf{y}$.
- Finalmente resolvemos $U\mathbf{x} = \mathbf{y}$, que também é fácil porque U é triangular, e obtemos $\mathbf{x}$. ●

4.6.3 Estabilidade numérica

A resolução de sistemas lineares envolve repetidos passos de computação numérica, e isso normalmente resulta em erros de arredondamento que tornam-se maiores no decorrer do processo. Dizemos que estes algoritmos tem um problema de *estabilidade numérica*. Uma maneira de mitigar este problema é tentar evitar divisões por números muito pequenos, através de permutação de linhas ou multiplicando linhas com coeficientes pequenos por constantes grandes. Mais detalhes sobre métodos para computar soluções para sistemas lineates podem ser obtidos na literatura de Cálculo Numérico – por exemplo, no livro de Neide Franco [Fra07].

★ 4.7 Matrizes complexas

Podemos também representar transformações lineares em espaços vetoriais sobre corpos complexos, sendo portanto útil conhecer um pouco da álgebra das matrizes complexas.

Exemplo 4.104. A matriz

$$T = \begin{pmatrix} -i & 3 \\ 1 & 2 \end{pmatrix}$$

representa uma transformação linear.

Se o domínio for $\mathbb{R}^2$, temos $T : \mathbb{R}^2 \to \mathbb{C}^2$.

Se o domínio for $\mathbb{C}^2$, temos $T : \mathbb{C}^2 \to \mathbb{C}^2$.

Se o domínio for a reta X composta pelos pontos $(3x, ix)$, com $x \in \mathbb{R}$, mesmo tendo domínio complexo, a transformação é

$$T(x, 3x)^T = (-i(3x) + 3(ix), 3x + 2x)^T = (0, 3x + 2x)^T,$$

e a imagem de T está contida em $\mathbb{R}^2$, logo poderíamos definir $\mathbb{R}^2$ como contradomínio, e teríamos $T : X \to \mathbb{R}^2$. ◀

Definição 4.105. Se A é uma matriz complexa, $\overline{A}$ é a *matriz dos conjugados* de A, que contém os conjugados complexos dos elementos de A. ♦

Exemplo 4.106. Sejam

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 2+3i \end{pmatrix}, \quad B, = \begin{pmatrix} i & 0 \\ -i & 1 \end{pmatrix} \quad C = \begin{pmatrix} 2+i & 2-i \\ i\sqrt{2} & 1+\sqrt{3} \end{pmatrix}.$$

Então

$$\overline{A} = \begin{pmatrix} 1 & 2 \\ 0 & 2-3i \end{pmatrix}, \quad \overline{B}, = \begin{pmatrix} -i & 0 \\ i & 1 \end{pmatrix} \quad \overline{C} = \begin{pmatrix} 2-i & 2+i \\ -i\sqrt{2} & 1+\sqrt{3} \end{pmatrix}. \quad ◀$$

Definição 4.107 (Conjugado transposto)**.** O *conjugado transposto*, ou a *matriz adjunta* de uma matriz A é a transposta da matriz com os conjugados dos elementos de A:

$$A^H = \overline{A}^T,$$

Também é usada a notação A^*. ♦

Observe que se A somente tem elementos reais, então $A^H = A^T$.

Exemplo 4.108. Seja

$$A = \begin{pmatrix} 2-3i & 5 & i \\ -i & 0 & 1 \\ 0 & 1+2i & 1-i \end{pmatrix}$$

Então

$$A^H = \begin{pmatrix} 2+3i & i & 0 \\ 5 & 0 & 1-2i \\ -i & 1 & 1+i \end{pmatrix} \quad ◀$$

Teorema 4.109. *Sejam* A *e* B *matrizes complexas* $m \times n$*, e* z *um número complexo. Então*

i) $(A^H)^H = A$

ii) $(zA)^H = \overline{z}(A^H)$

iii) $(A + B)^H = A^H + B^H$

iv) $(AB)^H = B^H A^H$

v) Se A *tem inversa,* $(A^{-1})^H = (A^H)^{-1}$

4.8 Aplicações

4.8.1 Cálculo de uma única coluna da inversa [decomposição LU]

Se quisermos calcular somente uma coluna da inversa de uma matriz A, podemos obter sua fatoração LU e usar a matriz U para obter a coluna desejada. Para isto basta usar substituição:

$$U\mathbf{x} = \mathbf{e}_i$$

nos dará a i-ésima coluna da inversa.

Por exemplo,

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 1 & 0 & 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & -1/2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & -1/2 \end{pmatrix}$$

Usamos somente a matriz U para computar, por exemplo, a terceira coluna de A^{-1}. Resolvemos

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & -1/2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

e obtemos

$$\begin{aligned} x_1 &= 1 \\ x_2 &= 5/2 \\ x_3 &= -2 \end{aligned}$$

ou seja, a terceira coluna da inversa de A deve ser

$$\begin{pmatrix} 1 \\ 5/2 \\ -2 \end{pmatrix}.$$

De fato, a inversa de A é

$$\begin{pmatrix} 0 & 0 & 1 \\ -5/2 & 3/2 & 5/2 \\ 2 & -1 & -2 \end{pmatrix}$$

Este método requer menos esforço do que computar a inversa completamente.

4.8.2 Otimização linear [base; espaço-coluna; dimensão; fatoração LU]

Nesta seção introduzimos conceitos de otimização linear a partir de um exemplo.

Uma indústria fabrica tintas de dois tipos, A e B. Queremos saber quanto de cada tinta pode ser fabricado a fim de maximizar o lucro da empresa, levando em consideração as seguintes restrições:

i) Cada lote do tipo A tem, para a empresa, um custo de 4, e cada galão do tipo B custa 3, e o orçamento da empresa prevê que se gaste até 20 com a produção das tintas por semana. O lucro para um litro da tinta do tipo A é de 5, e para um do tipo B é 10.

ii) Três lotes da tinta A demoram 3h para serem produzidos, enquanto a mesma quantidade da tinta B demora 10h. A empresa tem 40 horas úteis disponíeis para a produção em uma semana

iii) A tinta A só é produzida por um fornecedor, que só oferece quatro lotes por semana, no máximo.

Estas são as *restrições* do problema. Chamamos de x_1 a quantidade de tinta do tipo A e x_2 a quantidade de tinta do tipo B. Queremos portanto maximizar o lucro,

$$z = 5x_1 + 10x_2. \tag{4.5}$$

Esta é a *função objetivo* que queremos otimizar.

Definição 4.110 (problema de programação linear)**.** Em um problema de programação linear, temos um conjunto de pontos definido por desigualdades ou igualdades lineares[4], e que podemos descrever como o conjunto de soluções de um sistema

$$A\mathbf{x} = \mathbf{b}.$$

Chamamos este conjunto de pontos de *região viável*.

Dentro da região viável, queremos encontrar o ponto $\mathbf{x}^*$ que maximiza o valor de uma função linear

$$\begin{aligned} f(\mathbf{x}) &= c_1x_1 + c_2x_2 + \cdots + c_nx_n \\ &= \mathbf{c}^T\mathbf{x}. \end{aligned}$$

Assim, um problema de programação linear pode ser descrito como

$$\begin{gathered} \text{maximize } \mathbf{c}^T\mathbf{x} \\ \text{sujeito a } A\mathbf{x} = \mathbf{b}, \\ \mathbf{x} \geq \mathbf{0}. \end{gathered}$$ ♦

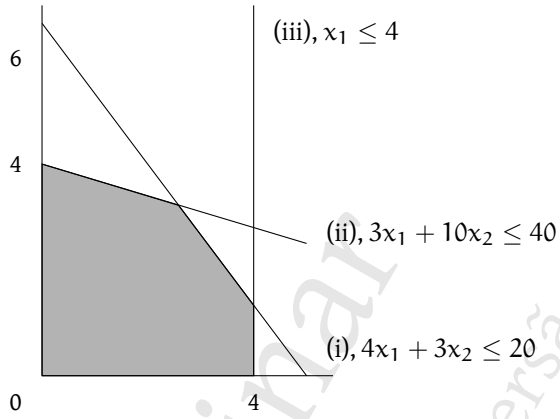
No problema que estamos modelando, as restrições que temos são:

$$\begin{array}{rcrcll} 4x_1 & + & 3x_2 & \leq & 20 & \text{(i)} \\ 3x_1 & + & 10x_2 & \leq & 40 & \text{(ii)} \\ x_1 & & & \leq & 4 & \text{(iii)} \end{array} \tag{4.6}$$

além, é claro, de $\mathbf{x} \geq \mathbf{0}$, uma vez que não faz sentido produzir quantidade negativa de tinta.

Temos portanto m restrições na forma de desigualdades, e duas variáveis. É útil visualizar graficamente a região definida por estas desigualdades.

[4]Note que $a_1x_1 + a_2x_2 + \cdots + a_nx_n \leq k$ é equivalente a $a_1x_2 + a_2x_2 + \cdots + a_nx_n + s \leq k, s \geq 0$



Assim, com as restrições (4.6) e a função objetivo (4.5), temos um problema de programação linear:

$$\begin{aligned} &\max \mathbf{c}^T\mathbf{x} \\ \text{s.a.:}\ &A\mathbf{x} = \mathbf{b}, \\ &\mathbf{x} \geq \mathbf{0} \end{aligned}$$

com

$$A = \begin{pmatrix} 4 & 3 \\ 3 & 10 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} 20 \\ 40 \\ 4 \end{pmatrix}, \quad \mathbf{c} = \begin{pmatrix} 5 \\ 10 \end{pmatrix}.$$

A região definida pelas desigualdades é chamada de *politopo*.

A solução ótima estará necessariamente num dos vértices do politopo. Como este é um problema pequeno, podemos enumerar as soluções definidas pelos vértices e determinar assim a melhor delas.

Agora observamos que cada desigualdade da forma

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \leq k$$

pode ser reescrita como

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n + \mathbf{s} = k,$$

usando uma *variável de folga* $s > 0$.

O sistema que modelamos, na forma matricial e usando igualdades, é $A\mathbf{v} = \mathbf{b}$:

$$\begin{matrix} x_1 & x_2 & s_1 & s_2 & s_3 \end{matrix}$$
$$\begin{pmatrix} 4 & 3 & 1 & 0 & 0 \\ 3 & 10 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ s_1 \\ s_2 \\ s_3 \end{pmatrix} = \begin{pmatrix} 20 \\ 40 \\ 4 \end{pmatrix},$$

onde s_1, s_2 e s_3 são as folgas das três desigualdades. Indicamos, acima da matriz, as variáveis relacionadas a cada coluna. Note que agora procuramos por uma solução em um espaço de dimensão maior (estávamos em $\mathbb{R}^2$, e quando passamos o problema para a forma de igualdade, caímos em $\mathbb{R}^5$).

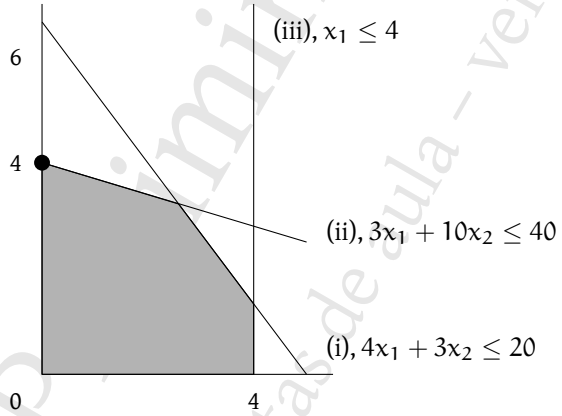
O espaço-coluna de A é $\mathbb{R}^3$, porque a matriz tem três colunas LI. Podemos formar bases para o espaço-coluna de A escolhendo quaisquer 3 colunas LI da matriz. Ao fazê-lo, estaremos escolhendo três das cinco variáveis. Dizemos que ao fazer isto estamos construíndo uma *solução básica*.

Definição 4.111. Seja $A\mathbf{x} = \mathbf{b}$ o conjunto de restrições de um programa linear com m restrições e n variáveis. Seja B uma matriz formada por m colunas de A (ou seja, as colunas de B são base para o espaço-coluna de A). As soluções de $B\mathbf{x} = \mathbf{b}$ são chamadas de *soluções básicas* para o problema. ♦

Por exemplo, considere o problema apresentado anteriormente. Se escolhermos as colunas de x_2, s_1, e s_3, teremos

$$\begin{pmatrix} \overset{x_2}{3} & \overset{s_1}{1} & \overset{s_3}{0} \\ 10 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_2 \\ s_1 \\ s_3 \end{pmatrix} = \begin{pmatrix} 20 \\ 40 \\ 4 \end{pmatrix}.$$

com $x_1 = s_2 = 0$; $x_2 = 4$; $s_1 = 8$; $s_3 = 4$.



Podemos formar bases diferentes para o espaço coluna de A, e cada base nos dará uma solução diferente. Além disso, o seguinte Teorema nos garante que estas soluções são pontos extremos do politopo.

Teorema 4.112. *Seja S o conjunto de soluções viáveis para um problema de programação linear. Uma solução $\mathbf{x}$ é básica se e somente se é ponto extremo de S.*

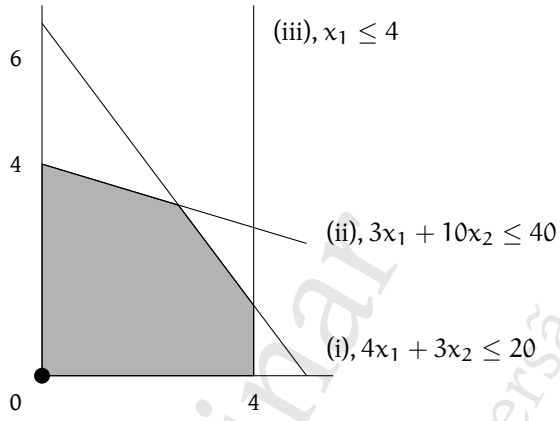
Como sabemos que só precisamos verificar os pontos extremos, podemos simplesmente verificar as soluções básicas. Isto também significa que nos pontos extremos (e portanto na solução ótima) teremos somente m variáveis diferentes de zero (incluindo as de folga).

Experimentamos agora com algumas bases.

Se usarmos s_1, s_2 e s_3 na base, teremos o ponto extremo na origem, e

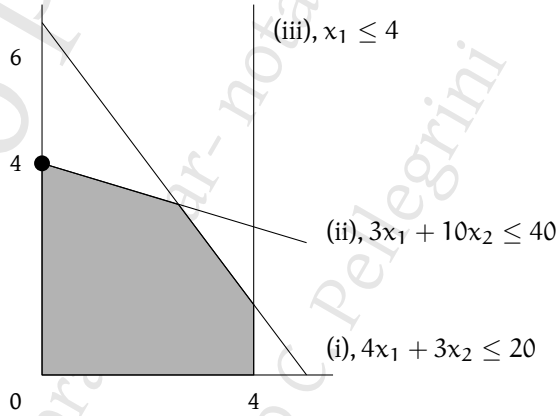
$$\begin{pmatrix} \overset{s_1}{1} & \overset{s_2}{0} & \overset{s_3}{0} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} = \begin{pmatrix} 20 \\ 40 \\ 4 \end{pmatrix}, \quad \begin{array}{l} x_1 = 0 \\ x_2 = 0 \\ s_1 = 20 \\ s_2 = 40 \\ s_3 = 4 \end{array} \quad z = 0.$$

com $x_1 = x_2 = 0$ (ou seja, usamos toda a folga em todas as restrições, e não demos valor positivo a nenhuma das variáveis).



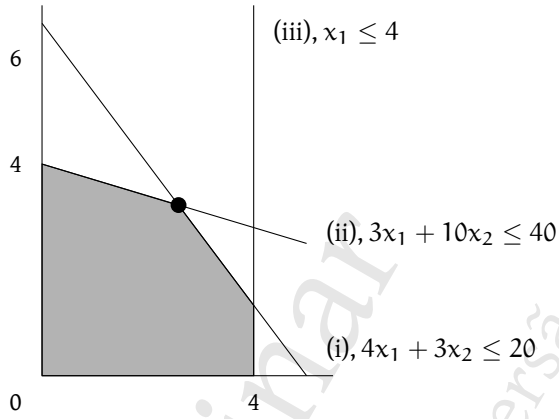
Se a base for x_2, s_1, s_3, teremos

$$\begin{pmatrix} x_2 & s_1 & s_3 \\ 3 & 1 & 0 \\ 10 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_2 \\ s_1 \\ s_3 \end{pmatrix} = \begin{pmatrix} 20 \\ 40 \\ 4 \end{pmatrix}, \quad \begin{array}{l} x_1 = 0 \\ x_2 = 4 \\ s_1 = 8 \\ s_2 = 0 \\ s_3 = 4 \end{array} \quad z = 40.$$



Se a base for x_1, x_2, s_3, teremos

$$\begin{pmatrix} x_1 & x_2 & s_3 \\ 4 & 3 & 0 \\ 3 & 10 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ s_3 \end{pmatrix} = \begin{pmatrix} 20 \\ 40 \\ 4 \end{pmatrix}, \quad \begin{array}{l} x_1 = 80/31 \approx 2.580 \\ x_2 = 100/31 \approx 3.225 \\ s_1 = 0 \\ s_2 = 0 \\ s_3 = 44/31 \approx 1.419 \end{array} \quad z = 1400/31 \approx 45.161.$$



Pode-se fazer o mesmo com todas as outras bases. A que tem maior valor é esta última que calculamos, e portanto a solução ótima para o problema é $x_1 = 80/31$ e $x_2 = 100/31$.

Terminamos o exemplo com duas variáveis, e agora olhamos brevemente para o caso em que temos mais variáveis e restrições, resumindo o que verificamos antes. Com m restrições e n variáveis, o problema por ser descrito como um *sistema de inequações lineares*,

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & \leq & b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & \leq & b_2 \\ & \vdots & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & \leq & b_m \end{array}$$

$$x_i \geq 0.$$

Cada inequação pode ser transformada em uma equação através da inclusão de uma *variável de folga*.

$$\begin{array}{rcl} a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n & \leq & b_i \\ \Updownarrow & & \\ a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n + \alpha_i s_i & = & b_i \end{array}$$

$$\alpha_i \geq 0.$$

Suponha que há apenas desigualdades do tipo $\leq$. Então adicionam-se m colunas às n já existentes.

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n + a_{1,n+1}s_1 & = & b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n + a_{2,n+2}s_2 & = & b_2 \\ & \vdots & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n + a_{m,n+m}s_m & = & b_m \end{array}$$

$$x_i, s_i \geq 0.$$

Se o problema só tem igualdades e há mais linhas do que colunas, podemos descartar linhas até obter uma matriz quadrada (porque as linhas excedentes são LD, e não modificam a solução do sistema); Um problema de otimização linear é descrito portanto por uma matriz com mais colunas do que linhas. Isso significa que há colunas LD, e que nem todas as colunas são necessárias para formar uma base para o espaço-coluna.

Cada base para o espaço coluna corresponde a uma *solução básica*.

Pode-se demonstrar que a solução ótima, se existir, é um ponto extremo, e consequentemente uma solução básica, e o que o algoritmo Simplex faz é percorrer cada uma destas soluções básicas até encontrar a ótima (o algoritmo Simplex as percorre de maneira inteligente, evitando enumerar todas elas – há $\binom{n}{m}$ possíveis bases!).

Normalmente, programas que realizam otimização linear não armazenam a base inteira. A fatoração LU de A é armazenada, e quando uma coluna da inversa é necessária, ela é calculada, como descrito na Seção 4.8.1.

O livro de Matousek [MG07] é u ma introdução à Programação Linear. Abordagens mais aprofundadas e detalhadas são encontradas nos livros de Bazaraa, Jarvis, e Sherali [BJS90], de Schrijver [Sch99], de de Bertsimas e Tsitsiklis [BT97] e de Luenberger e Ye [LY10].

4.8.3 Transformações em imagens [matriz de transformação]

Rotação por eixo canônico

Matrizes de rotação ao redor de um dos eixos da base canônica são descritas no Teorema 4.113, cuja demonstração é pedida no Exercício 115.

Teorema 4.113. *Em $\mathbb{R}^3$, seja $R_s(\alpha)$ a matriz de rotação* ao redor do eixo s*, pelo ângulo α. Para os três eixos da base canônica, temos*

$$R_x(\alpha) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\operatorname{sen}\alpha \\ 0 & \operatorname{sen}\alpha & \cos\alpha \end{pmatrix}, \quad R_y(\alpha) = \begin{pmatrix} \cos\alpha & 0 & -\operatorname{sen}\alpha \\ 0 & 1 & 0 \\ \operatorname{sen}\alpha & 0 & \cos\alpha \end{pmatrix}, \quad R_z(\alpha) = \begin{pmatrix} \cos\alpha & -\operatorname{sen}\alpha & 0 \\ \operatorname{sen}\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

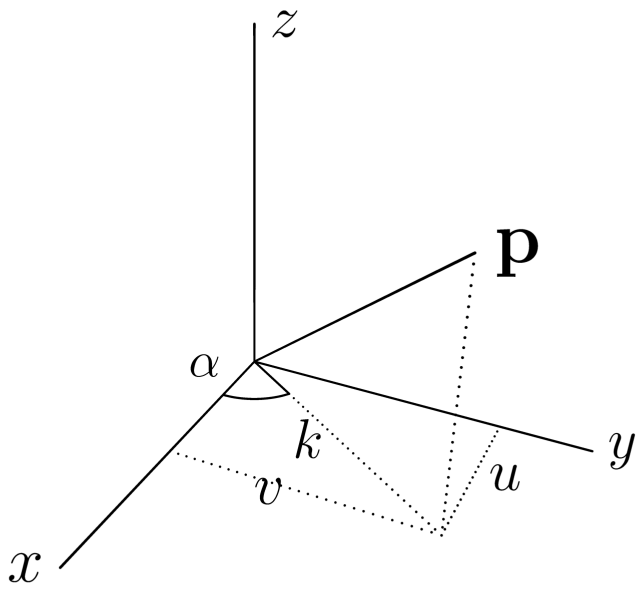
Rotação por eixo passando na origem

Teorema 4.114 (de Euler)**.** *Qualquer rotação passando pela origem em tres dimensões pode ser descrita como composição de rotações por tres eixos diferentes.*

Se quisermos realizar uma rotação por ângulo θ ao redor de um eixo qualquer passando pela origem (não necessariamente um dos três da base canônica), podemos usar o seguinte método.

0. escolha um ponto P, representado pelo vetor $(u, v, w)^T$ colinear com o eixo de rotação
1. aplique rotação por z, deixando o eixo de rotação no plano xz
2. aplique rotação por y, deixando o eixo de rotação colinear com z
3. realiza a rotação por θ ao redor do eixo z
4. desfaça (2)
5. desfaça (1)

Da Geometria Analítica, sabemos que a norma do vetor $(u, v, w)^T$ (o comprimento do segmento de reta indo da origem até P) é $q = \sqrt{u^2 + v^2 + w^2}$. A figura a seguir mostra o ângulo de rotação (α) que nos interessa para o passo (1), levando o ponto ao plano xz.



Verificamos que o comprimento do vetor projetado no plano xy é $k = \sqrt{u^2 + v^2}$. Da figura também

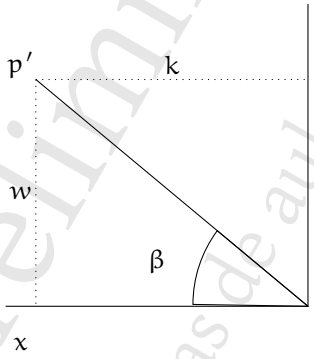
obtemos que

$$\cos\alpha = u/\sqrt{u^2+v^2}$$
$$\operatorname{sen}\alpha = v/\sqrt{u^2+v^2}$$

A matriz de rotação do passo (1) pode ser escrita portanto substituindo os valores de $\cos\alpha$ e $\operatorname{sen}\alpha$:

$$R_1 = \begin{pmatrix} u/\sqrt{u^2+v^2} & v/\sqrt{u^2+v^2} & 0 \\ -v/\sqrt{u^2+v^2} & u/\sqrt{u^2+v^2} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Olhamos agora a figura com o ponto já no plano xz, representado por p'. O ângulo que nos interessa para o passo (2), β, é mostrado na próxima figura.



Novamente, idntificamos seno e cosseno do ângulo na figura:

$$\cos\beta = w/\sqrt{u^2+v^2+w^2}$$
$$\operatorname{sen}\beta = \sqrt{u^2+v^2}/\sqrt{u^2+v^2+w^2}$$

A rotação (2) é realizada pela matriz

$$R_2 = \begin{pmatrix} w/\sqrt{u^2+v^2+w^2} & 0 & -\sqrt{u^2+v^2}/\sqrt{u^2+v^2+w^2} \\ 0 & 1 & 0 \\ \sqrt{u^2+v^2}/\sqrt{u^2+v^2+w^2} & 0 & w/\sqrt{u^2+v^2+w^2} \end{pmatrix}$$

A matriz de rotação final é $R_1^{-1}R_2^{-1}R_z(\theta)R_2R_1$, que exibimos a seguir. Seja $Q = \sqrt{u^2+v^2+w^2}$. Então

$$R_1^{-1}R_2^{-1}R_z(\theta)R_2R_1 = \frac{1}{q}\begin{pmatrix} u^2+(v^2+w^2)\cos\theta & uv(1-\cos\theta)-wq\sin\theta & uw(1-\cos\theta)+vq\sin\theta \\ uv(1-\cos\theta)+wq\sin\theta & v^2+(u^2+w^2)\cos\theta & vw(1-\cos\theta)-uq\sin\theta \\ uw(1-\cos\theta)-vq\sin\theta & vw(1-\cos\theta)+uq\sin\theta & w^2+(u^2+v^2)\cos\theta \end{pmatrix}$$

Se escolhermos o vetor do eixo de rotação de forma que $q = u^2+v^2+w^2 = 1$, temos

$$R_1^{-1}R_2^{-1}R_z(\theta)R_2R_1 = \begin{pmatrix} u^2+(v^2+w^2)\cos\theta & uv(1-\cos\theta)-w\sin\theta & uw(1-\cos\theta)+v\sin\theta \\ uv(1-\cos\theta)+w\sin\theta & v^2+(u^2+w^2)\cos\theta & vw(1-\cos\theta)-u\sin\theta \\ uw(1-\cos\theta)-v\sin\theta & vw(1-\cos\theta)+u\sin\theta & w^2+(u^2+v^2)\cos\theta \end{pmatrix}$$

Translações

Para translações em $\mathbb{R}^3$, podemos fazer o mesmo que descrevemos na seção 3.4.1: usamos uma coordenada adicional, que sempre valerá um. Assim, um vetor em $\mathbb{R}^3$ será representado por

$$\begin{pmatrix} x \\ y \\ z \\ 1 \end{pmatrix}$$

A operação que realiza um deslocamento por $(u, v, w)^T$ é

$$T[(x, y, z)] = (x + u, y + v, z + w)$$

Mas como representamos o vetor com a coordenada adicional, temos

$$T[(x, y, z, 1)] = (x + u, y + v, z + w, 1)$$

A matriz que realiza esta transformação é

$$\begin{pmatrix} 1 & 0 & 0 & u \\ 0 & 1 & 0 & v \\ 0 & 0 & 1 & w \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Rotação por eixo arbitrário

Suponha que tenhamos um eixo qualquer, descrito por dois pontos p, q (ou por um ponto p e um vetor $\mathbf{v}$). A operação de rotação ao redor deste eixo pode ser obtida da seguinte maneira:

1. aplique translação de forma que p fique na origem
2. aplique rotação pelo eixo transladado, usando o método descrito na seção 4.8.3
3. desfaça (1)

Outras transformações

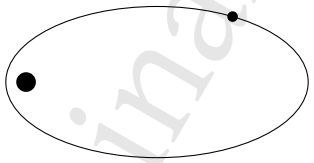
As outras transformações lineares escritas na seção 3.4.1 podem ser traduzidas para $\mathbb{R}^3$ da mesma maneira: por exemplo, se partindo de um vetor $(x, y, z)^T$, somarmos $2x$ em y, obteremos $(x, y + 2x, z)^T$, que é o cisalhamento realizado pela matriz a seguir.

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Outras transformações não lineares, como rotação ao redor de um eixo arbitrário (não passando pela origem), podem ser definidas como composição de translação com as transformações lineares que já definimos.

4.8.4 Órbitas celestes [mudança de base]

A primeira lei de Kepler para movimento planetário determina que as órbitas de planetas descrevem elipses, estando o Sol em um dos focos da elipse[5].

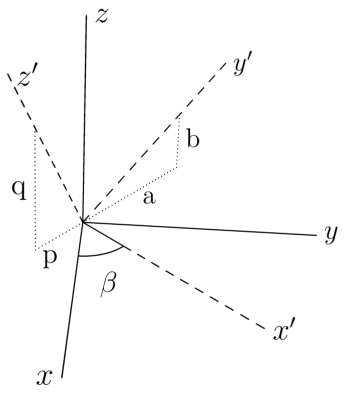


Suponha que queiramos descrever a órbita de Marte, de maneira simples quando observado a partir da Terra. As duas órbitas são elípticas. com o Sol em um dos focos de cada elipse, mas como não estão no mesmo plano, uma tentativa de descrevê-las usando o mesmo sistema de coordenadas será bastante complicada.

Escolhemos um sistema de coordenadas xyz de forma que a órbita da terra fique completamente contina no plano xy.

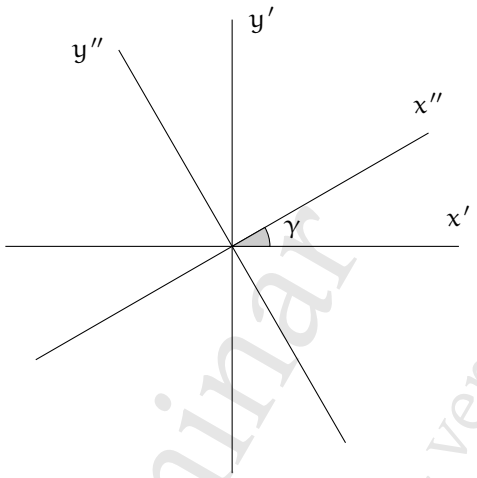
Seja x' a interseção entre os planos contendo as órbitas de Marte e da Terra. Determinamos outro sistema de coordenadas $x'y'z'$ de forma que o plano contendo a órbita de Marte fique contida no plano $x'y'$.

[5] As leis de Kepler são um caso especial da solução do problema gravitacional de n corpos onde os corpos são tratados como partículas com massa, e há uma única massa suficientemente grande para atrair outras (a do Sol).



A inclinação do plano $x'y'$ em relação ao plano xy (o ângulo entre as duas elipses) é dada pelo ângulo α, e o ângulo entre x e x' é β.

Agora, a elipse formada pela órbita de Marte não tem seus eixos alinhados com x' e y'. Determinamos portanto um novo sistema de coordenadas, $x''y''z''$, onde os eixos da elipse alinham-se com x'' e y''. Seja γ o ângulo entre x' e x''.



Sejam $\mathbf{p}$, $\mathbf{p}'$ e $\mathbf{p}''$ os vetores dando a posição de Marte nos sistemas de coordenadas xyz, $x'y'z'$ e $x''y''z''$. Cada sistema de coordenadas tem uma base formada por três vetores de magnitude um:

- B_1: tendo o plano xy alinhado com a elipse descrita pela Terra (sistema xyz);
- B_2: tendo o plano $x'y'$ alinhado com a elipse descrita por Marte (sistema $x'y'z'$);
- B_3: tendo o plano $x''y''$ alinhado com a elipse descrita por Marte, mas alinhando também os eixos da elipse com os vetores da base ($x''y''z''$).

Para mudar da base B_3 para B_2 precisamos de uma rotação ao redor de $z' = z''$. Seja γ o ângulo entre o eixo maior da elipse e x'. Então a transformação é

$$[\mathrm{id}]_{3\to 2} = \begin{pmatrix} \cos\gamma & -\operatorname{sen}\gamma & 0 \\ \operatorname{sen}\gamma & \cos\gamma & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

De B_1 para B_2: expressaremos os vetores da base B_1 na base B_2. Os vetores são

$$\begin{pmatrix} \cos\beta \\ \operatorname{sen}\beta \\ 0 \end{pmatrix},$$

Observando cuidadosamente a figura das duas bases na página 166, percebemos que os vetores unitários x', y', z' são descritos na base xyz como

$$[\mathbf{x}']_{B_1} = \begin{pmatrix} \cos\beta \\ \operatorname{sen}\beta \\ 0 \end{pmatrix}, \quad [\mathbf{y}']_{B_1} = \begin{pmatrix} r\cos(\beta+\pi/2) \\ r\operatorname{sen}(\beta+\pi/2) \\ \operatorname{sen}\alpha \end{pmatrix}, \quad [\mathbf{z}']_{B_1} = \begin{pmatrix} p\cos(\beta-\pi/2) \\ p\operatorname{sen}(\beta-\pi/2) \\ \cos\alpha \end{pmatrix}$$

Como os vetores são unitários, temos $p = b = \operatorname{sen}\alpha$ e $q = a = \cos\alpha$, logo podemos reescrever

$$[\mathbf{x}']_{B_1} = \begin{pmatrix} \cos\beta \\ \operatorname{sen}\beta \\ 0 \end{pmatrix}, \quad [\mathbf{y}']_{B_1} = \begin{pmatrix} \cos\alpha\cos(\beta+\pi/2) \\ \cos\alpha\operatorname{sen}(\beta+\pi/2) \\ \operatorname{sen}\alpha \end{pmatrix}, \quad [\mathbf{z}']_{B_1} = \begin{pmatrix} \operatorname{sen}\alpha\cos(\beta-\pi/2) \\ \operatorname{sen}\alpha\operatorname{sen}(\beta-\pi/2) \\ \cos\alpha \end{pmatrix}$$

Simplificando através de identidades trigonométricas, chegamos à matriz de mudança de base

$$[\mathrm{id}]_{B_2 \to B_1} = \begin{pmatrix} [\mathbf{x}']_{B_1} & [\mathbf{y}']_{B_1} & [\mathbf{z}']_{B_1} \end{pmatrix} = \begin{pmatrix} \cos\beta & -\cos\alpha \operatorname{sen}\beta & \operatorname{sen}\alpha \operatorname{sen}\beta \\ \operatorname{sen}\beta & \cos\alpha\cos\beta & -\operatorname{sen}\alpha\cos\beta \\ 0 & \operatorname{sen}\alpha & \cos\alpha \end{pmatrix}$$

Suponha que conheçamos $\alpha, \beta, \gamma, c, e$. Dado o ângulo θ descrito por Marte ao redor do Sol, podemos calcular o raio usando a fórmula que descreve elipses em coordenadas polares,

$$r(\omega) = c\frac{1-e^2}{1+e\cos\omega},$$

onde e é a excentricidade da elipse, e m é o comprimento de seu semieixo maior:

$$e = \sqrt{1 - \frac{n^2}{m^2}}.$$

A posição em coordenadas polares (r, θ) está relacionada com a posição em coordenadas cartesianas (x'', y'') através da identidade

$$\begin{aligned} x'' &= r\cos\theta \\ y'' &= r\operatorname{sen}\theta \end{aligned}$$

Assim, o ponto (r, θ) da trajetória, na base B_3, é

$$\begin{pmatrix} r\cos\theta \\ r\operatorname{sen}\theta \\ 0 \end{pmatrix}.$$

Podemos a partir daqui usar o operador de mudança de base $[\mathrm{id}]_{B_3 \to B_1}$ e seu inverso, $[\mathrm{id}]_{B_1 \to B_3}$ para efetuar cálculos com estas coordenadas.

O leitor poderá obter mais informações sobre órbitas no espaço e astrodinâmica nos livros de Roy [Roy04] e de Vallado [Val97]. O exemplo dado nesta seção é sugerido por Donald Teets [Tee98].

★ 4.8.5 Códigos corretores de erros [base; espaço-linha; multiplicação à direita]

Na seção 1.6.4 tratamos brevementet de códigos corretores de erros, e mencionamos que, dado um conjunto de mensagens com k bits, um código é um subespaço de $\mathbb{Z}_2^n$. Nesta seção abordamos o processo de codificação de mensagens, e o de detecção e correção de erros.

Quando trabalhamos com códigos corretores de erros, é comum denotar mensagens por vetores-linha, e não por colunas. Por exemplo, uma mensagem poderia ser

$$\mathbf{m} = (1, 0, 0, 1, 1).$$

Sabemos que uma base para o espaço $\mathbb{R}^n$, composto de vetores-coluna, pode ser descrita como uma matriz:

$$\begin{pmatrix} 1 & -3 \\ 0 & 0 \\ 0 & 2 \end{pmatrix}$$

é base para um subespaço de $\mathbb{R}^3$, porque tem duas colunas LI.

Da mesma forma, uma base para um espaço vetorial formado por linhas pode ser descrita por uma matriz com linhas LI. Seja $(\mathbb{R}^n)^*$ o espaço vetorial formado por todas as linhas com n números reais.

A matriz

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 5 \end{pmatrix}$$

é base para um subespaço de $(\mathbb{R}^3)^*$, com dimensão dois. As linhas neste espaço são combinações lineares das linhas da matriz, e portanto são da forma

$$a(2,0,0) + b(0,-1,5) = (2a, -b, 5b).$$

Como mencionamos no primeiro Capítulo, quando usamos códigos para corrigir erros, precisamos adicionar informação às mensagens. Assim, uma mensagem com três elementos, por exemplo, seria transformada em outra, com cinco:

$$(m_1, m_2, m_3) \xrightarrow{\text{codificação}} (c_1, c_2, c_3, c_4, c_5).$$

Além disso, usamos somente espaços vetoriais sobre corpos *finitos* para definir códigos corretores de erros (em nossos exemplos, usaremos apenas $\mathbb{Z}_2^n$, portanto *toda a aritmética usada será feita módulo dois*). Um subespaço V de $\mathbb{Z}_2^n$, portanto, determina um código. Uma base para este subespaço é chamada de *matriz geradora* do código.

Exemplo 4.115. A matriz

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

é base de um subespaço de $\mathbb{Z}_2^7$. Este subespaço tem dimensão 3 (porque a matriz tem três linhas LI). G é matriz geradora de um código. Podemos listar todas as palavras deste código enumerando todas as linhas que podem ser geradas pela matriz:

$$\begin{aligned}
(0,0,0)\cdot G &= (0,0,0,0,0,0,0) \\
(0,0,1)\cdot G &= (1,0,0,1,1,1,1) \\
(0,1,0)\cdot G &= (1,0,1,0,1,1,0) \\
(0,1,1)\cdot G &= (0,0,1,1,0,0,1) \\
(1,0,0)\cdot G &= (1,1,1,1,1,0,1) \\
(1,0,1)\cdot G &= (0,1,1,0,0,1,0) \\
(1,1,0)\cdot G &= (0,1,0,1,0,1,1) \\
(1,1,1)\cdot G &= (1,1,0,0,1,0,0)
\end{aligned}$$

◀

Teorema 4.116. *Se* G *é matriz geradora de um código então existe* G′*, também geradora do mesmo código, da forma*

$$(\mathcal{I} \mid A)$$

Exemplo 4.117. Obteremos uma nova matriz a partir da matriz G, do exemplo 4.115.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \xrightarrow{L_2 - L_1 ; L_3 - L_1} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \xrightarrow{L_3 - L_2} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \xrightarrow{L_1 - L_3}$$

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \xrightarrow{L_1 - L_2} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} = G'.$$

O espaço-linha de G' é igual ao de G, portanto ambas são geradoras do mesmo código. ◀

Se G é a matriz geradora de um código, as palavras $\mathbf{m}$ são codificadas como "$\mathbf{m}$G". Assim, as palavras do código de canal formam o espaço-linha de G.

Definição 4.118 (matriz de teste de paridade)**.** Seja $G = (\mathcal{I}\ A)$ a matriz geradora de um código. A matriz

$$H = (-A^T \mid \mathcal{I})$$

é uma *matriz de teste de paridade* do código. ♦

Exemplo 4.119. Para nosso código,

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad \text{e} \quad -A^T = A^T = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Note que como em $\mathbb{Z}_2$, 1 é $0 - 1$, porque $0 - 1 = 0 \oplus 1 = 1$, então $A = -A$.

Assim,

$$H = (-A^T \mid \mathcal{I}) = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

é *matriz de teste de paridade* para nosso código. ◀

Definição 4.120 (síndrome)**.** Se H é matriz de teste de paridade de um código e $\mathbf{c}$ uma palavra codificada, então $H\mathbf{c}^T$ é a *síndrome* de $\mathbf{c}$. ♦

Teorema 4.121. *Uma linha* $\mathbf{c}$ *pertence ao código* C *se sua síndrome é* $\mathbf{0}$*.*

A síndrome nos permite, portanto, verificar se uma palavra pertence ao código.

Exemplo 4.122. A mensaegm $\mathbf{c} = (0, 0, 1, 1, 0, 0, 1)$ *pertence* ao código, e sua síndrome é

$$H\mathbf{c}^T = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

A mensagem $\mathbf{d} = (0, 0, 1, 1, 0, 0, 0)$ n*ão pertence* ao código, e tem síndrome

$$H\mathbf{d}^T = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

◀

Teorema 4.123. *Se uma palavra codificada* $\mathbf{c}$ *tem no máximo* k *erros, onde* k *é o máximo de erros que o código suporta, então* $\mathbf{c}$ *tem a mesma síndrome que seu erro.*

Basta, portanto, manter uma tabela de erros e suas síndromes. Quando recebemos uma mensagem com erro, verificamos na tabela qual foi o erro introduzido. Podemos portanto simplesmente subtrair o erro da mensagem.

Exemplo 4.124. Nosso código corrige no máximo um erro. Calculamos a síndrome de cada um dos vetores de erro a seguir (os vetores são mostrados sem parênteses para simplificar a notação).

erro	síndrome
0000001	0001
0000010	0010
0000100	0100
0001000	1000
0010000	1001
0100000	1011
1000000	1111

Agora simulamos o envio de uma mensagem em que um erro é adicionado durante a transmissão. A mensagem original é $\mathbf{m} = (0,1,1)$. Codificada, ela se torna

$$\mathbf{c} = \mathbf{m}G = (0,1,1)G = (0,0,1,1,0,0,1).$$

Se durante a transmissão o terceiro bits da mensagem foi trocado, teremos adicionado um vetor de erro $(0,0,1,0,0,0,0)$:

$$\mathbf{c}' = (0,0,1,1,0,0,1) \oplus (0,0,1,0,0,0,0) = (0,0,0,1,0,0,1) \notin \mathcal{C}$$

O receptor verifica a síndrome da mensagem:

$$H(\mathbf{c}')^T = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

O erro que tem síndrome igual a $(1,0,0,1)^T$ é $\mathbf{e} = (0,0,1,0,0,0)$ O receptor calcula portanto $\mathbf{c} = \mathbf{c}' - \mathbf{m}$, obtendo a mensagem codificada original, $(0,0,1,1,0,0,1)$. ◀

Exercícios

Ex. 85 — Sejam A e B tais que AB seja definido. Se A tem uma linha inteira com zeros, o que pode ser dito a respeito do produto AB? Qual é o análogo disso para a matriz B?

Ex. 86 — Mostre que a inversa de uma matriz diagonal, se existir, é também diagonal.

Ex. 87 — Mostre que se A e B são matrizes diagonais, então $AB = BA$.

Ex. 88 — Demonstre a proposição 4.35.

Ex. 89 — Demonstre a proposição 4.23.

Ex. 90 — Para cada conjunto de matrizes quadradas abaixo, determine se elas sempre tem inversa, nunca tem inversa, ou se podem ou não ter inversa.

a) Todas as matrizes diagonais.

b) Todas as matrizes triangulares.

c) Todas as matrizes obtidas de matrizes diagonais usando apenas permutações de linhas.

d) Todas as matrizes onde mais da metade dos elementos é composta de zeros.

e) Todas as matrizes onde mais da metade dos elementos é composta de diferentes números primos.

f) Todas as matrizes $n \times n$, com n par, onde a diagonal principal e a diagonal secundária não tem elementos em comum.

g) Todas as matrizes onde pelo menos $n^2 - n + 1$ elementos são números primos.

h) Todas as matrizes cuja diagonal só contém uns.

i) Todas as matrizes $n \times n$ cujos elementos são os inteiros $1, 2, \ldots, n^2$, em qualquer ordem.

j) Todas as matrizes contendo uma linha inteira de zeros.

k) Todas as matrizes contendo uma linha inteira de uns.

l) Todas as matrizes cuja diagonal é composta de zeros.

m) Todas as matrizes $n \times n$, com n par, onde a diagonal principal e a diagonal secundária tem somente números primos.

Ex. 91 — Demonstre a proposição 4.31.

Ex. 92 — Uma matriz A é quase-diagonal se pode ser particionada em blocos de forma que apenas os blocos A_{ii} contém elementos não-nulos.

$$A = \begin{pmatrix} A_{11} & & & \\ & A_{22} & & \\ & & \ddots & \\ & & & A_{nn} \end{pmatrix}$$

Mostre que a inversa de uma matriz quase-diagonal é também uma matriz quase-diagonal, particionada da mesma forma, onde cada bloco A_{ii}^{-1} é a inversa do bloco A_{ii} original.

$$A^{-1} = \begin{pmatrix} (A_{11})^{-1} & & & \\ & (A_{22})^{-1} & & \\ & & \ddots & \\ & & & (A_{nn})^{-1} \end{pmatrix}$$

Ex. 93 — Prove o Lema 4.27.

Ex. 94 — Prove que o posto de linhas de uma matriz é igual ao posto de colunas, usando a forma escalonada reduzida por linhas *e colunas*.

Ex. 95 — Prove que o posto de linhas de uma matriz é igual ao posto de colunas, usando o teorema do núcleo e da imagem, e interpretando a matriz como a matriz de coeficientes de um sistema linear.

Ex. 96 — Para cada matriz, calcule a decomposição LU, se existir, ou a decomposição LUP caso a decomposição LU não exista. Caso seja necessário determine os valores de x para que a decomposição LU (não LUP) exista.

$$A = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & x \\ -4 & -x^2 \end{pmatrix}$$
$$C = \begin{pmatrix} x & 0 & 0 \\ 0 & 0 & x \\ 1 & 1 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} x & x & x^2 \\ -2 & +2 & x \\ +3 & -3 & x \end{pmatrix}.$$

Ex. 97 — Mostre como usar a fatoração LU para clacular $A^{-1}B$, sem precisar computar A^{-1}. Diga qual fatoração LU deve existir para que o método funcione.

Ex. 98 — Prove o Teorema 4.100.

Ex. 99 — Prove que para quaisquer matrizes A e B tais que AB seja definido,

$$\text{nul}(A) \leq \text{nul}(AB),$$

e que

$$\text{posto}(A) \geq \text{posto}(AB).$$

Ex. 100 — Mostre que para todo k, $(A_1 A_2 \dots A_k)^{-1} = A_k^{-}1 A_{k-1}^{-1} \dots A_1^{-1}$ se todas as matrizes A_i forem $n \times n$ e invertíveis.

Ex. 101 — Resolva o sistema de equações usando eliminação de Gauss.

$$\begin{cases} 3x_1 - 4x_2 + x_3 = 3 \\ -x_1 - x_2 - x_3 = 0 \\ x_1 + 8x_2 + 5x_3 = -1 \end{cases}$$

Ex. 102 — Prove que o processo de eliminação de Gauss e o algoritmo de decomposição LU podem ser aplicados a matrizes de blocos, e dê um exemplo de cada.

Ex. 103 — Sejam

$$A = \begin{pmatrix} 2 & 7 & -9 \\ -4 & -2 & -3 \\ 3 & -1 & 5 \end{pmatrix}, \quad \mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

Resolva os sistemas:

a) $A\mathbf{x} = (10, 1, -1)^T$

b) $A\mathbf{x} = (0, 2, 4)^T$

c) $A\mathbf{x} = (-1, -2, -3)^T$
d) $A\mathbf{x} = (20, -1, 0)^T$
e) $A\mathbf{x} = (x_1, x_1, -x_1)^T$
f) $A\mathbf{x} = (x_2, x_3, -x_1)^T$
g) $A\mathbf{x} = \mathcal{I}$

Ex. 104 — Ao enunciarmos o Teorema 4.95, e ao elaborarmos o Exemplo 4.97, dissemos que devemos deixar a matriz U na forma escalonada por linhas. O que acontece se a deixarmos na forma escalonada *reduzida* por linhas? Porque?

Ex. 105 — O Teorema 4.95 determina condições para a existência de fatoração LU de uma matriz, e o Teorema 4.98 faz o mesmo para decomposição LUP. Determine as condições para que A tenha decomposições UL, PUL e ULP, e mostre como obtê-las.

Ex. 106 — Mostre que toda matriz pode ser descrita como soma de uma matriz simétrica e uma anti-simétrica.

Ex. 107 — Seja A uma matriz real[6] anti-simétrica de ordem n. Mostre que $A = S_1S_2 - S_2S_2$, onde S_1 e S_2 são matrizes simétricas.

Ex. 108 — Suponha que seja necessário resolver os sistemas $A_1\mathbf{x} = \mathbf{b}$, $A_2\mathbf{x} = \mathbf{b}$, ..., $A_k\mathbf{x} = \mathbf{b}$, onde as matrizes A_i diferem apenas em uma única linha. Dê um método eficiente para resolver o problema. E se as matrizes diferissem em uma única coluna?

Ex. 109 — Demonstre o teorema 4.92.

Ex. 110 — Qual é a matriz elementar que inverte a ordem das linhas de uma matriz, de forma que a primeira linha passe a ser a última, a segunda passe a ser a penúltima, e assim por diante?

Ex. 111 — No exemplo 4.89, realizamos diversas operações elementares na matriz dos coeficientes do sistema. A matriz elementar que representa a primeira delas foi mostrada no final do exemplo. Mostre as outras.

Ex. 112 — Neste Capítulo desenvolvemos um método para fatoração PLU. Prove que toda matriz que tem fatoração PLU tem fatoração LUP. Mostre um método para obter tal fatoração, e diga como relacionam-se PLU e $L'U'P'$, quando $A = PLU = L'U'P'$.

Ex. 113 — Mostramos no exemplo 1.39 que as variáveis aleatórias reais em um espaço amostral formam um espaço vetorial. No exemplo 3.10, mostramos que a esperança é uma transformação linear. Como é a matriz da transformação linear que dá a esperança de uma variável aleatória discreta em um espaço amostral finito?

Ex. 114 — A seguir temos bases para $\mathbb{R}^3$ (o exemplo 4.42 mostra que uma matriz quadrada não-singular pode ser vista como base de $\mathbb{R}^n$).

$$A = \begin{pmatrix} 2 & 2 & 2 \\ 0 & 2 & 2 \\ 0 & 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 3 \\ -3 & -2 & -1 \\ 2 & 3 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} 4 & 5 & 7 \\ 1 & -2 & 0 \\ 1 & 0 & 3 \end{pmatrix}$$

[6] Ou complexa, ou com coeficientes em qualquer corpo infinito.

i) Mostre todas as matrizes de mudança de base entre elas.

ii) Seja $\mathbf{v} = (1, 2, 3)^T$ um vetor escrito na base canônica. Mostre $\mathbf{v}$ em todas as bases dadas.

iii) Escreva $[(1, -1, 0)^T]_A$ na base B

iv) Escreva $[(2, 1, 1)^T]_C$ na base D.

Ex. 115 — Demonstre o Teorema 4.113.

Ex. 116 — Prove que a rotação em duas dimensões é comutativa, mas que em tres dimensões, não é.

★ **Ex. 117 —** Prove que matrizes de rotação formam um grupo (os *elementos* do grupo são as reflexões; a operação do grupo é composição). Se adicionarmos reflexões, continuamos a ter um grupo?

Ex. 118 — Mostre a matriz que realiza a mudança de base, em $\mathbb{R}^2$, da base canônica $(\mathbf{e}_1, \mathbf{e}_2)$ para a base formada por $(\mathbf{f}_1, \mathbf{f}_2)$, tal que:

i) $\mathbf{f}_1 = (2, 4)^T$;

ii) $\mathbf{f}_2$ é obtido a partir de $\mathbf{f}_1$ com uma rotação por $3\pi/4$ radianos.

Ex. 119 — Demonstre a Proposição 4.53.

★ **Ex. 120 —** A base canônica para $\mathbb{Z}_2^3$ é $\{001, 010, 100\}$. Sejam $B = \{001, 011, 110\}$ e $C = \{111, 110, 100\}$ duas outras bases para este espaço.

a) Mostre a matriz de mudança de base de B para C.

b) Escreva $[111]_B$ na base C.

★ **Ex. 121 —** Prove o Teorema 4.109.

★ **Ex. 122 —** Sejam

$$A = \begin{pmatrix} i & 0 & 2+2i \\ -2i & 4 & 0 \\ 1 & 1-i & -1+3i \end{pmatrix}, \quad \mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

Resolva os sistemas

a) $A\mathbf{x} = (1, i, -i)^T$

b) $A\mathbf{x} = (0, 1, 0)^T$

c) $A\mathbf{x} = (1 + i, -1 + i, 0)^T$

Capítulo 5

Determinantes

De toda matriz de números reais pode-se extrair um número real que nos permite determinar diversas propriedades da matriz. Este número é chamado de *determinante* da matriz. Similarmente, toda matriz cujas entradas pertencem a um corpo K está relacionada tem um determinante, que é um elemento de K. Neste texto, trataremos especialmente do corpo dos reais

Determinantes estão relacionados a propriedades de sistemas lineares (e de fato, surgiram do estudo desses sistemas), mas também estão relacionados a diversos outros conceitos, inclusive o de volume em geometria. Neste Capítulo, definiremos uma função que dá o volume de um paralelepípedo em n dimensões. A partir de três propriedades desta função, mostraremos que ela existe e que é única – e esta será exatamente a função determinante de uma matriz que representa o paralelepípedo.

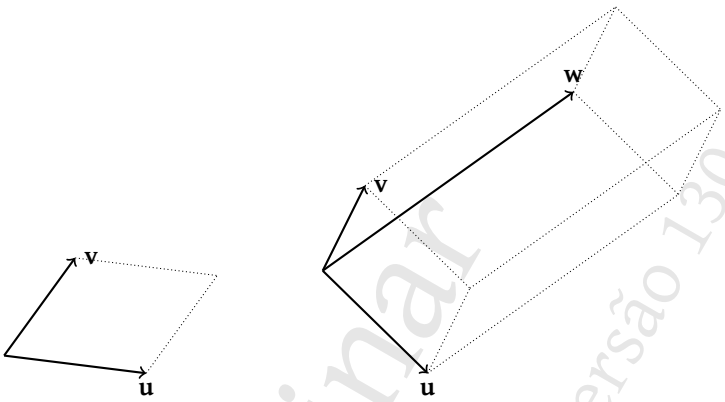
5.1 Volume orientado

Definição 5.1 (Paralelepípedo)**.** Seja $P = \{\mathbf{v}^1, \mathbf{v}^2, \ldots, \mathbf{v}^k\}$ um conjunto de n vetores linearmente independentes em um espaço de n dimensões. O conjunto de pontos

$$\{a_1\mathbf{v}^1 + a_2\mathbf{v}^2 + \ldots + a_n\mathbf{v}^k : \quad a_i \in [0,1]\}$$

é o *paralelepípedo* gerado pelos vetores. ⧫

A próxima figura mostra um paralelepípedo gerado por dois vetores em $\mathbb{R}^2$ e outro, gerado por três vetores em $\mathbb{R}^3$.



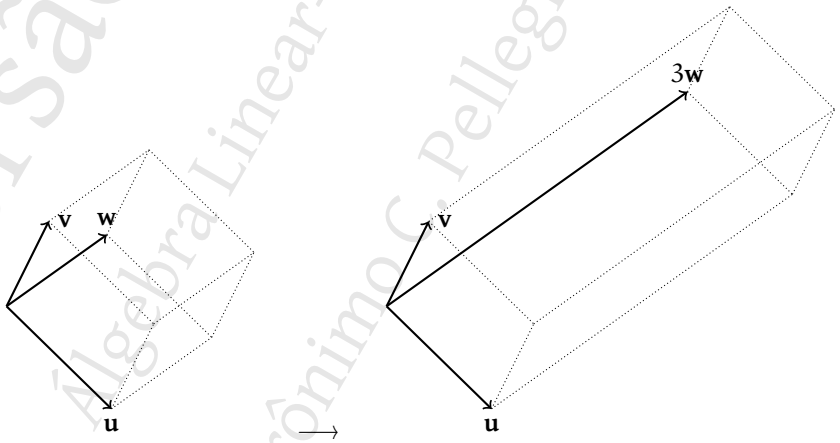
Em $\mathbb{R}^3$ e $\mathbb{R}^2$ temos as noções intuitivas de volume e área. Em $\mathbb{R}$, usamos um único vetor, e o volume do paralelepípedo é igual à distância da origem até o ponto que o vetor descreve – ou seja, é igual à norma do vetor.

Definimos o volume de um paralelepípedo em um espaço de n dimensões da seguinte forma.

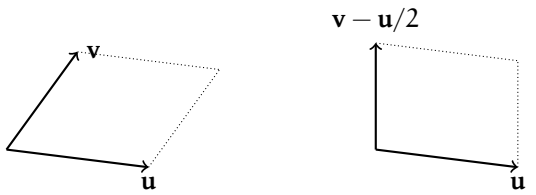
i) Se um paralelepípedo cabe em $n-1$ dimensões, seu volume é zero. Um paralelepípedo cabe em $n-1$ dimensões quando é descrito por $n-1$ vetores, *e portanto sua descrição em* n *dimensões deve necessariamente incluir somente* $n-1$ *vetores LI - sua descrição por* n *vetores é um conjunto LD.*

ii) O volume do hipercubo de lado unitário é um.

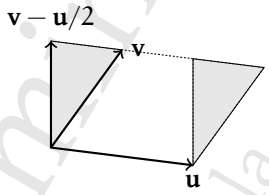
iii) Se multiplicarmos um dos vetores que descreve o paralelepípedo por uma constante, o efeito será de "esticá-lo" ou "encolhê-lo", e o volume será multiplicado pelo mesmo valor. Isso pode ser visualizado trivialmente no cubo unitário em $\mathbb{R}^3$, que é descrito por três vetores e tem volume um: se multiplicarmos um dos vetores por k, obteremos um paralelepípedo cuja forma é semelhante à de k cubos postos lado a lado.



Além de multiplicar um dos vetores por escalar, podemos somar o múltiplo de um dos vetores a outro, sem que o volume seja modificado. Na figura a seguir, somamos $-1/2\mathbf{u}$ ao vetor $\mathbf{v}$, gerando um paralelepípedo diferente.

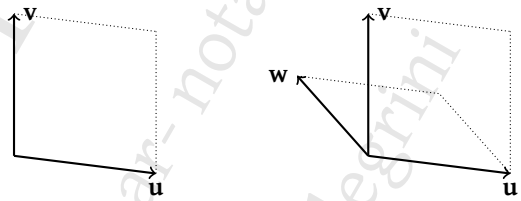


Ao sobrepormos as duas imagens, vemos que o paralelepípedo modificado tem o mesmo volume do primeiro (a área sombreada da esquerda só está em um deles; a da direita só está no outro – e as duas tem o mesmo volume).

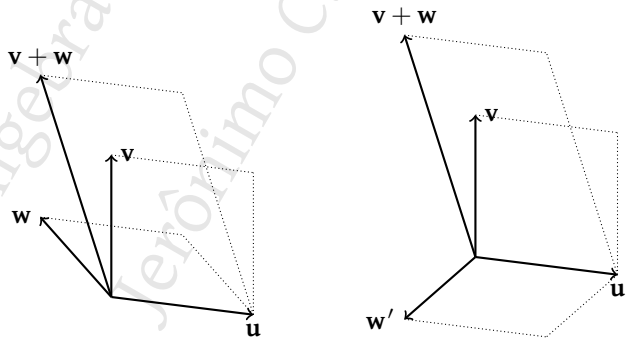


Uma consequência imediata disto é que dois paralelepípedos $P_1 = (\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{w})$ e $P_2 = (\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{u})$ que diferem somente em um vetor estão relacionados da seguinte maneira: o volume de $P_3 = (\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{w} + \mathbf{u})$ é a soma dos volumes de P_1 e P_2, como ilustra a seguinte sequencia de figuras.

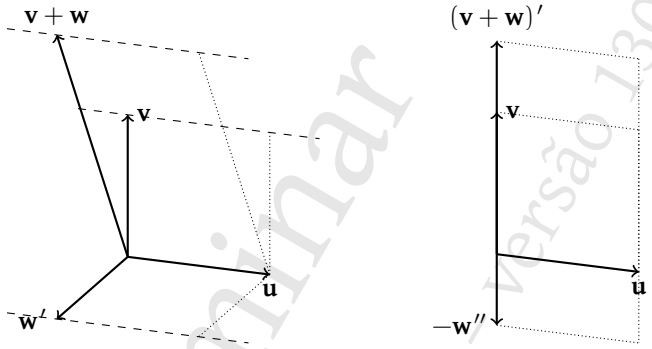
Começamos com o paralelepípedo $P(\mathbf{u}, \mathbf{v})$, e desenhamos em seguida o paralelepípedo $P(\mathbf{u}, \mathbf{w})$.



Agora desenhamos o paralelepípedo $P(\mathbf{u}, \mathbf{v} + \mathbf{w})$. Em seguida, fazemos a reflexão do paralelepípedo $P(\mathbf{u}, \mathbf{w})$ em $\mathbf{u}$, resultando em $P(\mathbf{u}, \mathbf{w}')$ somente para facilitar a visualização.



Agora, sabemos que as tres retas indicadas na figura da esquerda, a seguir, são paralelas a **u**. Somamos múltiplos de **u** aos paralelepípedos, deslocando-os por estas retas, até que fiquem alinhados como na figura da direita (mostramos anteriormente que podemos fazer isto sem mudar o volume dos paralelepípedos).



Agora fica claro que

$$\text{vol}\left[P(\mathbf{u}, \mathbf{v}+\mathbf{w})\right] = \text{vol}\left[P(\mathbf{u}, \mathbf{v})\right] + \text{vol}\left[P(\mathbf{u}, \mathbf{w})\right]$$

Assim, se fixarmos $n-1$ vetores e descrevermos o volume como função de um deles,

$$V(\mathbf{w}) = \text{vol}(\mathbf{v_1}, \mathbf{v}_2, \ldots, \mathbf{w}, \ldots, \mathbf{v}_n),$$

o volume deve ser linear em cada uma das colunas que descrevem o paralelepípedo. Ou seja, para quaisquer vetores **u**, **w** e qualquer escalar k,

$$V(k\mathbf{w}) = kV(\mathbf{w})$$
$$V(\mathbf{w}+\mathbf{u}) = V(\mathbf{w}) + V(\mathbf{u}).$$

Isso significa que o volume é uma *função multilinear* de seus argumentos (que são vetores coluna).

O item (i) significa que se o conjunto tiver n vetores LD o volume é zero. O item (ii) determina que o volume do paralelepípedo definido pelos vetores $\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_n}$ é um.

Se quisermos representar paralelepípedos como matrizes, podemos simplesmente alocar cada coluna (ou cada linha) da matriz para um dos vetores. Assim, o paralelepípedo descrito pelos vetores $(1,0,0)^T$, $(0,2,0)^T$ e $(0,1,5)^T$ pode ser representado pela matriz

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 5 \end{pmatrix}$$

Como já observamos, para os paralelepípedos com volume diferente de zero, as colunas da matriz serão sempre linearmente independentes (de outra forma o sólido caberia em $n-1$ dimensões).

5.1.1 Orientação

Quando o volume de um paralelepípedo é diferente de zero, a função determinante nos dará não apenas o volume, mas também sua *orientação*.

Um paralelepípedo em $\mathbb{R}^n$ só tem volume se é descrito por n vetores L.I., porque se os n vetores forem L.D. haverá pelo menos dois deles representando o mesmo hiperplano, e o paralelepípedo então teria volume zero – *e portanto um paralelepípedo tem volume não-nulo se e somente se é uma base para* $\mathbb{R}^n$.

Por exemplo, em $\mathbb{R}^2$ um par de vetores só tem volume se os vetores não são colineares (ou seja, se são L.I.). Em $\mathbb{R}^3$ o mesmo vale: três vetores só descrevem um paralelepípedo com volume se forem todos L.I. quando tomados dois a dois. Ao tratarmos desses objetos geométricos, nos referiremos então a "bases ordenadas", já que cada paralelepípedo equivale a uma base.

Damos aqui definições informais de orientação de bases em $\mathbb{R}^2$ e $\mathbb{R}^3$.

Denotamos a orientação de uma base B por $O(B)$, ou $O(\mathbf{b}_1, \mathbf{b}_2, \ldots)$.

Em $\mathbb{R}^1$, cada vetor (x) pode ser representado geometricamente na reta real como um segmento de reta com uma de suas extremidades no zero. Este segmento tem cumprimento x, e diremos que a orientação de dois vetores é a mesma (ou que suas orientações são *concordantes* se a magnitude de ambos tem o mesmo sinal (são ambos positivos ou ambos negativos). Desta forma dividimos os vetores em dois conjuntos: aqueles à esquerda do zero e aqueles à direita do zero.

Neste texto, decidimos *arbitrariamente* que a orientação dos vetores à direita do zero é $+1$, e que a orientação dos vetores à esquerda do zero é -1.

Exemplo 5.2. Os vetores mostrados nas duas figuras são (-2) e (2.5); o primeiro tem orientação negativa, e o segundo tem orientação positiva.

◀

Informalmente, dizemos que duas bases ordenadas de $\mathbb{R}^2$ tem a mesma orientação se os vetores de ambas são listados no mesmo sentido – horário ou anti-horário, e negativa caso contrário.

Novamente decidimos, *arbitrariamente*, que uma base com vetores listados no sentido anti-horário tem orientação positiva, e uma base com vetores listados no sentido horário tem orientação negativa.

Podemos definir orientação em $\mathbb{R}^3$ da seguinte maneira: sejam $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ e $(\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3)$ bases de $\mathbb{R}^3$. Estas bases podem ser representadas no espaço por três vetores cada uma.

Podemos imaginar movimentos rígidos entre estes vetores (isto é, movimentos que não mudam as distancias e ângulos entre eles). Através de movimentos rígidos, posicionamos as duas bases de forma a alinhar $\mathbf{v}_3$ e $\mathbf{w}_3$ com o terceiro vetor da base canônica, $\mathbf{e}_3$. Obtemos assim duas novas bases, $(\mathbf{v}'_1, \mathbf{v}'_2, \mathbf{v}'_3)$ e $(\mathbf{w}'_1, \mathbf{w}'_2, \mathbf{w}'_3)$. As bases originais de $\mathbb{R}^3$ tem a mesma orientação se e somente se ao percorrermos pontos em $\mathbf{v}'_1, \mathbf{v}'_2, \mathbf{v}'_3$, "giramos no mesmo sentido[1]" que se percorrermos três pontos em $\mathbf{w}'_1, \mathbf{w}'_2, \mathbf{w}'_3$. Esta noção é equivalente à "regra da mão direita".

5.2 Determinantes

A função determinante será positiva se a orientação do paralelepípedo for a mesma da base canônica, e negativo se a orientação for oposta. Para obter apenas o valor do volume, basta desconsiderar o sinal.

Queremos então uma função que nos dê o volume destes sólidos. Esta função terá como argumento uma sequência de vetores coluna – ou equivalentemente, uma matriz quadrada. A função determinante deve obedecer as propriedades que definimos anteriormente para volume com sinal. Uma função que obedeça

[1] Esta não é uma definição formal!

aquelas propriedades é chamada de *função determinante*; a definição dada a seguir traduz as propriedades para a representação por matrizes.

Definição 5.3 (Função determinante)**.** Uma função[2] $\det : M_{n\times n} \to \mathbb{R}$ é uma *função determinante* se e somente se tem as seguintes propriedades.

i) $\det(A) = 0$ se A tem colunas LD.

ii) $\det(\mathcal{I}) = +1$.

iii) $\det(A)$ é forma multilinear das colunas de A.

O item (iii) significa que uma função determinante é uma transformação linear quando fixamos todas as colunas e variamos apenas uma delas: para todo escalar λ, todo vetor coluna $\mathbf{v}$, e toda coluna $\mathbf{c}_j$,

$$\begin{aligned}\det(\mathbf{c}_1,\ldots,\lambda\mathbf{c}_j,\ldots,\mathbf{c}_n) &= \lambda\det(\mathbf{c}_1,\ldots,\mathbf{c}_j,\ldots,\mathbf{c}_n)\\ \det(\mathbf{c}_1,\ldots,\mathbf{c}_j+\mathbf{v},\ldots,\mathbf{c}_n) &= \det(\mathbf{c}_1,\ldots,\mathbf{c}_j,\ldots,\mathbf{c}_n)+\det(\mathbf{c}_1,\ldots,\mathbf{v},\ldots,\mathbf{c}_n).\end{aligned}$$ ♦

Note que a definição acima pode ser facilmente generalizada para corpos em geral, e não apenas $\mathbb{R}$.

Exemplo 5.4. Definimos uma função $D : \mathcal{M}_{2\times 2} \to \mathbb{R}$, tal que

$$D\left[\begin{pmatrix} a & b\\ c & d\end{pmatrix}\right] = ab - cd.$$

Mostramos agora que esta função satisfaz as propriedades que propusemos, e portanto ela *é uma função determinante*.

i) Se as colunas de A são LD, $D(A)$ deve ser zero:

$$D\begin{pmatrix} a & ka\\ b & kb\end{pmatrix} = kab - kab = 0.$$

ii) O determinante de $\mathcal{I}$ é 1:

$$D\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix} = 1 - 0 = 1.$$

iii) Se fixarmos uma coluna, o determinante é linear na outra. Verificamos a multiplicação por escalar:

$$D\begin{pmatrix} a & \lambda b\\ c & \lambda d\end{pmatrix} = \lambda ad - \lambda bc = \lambda(ad-bc) = \lambda D\begin{pmatrix} a & b\\ c & d\end{pmatrix}$$

Verificamos a soma:

$$\begin{aligned} D\begin{pmatrix} a & b+\beta\\ c & d+\delta\end{pmatrix} &= a(d+\delta) - c(b+\beta)\\ &= (ad-bc) + (a\delta - \beta c)\\ &= D\begin{pmatrix} a & b\\ c & d\end{pmatrix} + D\begin{pmatrix} a & \beta\\ c & \delta\end{pmatrix}\end{aligned}$$

[2] É também comum denotar o determinante de uma matriz A por $|A|$. Evitamos esta notação porque já usamos $|\cdot|$ para módulo.

Ilustramos o uso desta função a seguir.

$$D\begin{pmatrix}1 & 2\\ 3 & 5\end{pmatrix} = (1)(5) - (3)(2) = 5 - 6 = -1. \qquad \blacktriangleleft$$

Verificaremos agora que qualquer função com estas propriedades será necessariamente *alternante* (o valor da função mudará de sinal se trocarmos dois de seus argumentos de posição). Isso significa que o determinante de uma matriz A dará a orientação da base composta por suas colunas[3].

Teorema 5.5. *Uma função determinante é* alternante *– ou seja, quando dois de seus argumentos (que são colunas de uma matriz) tem suas posições trocadas, o valor da função é multiplicado por* -1.

Demonstração. Seja uma matriz quadrada com colunas $\mathbf{a_i}$ e $\mathbf{a_j}$, tal com determinante x. Suponha que quando trocamos as duas colunas de lugar, o determinante passa a ser um outro valor y:

$$\begin{aligned} &\det(\ldots, \mathbf{a_i}, \ldots, \mathbf{a_j}, \ldots) = x \\ &\det(\ldots, \mathbf{a_j}, \ldots, \mathbf{a_i}, \ldots) = y. && (\mathbf{a_i} \leftrightarrow \mathbf{a_j}) \end{aligned}$$

Agora, se somarmos cada uma dessas duas colunas à outra, temos uma nova matriz, e seu determinante será

$$\det(\ldots, \mathbf{a_i} + \mathbf{a_j}, \ldots, \mathbf{a_j} + \mathbf{a_i}, \ldots) = 0,$$

porque as colunas são LD (há duas colunas iguais).

Mas como o determinante é multilinear,

$$\begin{aligned} &\det(\ldots, \mathbf{a_i} + \mathbf{a_j}, \mathbf{a_j} + \mathbf{a_i}, \ldots) \\ &= \det(\ldots, \mathbf{a_i}, \mathbf{a_i} + \mathbf{a_j}, \ldots) \\ &+ \det(\ldots, \mathbf{a_j}, \mathbf{a_i} + \mathbf{a_j}, \ldots) \\ &= \Big[\det(\ldots, \mathbf{a_i}, \mathbf{a_i}, \ldots) && (\star) \\ &+ \det(\ldots, \mathbf{a_i}, \mathbf{a_j}, \ldots)\Big] && (\text{abrindo o primeiro } a_i + a_j) \\ &+ \Big[\det(\ldots, \mathbf{a_j}, \mathbf{a_j}, \ldots) && (\star) \\ &+ \det(\ldots, \mathbf{a_j}, \mathbf{a_i}, \ldots)\Big] && (\text{abrindo o segundo } a_i + a_j) \\ &= \det(\ldots, \mathbf{a_i}, \mathbf{a_j}, \ldots) && (\text{porque os casos } (\star) \text{ com colunas iguais são zero}) \\ &+ \det(\ldots, \mathbf{a_j}, \mathbf{a_i}, \ldots) \\ &= x + y, \end{aligned}$$

e como $x + y = 0$,

$$x = -y. \qquad \blacksquare$$

Exemplo 5.6. Verificamos agora o efeito de uma mudança de linhas em uma matriz de ordem 2. Seja

$$A = \begin{pmatrix}1 & 3\\ 2 & -1\end{pmatrix}, \quad B = \begin{pmatrix}2 & -1\\ 1 & 3\end{pmatrix}.$$

[3] A relação entre orientação e a troca da ordem dos vetores da base está detalhada no teorema $\gamma.2$, no Apêndice γ, página 498. A demosntração do teorema é pedida no exercício 372, e uma idéia superficial de como poderia ser a demonstração se encontra no Apêndice ζ.

Então

$$\det A = -1 - 6 = -7$$
$$\det B = 6 + 1 = 7.$$

◀

A seguir listamos o efeito de operações elementares sobre o determinante de matrizes.

Teorema 5.7. *Seja A uma matriz quadrada. Então*

i) $\det(E_{i,j}A) = -\det A$, *se* $i \neq j$ *(se trocarmos duas linhas de uma matriz, o determinante é multiplicado por* -1*);*

ii) $\det(E_{cLi}A) = c \det A$ *(se multiplicarmos uma linha de A por c o determinante também é multiplicado por c);*

iii) $\det(E_{i+cLj}A) = \det A$ *(adicionar múltiplo de uma linha a outra não modifica o determinante).*

Do Teorema 5.7 obtemos o Lema a seguir, cuja demonstração é pedida no exercício 132

Lema 5.8. *Seja E uma matriz elementar e A uma matriz quadrada, ambas de mesma ordem. Então* $\det(EA) = \det(E)\det(A)$.

Com estes fatos já é possível obter o determinante de matrizes, se soubermos como escrevê-las como produto de matrizes elementares.

Exemplo 5.9. Sabemos que o determinante da matriz identidade é um. Consequentemente,

$$\det E_{i,j} = -1$$
$$\det E_{cLi} = c$$
$$\det E_{i+cLj} = 1$$

Consequentemente, podemos deduzir que se

$$\begin{aligned} A &= E_{1,2}E_{2L1}E_{1+5L2}\mathcal{I} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 2 & 10 \end{pmatrix}, \end{aligned}$$

então

$$\begin{aligned} \det A &= \det(E_{1,2}E_{2L1}E_{1+5L2)}\mathcal{I}) \\ &= \det E_{1,2} \det\left(E_{2L1}E_{1+5L2}\mathcal{I}\right) \\ &= (-1)\det E_{2L1} \det\left(E_{1+5L2}\mathcal{I}\right) \\ &= (-1)(2)\det E_{1+5L2} \det(\mathcal{I}) \\ &= (-1)(2)(1)(1) = -2. \end{aligned}$$

◀

Outras propriedades de uma função determinante são discutidas a seguir.

Teorema 5.10. *Sejam* A *e* B *matrizes quadradas de mesma ordem. Então* $\det(AB) = \det(A)\det(B)$.

Demonstração. Se A é singular, $\det(A) = \det(AB) = 0$, porque AB também não é singular.

Se A não é singular, então é produto de matrizes elementares:

$$A = E_1 E_2 \dots E_k.$$

Então,

$$\begin{aligned} \det(AB) &= \det(E_1 E_2 \dots E_k B) \\ &= \det(E_1)\det(E_2)\cdots\det(E_k)\det(B) && \text{(pelo Lema 5.8)} \\ &= \det(A)\det(B), \end{aligned}$$

completando a demonstração. ■

Exemplo 5.11. Sejam

$$A = \begin{pmatrix} 2 & 3 \\ 4 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 2 \\ 3 & 2 \end{pmatrix},$$

e consequentemente

$$AB = \begin{pmatrix} 7 & 10 \\ -7 & 6 \end{pmatrix},$$

e

$$\begin{aligned} \det AB &= (ab)_{11}(ab)_{22} - (ab)_{12}(ab)_{21} \\ &= (7)(6) - (10)(-7) \\ &= 112 \end{aligned}$$

Temos

$$\begin{aligned} \det A &= (a)_{11}(a)_{22} - (a)_{12}(a)_{21} \\ &= (2)(-1) - (3)(4) \\ &= -14 \\ \det B &= (b)_{11}(b)_{22} - (b)_{12}(b)_{21} \\ &= (-1)(2) - (2)(3) \qquad = -8 \end{aligned}$$

Claramente, $\det A \det B = \det(AB)$, ou seja, $(-14)(-8) = 112$. ◄

O exercício 133 pede a demonstração do Teorema a seguir.

Teorema 5.12. *Sejam* A *uma matriz quadrada de ordem* n *e* c *um escalar.*

i) $\det(A) = \det(A^T)$.

ii) $\det(cA) = c^n \det(A)$.

iii) $\det(A) = 0$ *se* A *tem uma linha ou coluna com zeros.*

iv) $\det(A) = 0$ *se e somente se* A *é singular.*

v) $\det(A^{-1}) = \frac{1}{\det(A)}$*, se* A *tem inversa.*

Do item (iv) do Teorema 5.12 obtemos também o seguinte corolário.

Corolário 5.13. *Um sistema de equações lineares* $A\mathbf{x} = \mathbf{b}$ *é determinado se e somente se* $\det A \neq 0$.

Lema 5.14. *O determinante de uma matriz diagonal é o produtório dos elementos em sua diagonal.*

Demonstração. Seja A uma matriz diagonal. Como o determinante é multilinear,

$$\det A = \det \left(\begin{array}{c|c} a_{11} & \mathbf{0}^T \\ \hline \mathbf{0} & [A]_{11} \end{array}\right) = a_{11} \det \left(\begin{array}{c|c} 1 & \mathbf{0}^T \\ \hline \mathbf{0} & [A]_{11} \end{array}\right)$$

e por indução nas colunas, $\det(A) = a_{11}a_{22}\ldots a_{nn}\det(\mathcal{I})$. ■

O seguinte Lema garante que existe determinante para matrizes triangulares.

Lema 5.15. *O determinante de uma matriz triangular é o produto dos elementos de sua diagonal.*

Demonstração. Seja A triangular superior. Aplicando eliminação de Gauss obtemos uma matriz diagonal. Se não houve troca de linhas durante o processo de eliminação, temos $\det(A) = \prod_i a_{ii}$.

Se houve troca de linhas, o resultado será uma matriz com alguma linha inteira igual a zero, e portanto $\det(A) = 0$.

O mesmo se aplica a matrizes triangulares inferiores, porque $\det(A) = \det(A^T)$. ■

Observe que este Lema também nos dá uma forma de calcular o determinante de qualquer matriz quadrada: se pudermos pô-la na forma triangular sem troca de linhas, somente usando operações elementares do tipo E_{i+kL}, seu determinante será o produto da diagonal. Quando houver troca de linhas, podemos lembrar a quantidade de trocas, e quando esta for ímpar, multiplicamos o produto da diagonal por -1.

O Exercício 128 pede a demonstração do Teorema 5.16.

Teorema 5.16. *Matrizes similares tem o mesmo determinante e o mesmo traço.*

O Lema 5.17 será usado quando descrevermos métodos para calcular determinantes.

Lema 5.17. *Se uma coluna* i *de uma matriz é combinação linear das outras (ou seja, as colunas são LD), então o determinante da matriz não muda se substituirmos a coluna* i *por zeros.*

Demonstração. Se uma coluna i de A é combinação linear das outras, então uma *linha* i de A^T é combinação linear das outras. Mas isto é o mesmo que dizer que a linha i pode ser obtida a partir da linha zero, somando múltiplos das outras linhas. Somar múltiplos de linhas a outras é uma operação elementar que não muda o determinante, portanto a matriz teria o mesmo determinante se a linha i de A^T fosse zero. Como $\det A = \det A^T$, terminamos a demonstração. ■

5.3 Existência e unicidade do determinante

Até agora temos falado de "funções determinante" (aquelas que satisfazem a definição 5.3); até mesmo definimos "uma" função determinante para matrizes de ordem dois. No entanto, não mostramos que existe uma função determinante para matrizes quadradas de qualquer ordem. E não provamos também que não há funções diferentes que satisfazem a definição.

Começamos pela existência. Para provar a existência do determinante para toda matriz, simplesmente mostramos um método para calcular determinantes de matrizes qualquer ordem.

Teorema 5.18. *Toda matriz quadrada tem um determinante (ou "há uma função determinante definida para todas as matrizes quadradas").*

Demonstração. Segue diretamente do Teorema 4.95 e do Lema 5.15: como podemos decompor qualquer matriz A em

$$A = PLU,$$

temos

$$\begin{aligned} \det P &= \pm 1 && \text{(matriz do tipo } E_{ij}) \\ \det L &= 1 && \text{(triangular, tem uns na diagonal)} \\ \det U &= \prod u_{ii}. && \text{(triangular)} \end{aligned}$$

Assim, como os tres determinantes são definidos, então para qualquer matriz $A = PLU$,

$$\det A = \det P \det U. \qquad \blacksquare$$

Nossa demonstração de existência não garante unicidade, porque a decomposição LU não é única. Assim, provaremos em seguida a unicidade do determinante. A técnica usual para mostrar que algo (uma função, ou qualquer outro objeto matemático) é único consiste em presumir que haja dois objetos satisfazendo a definição, e depois provar que ambos tem que necessariamente ser iguais.

Teorema 5.19. *O determinante de qualquer matriz é único.*

Demonstração. Sejam $\det^{(1)}$ e $\det^{(2)}$ duas funções determinante para matrizes de ordem n. Seja também $\delta = \det^{(1)} - \det^{(2)}$ a diferença entre elas.

Sabemos que para qualquer matriz quadrada A vale uma das duas afirmações:

i) Se A *não* é singular (ou seja, tem inversa), existe uma sequência de matrizes elementares que transformam A na identidade:

$$E_1 E_2 \dots E_k A = \mathcal{I}.$$

Como cada E_i tem inversas, podemos isolar a matriz A,

$$A = E_k^{-1} \dots E_2^{-1} E_1^{-1}.$$

ii) A é singular (não tem inversa). Neste caso, podemos levá-la à forma triangular, e a matriz resultante terá uma linha inteira com zeros. Assim, existe uma sequência de matrizes elementares *que somam múltiplos de linhas a outras*, ou seja, que não mudam o determinante, e que transformam A numa matriz

$$X = E_1 E_2 \dots E_k A$$

contendo uma linha inteira de zeros (ou seja, ao tentarmos resolver o sistema linear percebemos que a matriz é singular). Podemos também escrever

$$A = E_k^{-1} \dots E_2^{-1} E_1^{-1} X$$

Tratamos o caso (i). Observamos que

$$\begin{aligned}
\delta(A) &= \det^{(1)}(A) - \det^{(2)}(A) \\
&= \det^{(1)}(E_k^{-1} \dots E_2^{-1} E_1^{-1}) - \det^{(2)}(E_k^{-1} \dots E_2^{-1} E_1^{-1}). \\
&= \det^{(1)}(E_k^{-1}) \dots \overset{(1)}{\det}(E_2^{-1}) \det^{(1)}(E_1^{-1}) - \det^{(2)}(E_k^{-1}) \dots \det^{(2)}(E_2^{-1}) \det^{(2)}(E_1^{-1}) \\
& \qquad \text{(porque } \det AB = \det A \det B\text{)}
\end{aligned}$$

Mas como, de acordo com o Teorema 5.7, as duas funções determinante devem dar o mesmo valor para cada matriz elementar,

$$\begin{aligned}
\delta(A) &= \det^{(1)}(E_k^{-1}) \dots \det^{(1)}(E_2^{-1}) \det^{(1)}(E_1^{-1}) - \det^{(2)}(E_k^{-1}) \dots \det^{(2)}(E_2^{-1}) \det^{(2)}(E_1^{-1}) \\
&= 0.
\end{aligned}$$

Assim, no caso (i) temos $\delta(A) = 0$.

Agora abordamos o caso (ii). Se X tem uma linha com zeros,

$$\delta(X) = 0 - 0 = 0,$$

e como

$$\begin{aligned}
\delta(A) &= \det^{(1)}(A) - \det^{(2)}(A) \\
&= \det^{(1)}(E_k^{-1} \dots E_2^{-1} E_1^{-1} X) - \det^{(2)}(E_k^{-1} \dots E_2^{-1} E_1^{-1} X) \\
&= \det^{(1)}(E_k^{-1} \dots E_2^{-1} E_1^{-1}) \det^{(1)}(X) - \det^{(2)}(E_k^{-1} \dots E_2^{-1} E_1^{-1}) \det^{(2)}(X) \\
& \qquad \text{(porque } \det AB = \det A \det B\text{)} \\
&= \det^{(1)}(E_k^{-1} \dots E_2^{-1} E_1^{-1})(0) - \det^{(2)}(E_k^{-1} \dots E_2^{-1} E_1^{-1})(0) \\
&= 0 - 0 = 0,
\end{aligned}$$

no caso (ii) também temos $\delta(A) = 0$.

Assim, $\delta(A) = 0$ para toda matriz A, e portanto $\det^{(1)} = \det^{(2)}$. ■

5.4 Calculando determinantes

Nesta seção tratamos de como calcular determinantes. Embora nossa atenção fique voltada especialmente ao corpo dos reais, é importante observar que no cálculo de determinantes, as operações usadas devem ser aquelas definidas para o corpo ao qual as entradas da matriz pertencem, como mostra o exemplo 5.20.

★ **Exemplo 5.20.** Seja

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

uma matriz com entradas em $\mathbb{Z}_2$. Seu determinante é

$$\begin{aligned}\det A &= a_{11}a_{22} - a_{12}a_{21}\\ &= (1)(1) \oplus (0)(1)\\ &= 1 \oplus 0\\ &= 1.\end{aligned}$$

O determinante de A também poderia ter sido obtido a partir dos elementos da diagonal, porque A é triangular:

$$\det A = a_{11}a_{22} = (1)(1) = 1. \qquad \blacktriangleleft$$

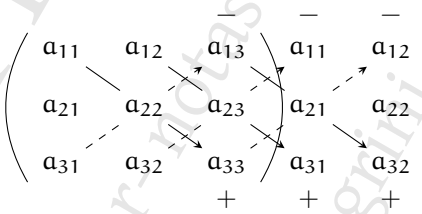
5.4.1 Determinantes de ordem 3: regra de Sarrus

Para ordem 3, a *regra de Sarrus* diz que

$$\det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = aei + bgf + dhc - ceg - bdi - fha.$$

Pode-se verificar que esta fórmula também mantém as propriedades de função determinante.

Há uma ilustração muito usada como auxílio para que se possa recordar deste regra: copiamos as duas primeiras colunas da matriz, pondo-as no lado direito. Em seguida, traçamos a diagonal principal e duas outrs paralelas, com linha contínua; a diagonal secundária e duas outras paralelas, com linhas tracejadas.

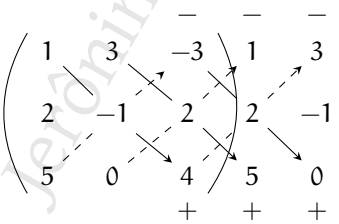


A figura nos diz que devemos somar os produtórios das diagonais marcadas com $(+)$, e subtrair do resultado os produtórios das diagonais marcadas com $(-)$.

Exemplo 5.21. Seja

$$A = \begin{pmatrix} 1 & 3 & -3 \\ 2 & -1 & 2 \\ 5 & 0 & 4 \end{pmatrix}$$

A regra de Sarrus nos diz que o determinante é dado por



E portanto temos

$$\begin{aligned}\det A &= +(1)(-1)(4) \quad +(3)(2)(5) \quad +(-3)(2)(0) \\ &\quad -(5)(-1)(-3) \quad -(0)(2)(1) \quad -(4)(2)(3) \\ &= -13.\end{aligned}$$

◀

5.4.2 Escalonamento e decomposição LU

Se uma matriz quadrada A tem ordem $n > 3$, podemos escaloná-la e calcular o produtório da diagonal, que será igual ao determinante. Se houver troca de linhas em quantidade ímpar, multiplicamos o determinante por -1.

Há algoritmos muito eficientes para obter a decomposição PLU de uma matriz, portanto também podemos tomar sua fatoração PLU e calcular $\det P \det L \det U$, ou simplesmente $\det P \det U$, porque o determinante de L sempre será um.

Exemplo 5.22. A seguir mostramos uma matriz e sua decomposição LU.

$$A = \begin{pmatrix} 1 & 2 & 0 & 4 \\ 3 & 0 & -2 & 0 \\ -1 & -1 & 1 & -4 \\ 0 & 0 & 3 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 \\ -1 & -1/6 & 1 & 0 \\ 0 & 0 & 9/2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 0 & 4 \\ 0 & -6 & -2 & -12 \\ 0 & 0 & 2/3 & -2 \\ 0 & 0 & 0 & 9 \end{pmatrix}$$

O determinante de A é $(-6)(2/3)(9) = -36$. ◀

Este é o método mais usado na prática para obtenção de determinante. Podemos resumi-lo da seguinte forma: se a decomposição PLU de A é $A = PLU$, então

$$\det A = (-1)^k \prod u_{ii},$$

onde k é a quantidade de operações de troca de linhas usada ao fatorar A em PLU.

Não mostraremos que este método de fato resulta em uma função determinante porque já o fizemos quando mostramos que o produtório da diagonal de matrizes triangulares é o determinante da matriz.

5.4.3 Expansão de Laplace

Apesar do uso de escalonamento ou decomposição PLU ser mais eficiente para calcular determinantes, há um outros método, bastante conhecido, que pode ser útil em algumas situações, e que é importante no desenvolvimento teórico de outros fatos.

Definição 5.23 (Menores e cofatores)**.** Seja A uma matriz quadrada. Denotamos por $[A]_{ij}$ a matriz de ordem $n-1$ obtida de A removendo sua i-ésima linha e j-ésima coluna.

O *menor complementar* de A relativo ao elemento a_{ij} é $\det[A]_{ij}$.

O *cofator* de um elemento a_{ij} de A é $(-1)^{i+j} \det[A]_{ij}$. Denotamos $\operatorname{cof}(A, i, j)$. ♦

Exemplo 5.24. Considere a matriz

$$A = \begin{pmatrix} 2 & -5 & 1 \\ 0 & 3 & 7 \\ -1 & 4 & 6 \end{pmatrix}$$

O menor complementar do elemento a_{23} é

$$\det[A]_{23} \begin{pmatrix} 2 & -5 \\ -1 & 4 \end{pmatrix} = 2 \cdot 4 - (-5)(-1) = 8 - 5 = 3.$$

Já o cofator é $(-1)^{2+3} \det[A]_{23} = -3$. ◀

O Teorema de Laplace explicita um método para obtenção do determinante de uma matriz quadrada de qualquer ordem.

Teorema 5.25. *Seja A uma matriz quadrada. Então, para qualquer linha i de A,*

$$\det(A) = \sum_j a_{ij}(-1)^{i+j} \det([A]_{ij}).$$

A demonstração a seguir foi redigida em grau de abstração e concisão um pouco acima do usado no resto do texto, e deve ser considerada opcional.

Demonstração. Como o determinante é único, basta mostrar que a função definida pela expansão de Laplace tem as propriedades que definem a função determinante.

(i) $\det(\mathcal{I}) = 1$. Segue por indução. A base é $\det(1) = 1$. A hipótese é que $\det(\mathcal{I}_{k-1}) = 1$. Para o passo, tomamos $\mathcal{I}_k$, Basta dividir a matriz em blocos:

$$\mathcal{I}_k = \left(\begin{array}{c:c} 1 & \mathbf{0}^t \\ \hdashline \mathbf{0} & \mathcal{I}_{k-1} \end{array}\right)$$

O determinante, de acordo com a expansão de Laplace é 1 multiplicado por $\det(\mathcal{I}_{k-1})$, que é 1.

(ii) *Colunas LD implicam em determinante zero.* Mostramos simplesmente que se há uma coluna zero, o determinante é zero (o Lema 5.17 nos diz que isso implica que o determinante deve ser zero também quando há colunas LD).

Se há uma coluna zero na matriz, haverá em todos os menores, e portanto todos os cofatores serão zero.

(iii) *Determinante é multilinear.* Para mostrar a multilinearidade, escolhemos uma linha i e mostramos (a) o efeito da multiplicação da linha i por um escalar k; e (b) se duas matrizes A e B são iguais, diferindo apenas pela i-ésima linha, o determinante de $A + B$ é o determinante da matriz que difere delas por ter a *soma* das duas linhas diferentes na posição i.

(a) Multiplicação de coluna i por escalar k: mostraremos que *cada termo da soma na expansão de Laplace é multiplicado por* k:

$$\det(A) = \sum_j \Big(k a_{ij}\Big)(-1)^{i+j} \det([A]_{ij}) \qquad = k \sum_j a_{ij}(-1)^{i+j} \det([A]_{ij})$$

O j-ésimo termo é multiplicado por k porque seu coeficiente na expansão de Laplace é $k a_{ij}$.

(b) Se A e B são iguais, diferindo apenas pela linha i, ou seja,

$$A = \left(\begin{array}{c} M_1 \\ \hdashline \alpha \\ \hdashline M_2 \end{array}\right), \quad B = \left(\begin{array}{c} M_1 \\ \hdashline \beta \\ \hdashline M_2 \end{array}\right),$$

e

$$C = \left(\begin{array}{c} M_1 \\ \hdashline \alpha + \beta \\ \hdashline M_2 \end{array}\right),$$

então temos

$$\begin{aligned}\det(C) &= \sum_j (a_{ij} + b_{ij})(-1)^{i+j} \det([A]_{ij}) \\ &= \left[\sum_j (a_{ij})(-1)^{i+j} \det([A]_{ij})\right] + \left[\sum_j (b_{ij})(-1)^{i+j} \det([A]_{ij})\right] \\ &= \det A + \det B. \end{aligned}$$ ■

Exemplo 5.26. Seja

$$A = \begin{pmatrix} 1 & 2 & -1 & -2 \\ 0 & 3 & 4 & 1 \\ 3 & 5 & 0 & 0 \\ -1 & 2 & 3 & 1 \end{pmatrix}.$$

Evidentemente escolhemos a linha com dois zeros, para facilitar o cálculo.

$$\begin{aligned}\det A &= 3(-1)^{3+1} \det[A]_{31} + 5(-1)^{3+2} \det[A]_{32} + 0(-1)^{3+3} \det[A]_{33} + 0(-1)^{3+4} \det[A]_{34} \\ &= 3(-1)^{3+1} \det[A]_{31} + 5(-1)^{3+2} \det[A]_{32} \\ &= 3(-1)^{3+1} \det \begin{pmatrix} 2 & -1 & -2 \\ 3 & 4 & 1 \\ 2 & 3 & 1 \end{pmatrix} + 5(-1)^{3+2} \det \begin{pmatrix} 1 & -1 & -2 \\ 0 & 4 & 1 \\ -1 & 3 & 1 \end{pmatrix} \\ &= 3 \cdot 1 + (-5)(-6) = 33. \end{aligned}$$ ◄

5.4.4 Fórmula de Leibniz

Embora tenhamos descrito *métodos* para calcular o determinante de matrizes de ordem n, nenhum deles era uma fórmula (uma forma fechada). Há uma fórmula que descreve o determinante, chamada de *fórmula de Leibniz*.

Definição 5.27 (permutação)**.** Uma *permutação* é uma função que recebe uma tupla de n elementos e devolve outra tupla, com os mesmos elementos, reordenando-os.

Denotamos por S_n o conjunto de todas as permutações de n elementos. ♦

Exemplo 5.28. Seja σ a permutação que recebe quatro elementos, e devolve o primeiro na terceira posição, o segundo na primeira posição, o terceiro na segunda posição e o quarto em sua posição original. Denotamos esta permutação por

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

Assim, $\sigma(a, b, c, d) = (b, c, a, d)$. ◄

Na fórmula de Leibniz usaremos permutações dos índices das colunas da matriz. Quando denotarmos a_{i,σ_i}, o significado é "o elemento da matriz, na linha i e a coluna dada pela permutação σ no i-ésimo argumento (ou seja, $\sigma(i)$). Por exemplo, usando a permutação

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

teríamos a_{1,σ_1} igual a $a_{1,2}$; a_{2,σ_2} igual a $a_{2,1}$; e a_{3,σ_3} igual a $a_{3,3}$.

Definição 5.29 (paridade de permutação)**.** A *paridade* de uma permutação σ é denotada por $\text{sgn}(\sigma)$, e é $+1$ se o número de inversões que aquela permutação induz é par, e -1 se o número de inversões é ímpar. ♦

Exemplo 5.30. Sejam σ_1, σ_2 e σ_3 permutações:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

A permutação σ_1 tem uma única inversão, $2 \leftrightarrow 1$ portanto $\text{sgn}(\sigma_1) = -1$.

A permutação σ_2 tem quatro inversões, $3 \leftrightarrow 1, 3 \leftrightarrow 2, 4 \leftrightarrow 1, 4 \leftrightarrow 2$, portanto $\text{sgn}(\sigma_1) = +1$.

A permutação σ_1 tem três inversões, $4 \leftrightarrow 1, 4 \leftrightarrow 2, 4 \leftrightarrow 3$ portanto $\text{sgn}(\sigma_1) = -1$. ◄

Teorema 5.31. *O determinante de qualquer matriz quadrada A é dado por*

$$\det(A) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma_i}.$$

O determinante de A é uma soma com $n!$ termos (um para cada σ em S_n). Cada termo é da forma

$$(\pm 1) a_{1\square} a_{2\square} \ldots a_{n\square}.$$

Os índices indicados por $\square$ nesta última fórmula são os índices $1, 2, \ldots, n$, *permutados* de alguma forma, e o sinal ± 1 é $+1$ se o número de inversões desta permutação é par, e -1 caso contrário.

Demonstração. Mostramos que a função expressa pela fórmula de Leibniz tem as propriedades de função determinante.

(i) $\det(\mathcal{I}) = 1$. Pode-se verificar claramente que todos os termos do somatório na fórmula de Leibniz serão zero, exceto $a_{11} a_{22} \ldots a_{nn}$, que resultará em 1.

(ii) *Colunas LD implicam em determinante zero.* Usamos o Lema 5.17 e mostramos que se há uma coluna zero, o determinante é zero. Se uma coluna i é composta de zeros, teremos $a_{ij} = 0$ para todo j. Mas cada termo da soma na fórmula de Leibniz inclui $a_{i\square}$, e portanto todos os termos serão zero.

(iii) *Determinante é multilinear.* Mostraremos (a) que a multiplicação de uma linha por escalar resulta na multiplicação do determinante pelo mesmo escalar; e (b) que se A e B diferem somente na linha i, então a soma dos determinantes de A e B é o determinante da matriz que só difere de A e B por ter a soma da i-ésima linha (de A e de B).

(a) Multiplicar uma coluna por k significa multiplicar todos os $a_{i\square}$ por k. Como na fórmula de Leibniz cada termo terá exatamente um $a_{i\square}$:

$$\text{sgn}(\sigma_1) a_{\square 1} \cdots k a_{\square 1} \cdots a_{\square n} + \text{sgn}(\sigma_2) a_{\square 1} \cdots k a_{\square 1} \cdots a_{\square n} + \cdots$$

fatoramos e obtemos k multiplicado pelo valor anterior de determinante:

$$k \Big(\text{sgn}(\sigma_1) a_{\square 1} \cdots a_{\square i} \cdots a_{\square n} + \text{sgn}(\sigma_2) a_{\square 1} \cdots a_{\square i} \cdots a_{\square n} + \cdots \Big)$$

(b) Se A e B são iguais, exceto pela linha i, ou seja,

$$A = \begin{pmatrix} M_1 \\ \hdashline \alpha \\ \hdashline M_2 \end{pmatrix}, \quad B = \begin{pmatrix} M_1 \\ \hdashline \beta \\ \hdashline M_2 \end{pmatrix},$$

e

$$C = \begin{pmatrix} M_1 \\ \alpha + \beta \\ M_2 \end{pmatrix},$$

então

$$\det(C) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} c_{j,\sigma_j}.$$

Mas como em cada permutação haverá um elemento da linha i (ou seja, a linha contendo $\alpha + \beta$),

$$\begin{aligned}
\det(C) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \Big(\prod_{j \neq i} c_{j\sigma_j} \Big) (a_{i,\sigma_i} + b_{i,\sigma_i}) \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \Big(\prod_{j \neq i} c_{j\sigma_j} \Big) (a_{i,\sigma_i}) + \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \Big(\prod_{j \neq i} c_{j\sigma_j} \Big) (b_{i,\sigma_i}) \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} a_{j\sigma_j} + \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} b_{j\sigma_j} \\
&= \det A + \det B.
\end{aligned}$$

■

Exemplo 5.32. Seja

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

As permutações de $(1, 2, 3)$ e suas paridades são

$$\begin{aligned}
&(1,2,3), +1 \\
&(2,3,1), +1 \\
&(3,1,2), +1 \\
&(1,3,2), -1 \\
&(2,1,3), -1 \\
&(3,2,1), -1
\end{aligned}$$

Então

$$\begin{aligned}
\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma_i} \\
&= +a_{11}a_{22}a_{33} \\
&\quad + a_{12}a_{23}a_{31} \\
&\quad + a_{13}a_{21}a_{32} \\
&\quad - a_{11}a_{23}a_{32} \\
&\quad - a_{12}a_{21}a_{33} \\
&\quad - a_{13}a_{22}a_{31},
\end{aligned}$$

exatamente como descrevemos anteriormente pela regra de Sarrus. ◄

5.4.5 Por blocos

Pode ser útil em diversas situações calcular o determinante de matrizes particionadas em blocos. Nesta Seção apresentamos alguns Teoremas a respeito destes determinantes.

Teorema 5.33.

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

Exemplo 5.34.

$$\det \left(\begin{array}{cc:cc} 1 & 2 & 37 & 20 \\ 3 & 8 & 1 & 0 \\ \hdashline 0 & 0 & 2 & 9 \\ 0 & 0 & 1 & 4 \end{array}\right) = \det \begin{pmatrix} 1 & 2 \\ 3 & 8 \end{pmatrix} \det \begin{pmatrix} 9 & 4 \\ 2 & 1 \end{pmatrix} = (2)(-1) = -2.$$

◀

Teorema 5.35. *Se* $\mathbf{b}$ *é coluna,* $\mathbf{c}^T$ *é linha, e* d *é um único elemento,*

$$\det \begin{pmatrix} A & \mathbf{b} \\ \mathbf{c}^T & d \end{pmatrix} = (d+1)\det A - \det(A + \mathbf{b}\mathbf{c}^T).$$

Exemplo 5.36.

$$\begin{aligned} \det \left(\begin{array}{ccc:c} 1 & 2 & 37 & 20 \\ 3 & 8 & 1 & 0 \\ 0 & 0 & 2 & 9 \\ \hdashline 0 & 0 & 1 & 4 \end{array}\right) &= (4+1)\det \begin{pmatrix} 1 & 2 & 37 \\ 3 & 8 & 1 \\ 0 & 0 & 2 \end{pmatrix} - \det \left[A + \begin{pmatrix} 20 \\ 0 \\ 9 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \end{pmatrix} \right] \\ &= (5)(4) - \det \begin{pmatrix} 1 & 2 & 57 \\ 3 & 8 & 1 \\ 0 & 0 & 11 \end{pmatrix} \\ &= 20 - 22 = -2. \end{aligned}$$

◀

★ 5.5 Matrizes complexas

O determinante de uma matriz complexa é definido e calculado da mesma forma que o de matrizes reais.

Teorema 5.37. *Seja* A *uma matriz quadrada complexa. Então*

i) $\det(A^H) = \overline{\det A}$,

ii) $\operatorname{Tr}(A^H) = \overline{\operatorname{Tr} A}$.

Exemplo 5.38. Se

$$A \begin{pmatrix} 1 & 1-i \\ 3 & 2-i \end{pmatrix},$$

temos

$$A^H = \begin{pmatrix} 1 & 3 \\ 1+i & 2+i \end{pmatrix}.$$

Agora,

$$\det A = \det \begin{pmatrix} 1 & 1-i \\ 3 & 2-i \end{pmatrix} = (2-i) - (3-3i) = -1 + 2i$$

e

$$\det A^H = \det \begin{pmatrix} 1 & 3 \\ 1+i & 2+i \end{pmatrix} = (2+i) - (3+3i) = -1 - 2i \qquad \blacktriangleleft$$

Exemplo 5.39. Se

$$A \begin{pmatrix} 2 & 1-i \\ 3 & 2-i \end{pmatrix}, \quad A^H = \begin{pmatrix} 2 & 3 \\ 1+i & 2+i \end{pmatrix},$$

temos

$$\begin{aligned} \mathrm{Tr}(A) &= 4 - i \\ \mathrm{Tr}(A^H) &= 4 + i. \end{aligned} \qquad \blacktriangleleft$$

5.6 Aplicações

5.6.1 Regra de Cramer

A "regra de Cramer" é um teorema que dá um método simples para resolver sistemas de equações lineares usando determinantes. É possivelmente a aplicação mais conhecida de determinantes.

Teorema 5.40 (Regra de Cramer)**.** *Em um sistma linear representado por* $A\mathbf{x} = \mathbf{b}$*, onde o vetor* $\mathbf{x}$ *é a incógnita, tem-se que*

$$x_i = \frac{\det(A_i)}{\det(A)},$$

onde A_i *é a matriz obtida trocando a* i*-ésima coluna de* A *por* $\mathbf{b}$*.*

Demonstração. Seja $\mathbf{s}$ a solução para $A\mathbf{s} = \mathbf{b}$ – ou seja,

$$\begin{aligned} a_{11}s_1 + a_{12}s_2 + \ldots + a_{1n}s_n &= b_1 \\ a_{21}s_1 + a_{22}s_2 + \ldots + a_{2n}s_n &= b_2 \\ &\vdots \\ a_{n1}s_1 + a_{n2}s_2 + \ldots + a_{nn}s_n &= b_n \end{aligned}$$

Agora, multiplicamos cada i-ésima equação pelo cofator A_{i1}.

$$\begin{aligned} A_{11}a_{11}s_1 + A_{11}a_{12}s_2 + \ldots + A_{11}a_{1n}s_n) &= A_{11}b_1 \\ A_{21}a_{21}s_1 + A_{21}a_{22}s_2 + \ldots + A_{21}a_{2n}s_n &= A_{21}b_2 \\ &\vdots \\ A_{n1}a_{n1}s_1 + A_{n1}a_{n2}s_2 + \ldots + A_{n1}a_{nn}s_n &= A_{n1}b_n \end{aligned}$$

Somando as equações, obtemos

$$s_1(A_{11}a_{11} + A_{21}a_{21} + \ldots + A_{n1}a_{n1})$$

$$
\begin{aligned}
&+s_2(A_{11}a_{12} + A_{21}a_{22} + \ldots + A_{n1}a_{n2}) \\
&+\ldots \\
&+s_n(A_{11}a_{1n} + A_{21}a_{2n} + \ldots + A_{n1}a_{nn}) \\
&= b_1A_{11} + b_2A_{21} + \ldots + b_nA_{n1}.
\end{aligned}
$$

O primeiro termo é s_1 multiplicado pelo determinante de A (pelo teorema de Laplace). Os outros termos do lado esquerdo são zero. O lado direito é o determinante de

$$
A_1 = \begin{pmatrix} b_1 & a_{12} & \cdots & a_{1n} \\ b_2 & a_{22} & & a_{2n} \\ \vdots & & \ddots & \\ b_n & a_{n2} & & a_{nn} \end{pmatrix}
$$

Então

$$
s_1 \det(A) = \det(A_1),
$$

e

$$
s_1 = \frac{\det(A_1)}{\det(A)}.
$$

O mesmo vale para os outros s_i. ■

Quando o determinante de A é zero, o sistema não tem solução.

Exemplo 5.41. Considere o sistema linear

$$
\begin{cases} 2x_1 - 3x_2 + 3x_3 = 2 \\ x_1 + x_2 + x_3 = 1 \\ x_1 - 2x_2 - x_3 = -2. \end{cases}
$$

Este sistema pode ser representado como $A\mathbf{x} = \mathbf{b}$, com

$$
A = \begin{pmatrix} 2 & -3 & 3 \\ 1 & 1 & 1 \\ 1 & -2 & -1 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} 2 \\ 1 \\ -2 \end{pmatrix}.
$$

O determinante de A é -13. As matrizes A_1, A_2 e A_3 são

$$
A_1 = \begin{pmatrix} \mathbf{2} & -3 & 3 \\ \mathbf{1} & 1 & 1 \\ \mathbf{-2} & -2 & -1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 2 & \mathbf{2} & 3 \\ 1 & \mathbf{1} & 1 \\ 1 & \mathbf{-2} & -1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 2 & -3 & \mathbf{2} \\ 1 & 1 & \mathbf{1} \\ 1 & -2 & \mathbf{-2} \end{pmatrix},
$$

e calculamos

$$
\det(A_1) = 5, \qquad \det(A_2) = -3, \qquad \det(A_3) = -15.
$$

Já temos a solução para o sistema:

$$
\begin{aligned}
x_1 &= \frac{\det(A_1)}{\det(A)} = -\frac{5}{13}, \\
x_2 &= \frac{\det(A_2)}{\det(A)} = \frac{3}{13}, \\
x_3 &= \frac{\det(A_3)}{\det(A)} = \frac{15}{13}.
\end{aligned}
$$

◄

Sistemas lineares com soluções integrais

Aqui apresentamos uma aplicação da regra de Cramer na demonstração de um teorema, que nos garante qua sob certas condições a solução para um sistema de equações será inteira.

Definição 5.42 (matriz totalmente unimodular)**.** Uma matriz A é *totalmente unimodular* se os determinantes de todas as suas submatrizes quadradas são iguais a 1, -1 ou 0. ♦

Note que uma matriz não precisa ser quadrada para ser totalmente unimodular. Apenas exigimos que os determinantes de todas suas submatrizes quadradas sejam unitários ou zero.

Exemplo 5.43. A matriz

$$A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

é totalmente unimodular, porque as suas submatrizes quadradas tem determinante 1, -1 ou zero. ◀

Teorema 5.44. *Se A é quadrada e totalmente unimodular e $\mathbf{b} \in \mathbb{Z}^n$, então a solução para o sistema $A\mathbf{x} = \mathbf{b}$, se existir, pertence a $\mathbb{Z}^n$.*

Demonstração. Se o sistema tem solução, o valor de x_i é dado por

$$x_i = \frac{\det(A_i)}{\det(A)}.$$

O determinante de A_i será inteiro, porque a matriz A só tinha coeficientes inteiros, e o vetor $\mathbf{b}$, que substitui uma das colunas, também. Como $\det(A) = \pm 1$, dividimos um inteiro por ± 1, obtendo $x_i \in \mathbb{Z}$. ■

Exemplo 5.45. Seja

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

totalmente unimodular, e $\mathbf{b} = (3, 2, 8)^T$. Considere o sistema $A\mathbf{x} = \mathbf{b}$:

$$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \\ 8 \end{pmatrix}$$

Reescrevemos o sistema, obtendo

$$\begin{array}{rrl} x_1 & +x_3 & = 3 \\ x_1 + x_2 & & = 2 \\ x_2 & & = 8 \end{array}$$

Temos $x_2 = 8$, o que implica que $x_1 = -6$. Consequentemente, $x_3 = 9$, e a solução $\mathbf{x} = (-6, 8, 9)^T$ é integral. ◀

Sistemas lineares em $\mathbb{C}$

A regra de Cramer funciona em qualquer corpo, portanto podemos usá-la para resolver sistemas lineares em $\mathbb{C}$.

Considere o sistema linear a seguir, com variáveis complexas.

$$\begin{cases} 2ix_1 & & -2x_3 = & 1 \\ x_1 & +3x_2 & = & 0 \\ ix_1 & & -ix_3 = & 4i \end{cases}$$

O sistema pode ser reescrito como $A\mathbf{x} = \mathbf{b}$, com

$$A = \begin{pmatrix} 2i & 0 & -2 \\ 1 & 3 & 0 \\ i & 0 & -i \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} 1 \\ 0 \\ 4i \end{pmatrix}$$

Temos

$$\det A = 6i + 6,$$

e

$$A_1 = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 3 & 0 \\ 4i & 0 & -i \end{pmatrix}, \quad A_2 = \begin{pmatrix} 2i & 1 & -2 \\ 1 & 0 & 0 \\ i & 4i & -i \end{pmatrix}, \quad A_3 = \begin{pmatrix} 2i & 0 & 1 \\ 1 & 3 & 0 \\ i & 0 & 4i \end{pmatrix}.$$

Os determinantes são

$$\begin{aligned} \det A_1 &= 21i, \\ \det A_2 &= -7i, \\ \det A_3 &= -3i - 24 \end{aligned}$$

A solução é, portanto,

$$\begin{array}{lllll} x_1 & = \frac{21i}{6i+6} & = \frac{7i}{2i+2} & = \frac{7}{4} + \frac{7}{4}i, \\ x_2 & = \frac{9i}{6i+6} & = -\frac{7i}{6i+6} & = -\frac{7}{12} - \frac{7}{12}i, \\ x_3 & = \frac{-3i-24}{6i+6} & = -\frac{i+8}{2i+2} & = -\frac{9}{4} + \frac{7}{4}i. \end{array}$$

Sistemas lineares em $\mathbb{Z}_2$

Damos um exemplo de resolução de sistema linear sobre $\mathbb{Z}_2$, usando a regra de Cramer.

★ **Exemplo 5.46.** No exemplo 5.20 verificamos que o determinante de

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

com entradas em $\mathbb{Z}_2$, é 1. Agora resolveremos o sistema $A\mathbf{x} = \mathbf{b}$, com

$$\mathbf{b} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Usando a regra de Cramer,

$$A_1 = \begin{pmatrix} \mathbf{1} & 0 \\ \mathbf{0} & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & \mathbf{1} \\ 1 & \mathbf{0} \end{pmatrix},$$

e temos

$$\begin{aligned}
\det A_1 &= (A_1)_{11}(A_1)_{22} \oplus (A_1)_{12}(A_1)_{21} \\
&= (1)(1) \oplus (0)(0) \\
&= 1 \oplus 0 \\
&= 1, \\
\det A_2 &= (A_1)_{11}(A_1)_{22} \oplus (A_1)_{12}(A_1)_{21} \\
&= (1)(0) \oplus (1)(1) \\
&= 0 \oplus 1 \\
&= 1.
\end{aligned}$$

Para calcular os valores de x_1 e x_2, multiplicamos $\det A_i$ pelo inverso multiplicativo de $\det A$. Como $\det A = 1$, seu inverso em $\mathbb{Z}_2$ é também 1.

$$\begin{aligned}
x_1 &= \det A_1 (\det A)^{-1} \\
&= (1)(1) \\
&= 1, \\
x_2 &= \det A_2 (\det A)^{-1} \\
&= (1)(1) \\
&= 1.
\end{aligned}$$

Facilmente verificamos que

$$\begin{aligned}
A\mathbf{x} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\
&= 1 \begin{pmatrix} 1 \\ 1 \end{pmatrix} \oplus 1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} && \text{(combinação linear de colunas, sec.4.2.2)} \\
&= \begin{pmatrix} 1 \oplus 0 \\ 1 \oplus 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
&= \mathbf{b}.
\end{aligned}$$

◀

5.6.2 Área de triângulos, volume de pirâmides

O cálculo da área de triângulos em $\mathbb{R}^2$ a partir dos vértices pode ser descrito pelo determinante de uma matriz de ordem 3.

Teorema 5.47. *A área do triângulo com vértices* $A = (a_1, a_2)^T$, $B = (b_1, b_2)^T$, $C = (c_1, c_2)^T$ *é dada por*

$$\left| \frac{1}{2} \det \begin{pmatrix} b_1 - a_1 & c_1 - a_1 \\ b_2 - a_2 & c_2 - a_2 \end{pmatrix} \right| = \left| \frac{1}{2} \det \begin{pmatrix} a_1 & a_2 & 1 \\ b_1 & b_2 & 1 \\ c_1 & c_2 & 1 \end{pmatrix} \right|$$

Demonstração. Sejam A, B, C pontos em $\mathbb{R}^2$. Observamos que $B - A$ e $C - A$ podem ser vistos como dois vetores com tamanho igual a dois lados do triângulo $\triangle_{ABC}$. A área do paralelogramo gerado por esses vetores, dividida por dois, é igual à área do triângulo. Com isso chegamos a

$$\left|\frac{1}{2}\det\begin{pmatrix} b_1 - a_1 & c_1 - a_1 \\ b_2 - a_2 & c_2 - a_2 \end{pmatrix}\right|.$$

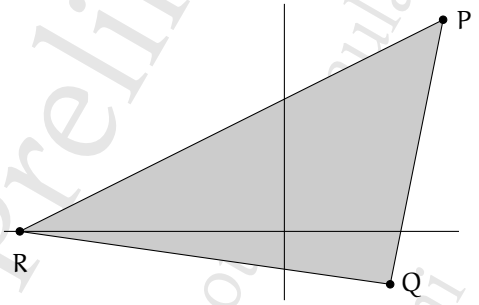
Este determinante é igual a

$$(b_1 - a_1)c_2 + (a_2 - b_2)c_1 + a_1 b_2 - a_2 b_1,$$

o mesmo valor do determinante de ordem 3 dado no enunciado do teorema. ■

Removendo o módulo da fórmula, tem-se a área com orientação (volume orientado) do triângulo: se o triângulo não é degenerado, os dois vetores $B - A$ e $C - A$ formam uma base para $\mathbb{R}^2$. O sinal do determinante nos dará a orientação destes vetores com relação à base canônica.

Exemplo 5.48. O triângulo com vértices $P = (3, 4)^T$, $Q = (2, -1)^T$, e $R = (-5, 0)^T$, na figura a seguir,



tem área igual a

$$\left|\frac{1}{2}\det\begin{pmatrix} 3 & 4 & 1 \\ 2 & -1 & 1 \\ -5 & 0 & 1 \end{pmatrix}\right| = \left|\frac{-36}{2}\right| = 18. \quad ◀$$

O exeercício 125 pede a demonstração do Teorema 5.49, que nos dá uma fórmula para o volume de tetraedros.

Teorema 5.49. *Sejam P, Q, R, S pontos em $\mathbb{R}^3$ formando uma pirâmide. O volume da pirâmide é dado por*

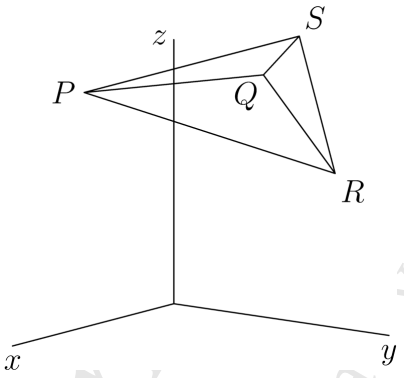
$$\frac{1}{6}\left|\det\begin{pmatrix} q_x - p_x & r_x - p_x & s_x - p_x \\ q_y - p_y & r_y - p_y & s_y - p_y \\ q_z - p_z & r_z - p_z & s_z - p_z \end{pmatrix}\right| = \frac{1}{6}\left|\det\begin{pmatrix} 1 & 1 & 1 & 1 \\ p_x & q_x & r_x & s_x \\ p_y & q_y & r_y & s_y \\ p_z & q_z & r_z & s_z \end{pmatrix}\right|.$$

Assim como para triângulos, a remoção do módulo nos dará volume orientado, permitindo verificar a base de $\mathbb{R}^3$ formada por $Q - P$, $R - P$ e $S - P$.

Exemplo 5.50. Calcularemos o volume da pirâmide PQRS, sendo

$$P = (3, 1, 3)^T$$

$$Q = (1,2,3)^T$$
$$R = (1,3,2)^T$$
$$S = (3,4,4)^T$$



De acordo como Teorema 5.49, o volume é

$$\frac{1}{6}\det\begin{pmatrix}1&1&1&1\\3&1&1&3\\1&2&3&4\\3&3&2&4\end{pmatrix} = -\frac{8}{6}.$$

O sinal negativo, como visto no início deste Capítulo, é indicativo da orientação da base formada por (P, Q, R, S), que não é concordante com a base canônica (se trocarmos dois dos vetores de posição ao montar a matriz, por exemplo para (P, Q, S, R), a base passará ater a mesma orientação da bae canônica, e o sinal passará a ser positivo). ◀

5.6.3 Equação da circunferência passando por tres pontos

Mostraremos agora como obter a equação da circunferencia que passa por tres pontos dados. começamos mostrando uma forma alternativa da equação da circunferência.

Usualmente a equação da circunferência é escrita como

$$\begin{aligned}(x-a)^2 + (y-b)^2 &= r^2\\ (x^2 - 2ax + a^2) + (y^2 - 2by + b^2) &= r^2\\ x^2 + y^2 - 2ax - 2by + a^2 + b^2 - r^2 &= 0\end{aligned}$$

Multiplicamos ambos os lados por algum número $\alpha \neq 0$,

$$A(x^2 + y^2) - 2Aax - 2Aby + A(a^2 + b^2 - r^2) = 0$$

Substituindo $B = -2Aa$, $C = -2Ab$, $D = A(a^2 + b^2 - r^2)$,

$$A(x^2 + y^2) + Bx + Cy + D = 0. \tag{5.1}$$

Teorema 5.51. *Dados pontos* P, Q, R *em* $\mathbb{R}^2$*, a equação da reta que passa por eles é dada por*

$$\det \begin{pmatrix} x^2+y^2 & x & y & 1 \\ x_p^2+y_p^2 & x_p & y_p & 1 \\ x_q^2+y_q^2 & x_q & y_q & 1 \\ x_r^2+y_r^2 & x_r & y_r & 1 \end{pmatrix} = 0. \tag{5.2}$$

Demonstração. Usando a expansão de Laplace na primeira linha, o determinante é

$$\det \begin{pmatrix} x^2+y^2 & x & y & 1 \\ x_p^2+y_p^2 & x_p & y_p & 1 \\ x_q^2+y_q^2 & x_q & y_q & 1 \\ x_r^2+y_r^2 & x_r & y_r & 1 \end{pmatrix} = (x^2+y^2)\det \begin{pmatrix} x_p & y_p & 1 \\ x_q & y_q & 1 \\ x_r & y_r & 1 \end{pmatrix} + Bx + Cy + D,$$

que é claramente a equação de uma circunferência, conforme a equação (5.1). Para verificarmos que ela passa por P, Q e R, observamos que

- O determinante de ordem 3 que aparece na expressão é a área do triângulo PQR, e portanto será positivo a não ser quanto os tres pontos forem colineares (quando então será zero);
- quando substituímos as coordenadas de um desses pontos – por exemplo P, em x e y, teremos duas linhas iguais em (5.2),e o determinante é zero (ou seja, o ponto satisfaz a equação). ■

Exemplo 5.52. Sejam $P = (1,1)^T$, $Q = (1,2)^T$ e $R = (3,3)^T$. De acordo com o Teorema 5.51, a circunferência passando por estes pontos é

$$\det \begin{pmatrix} x^2+y^2 & x & y & 1 \\ 1^2+1^2 & 1 & 1 & 1 \\ 1^2+2^2 & 1 & 2 & 1 \\ 3^2+3^2 & 3 & 3 & 1 \end{pmatrix} = \det \begin{pmatrix} x^2+y^2 & x & y & 1 \\ 2 & 1 & 1 & 1 \\ 5 & 1 & 2 & 1 \\ 18 & 3 & 3 & 1 \end{pmatrix} = 0,$$

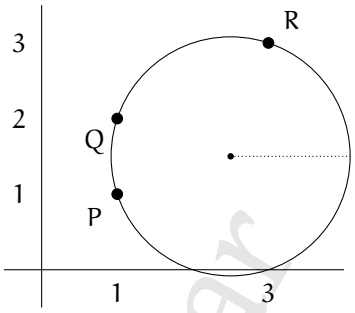
o que nos dá

$$\begin{aligned} -2(x^2+y^2)+10x+6y-12 &= 0 \\ (x^2+y^2)-5x-3y+6 &= 0 && \text{(dividimos por } -2) \\ (x^2-5x)+(y^2-3y)+6 &= 0 \\ \left(x^2-5x+\frac{25}{4}\right)+\left(y^2-3y+\frac{9}{4}\right)+6+\left[-\frac{25}{4}-\frac{9}{4}\right] &= 0 && \text{(completamos quadrados)} \\ \left(x-\frac{5}{2}\right)^2+\left(y-\frac{3}{2}\right)^2-\frac{5}{2} &= 0. \end{aligned}$$

Concluímos que a circunferência que procuramos tem centro $(5/2, 3/2)$ e raio $\sqrt{5/2}$. Verificamos que os três pontos de fato estão na borda da circunferencia:

$$\begin{aligned} (1-5/2)^2+(1-3/2)^2-5/2 &= 9/4+1/4-5/2 = 0 \\ (1-5/2)^2+(2-3/2)^2-5/2 &= 9/4+1/4-5/2 = 0 \\ (3-5/2)^2+(3-3/2)^2-5/2 &= 1/4+9/4-5/2 = 0 \end{aligned}$$

A figura a seguir ilustra a circunferencia e os pontos P, Q e R.



A circunferencia da figura tem o centro e raio que determinamos, e vemos que ela passa pelos tres pontos dados. ◀

5.6.4 O Teorema do Valor Médio (generalizado)

Relembramos do Cálculo o Teorema do Valor Médio.

Teorema 5.53 (do valor médio)**.** *Seja* f *uma função contínua no intevalo* $[a,b] \in \mathbb{R}$*, e diferenciável em* (a,b)*. Então existe* $c \in (a,b)$ *tal que*

$$\frac{f(b)-f(a)}{b-a} = f'(c).$$

Há uma generalização deste Teorema para duas variáveis. Esta forma mais geral é chamada de "Teorema do Valor Médio de Cauchy", ou "Teorema do Valor Médio Generalizado".

Teorema 5.54 (do valor médio, generalizado)**.** *Se* f *e* g *são contínuas no intevalo* $[a,b] \in \mathbb{R}$*, e diferenciáveis em* (a,b)*, com* $g(a) \neq g(b)$*, então existe* $c \in (a,b)$ *tal que*

$$\frac{f(b)-f(a)}{g(b)-g(a)} = \frac{f'(c)}{g'(c)}.$$

Demonstração. Seja

$$H(x) = \det \begin{pmatrix} f(x)-f(a) & f(b)-f(a) \\ g(x)-g(a) & g(b)-g(a) \end{pmatrix} = \det \begin{pmatrix} f(a) & f(x) & f(b) \\ g(a) & f(x) & g(b) \\ 1 & 1 & 1 \end{pmatrix}$$

Claramente, H é zero quando $x = a$ e quando $x = b$, porque isto implicaria em duas colunas iguais no determinante da direita.

A função H vale

$$\begin{aligned} H(x) &= \big[f(x)-f(a)\big] \underbrace{\big[g(b)-g(a)\big]}_{A} - \underbrace{\big[f(b)-f(a)\big]}_{B} \big[g(x)-g(a)\big] \\ &= Af(x) - Af(a) - Bg(x) + Bg(a) \\ &= Af(x) - Bg(x) + k, \end{aligned}$$

e como f e g são diferenciáveis e k é constante, H é diferenciável.

Temos agora dois fatos:

i) $H(a) = H(b) = 0$;

ii) H é diferenciável em (a, b).

Pelo Teorema do valor médio, (i) e (ii) implicam na existência de um ponto $c \in [a, b]$ tal que

$$\frac{H(b) - H(a)}{b - a} = H'(c)$$
$$\frac{0}{b - a} = H'(c),$$

ou seja, há um ponto no intervalo onde a derivada de H é zero.

A deerivada do determinante de ordem dois é fácil de calcular: a variável x aparece apenas na primeira coluna, portanto derivamos esta coluna:

$$H'(x) = \det \begin{pmatrix} f'(x) & f(b) - f(a) \\ g'(x) & g(b) - g(a) \end{pmatrix}$$

Como o enunciado nos garante que $g(a) \neq g(b)$, substituímos c em x e temos

$$f'(c)\big[g(b) - g(a)\big] - g'(c)\big[f(b) - f(a)\big] = 0$$
$$\frac{f'(c)}{g'(c)} = \frac{f(b) - f(a)}{g(b) - g(a)}.$$ ■

Exemplo 5.55. Sejam $f(x) = x^2$ e $g(x) = \sqrt{x}$ em $[0, 4]$.

$$\frac{4^2 - 0^2}{\sqrt{4} - \sqrt{0}} = \frac{\frac{d}{dc}c^2}{\frac{d}{dc}\sqrt{c}}$$
$$\frac{16}{2} = \frac{2c}{c\sqrt{c}}$$
$$8 = \frac{2}{\sqrt{c}}$$
$$\sqrt{c} = \frac{1}{4}$$
$$c = \frac{1}{16}.$$

No entanto, nem sempre é possível determinar c assim facilmente. ◄

O Teorema do Valor Médio de Cauchy pode ser usado para demonstrar a validade da regrade L'Hôpital. A seguir esboçamos esta demonstração.

Teorema 5.56 (regra de L'Hôpital)**.** *Sejam f e g contínuas no intevalo $[a, b] \in \mathbb{R}$, e diferenciáveis em (a, b), com $g'(x) \neq 0$ para todo $x \in (a, b)$. Seja $c \in (a, b)$, com $f(c) = g(c) = 0$. Então*

$$\lim_{x \to c} \frac{f(x)}{g(x)} = \lim_{x \to c} \frac{f'(x)}{g'(x)},$$

se o limite no lado direito da equação existir.

Demonstração. (Esboço)

Usamos o Teorema do Valor Médio de Cauchy, mas ao invés de fixar um intervalo $[a, b]$, variamos o limite superior, e denotamos nosso intervalo por $[a, x]$.

Assim, fixado a e definido algum $x > a$, sabemos que existe algum $c \in [a, x]$ tal que

$$\frac{f'(c)}{g'(c)} = \frac{f(x) - f(a)}{g(x) - g(a)}.$$

Mas se $f(a) = g(a) = 0$, então

$$\frac{f'(c)}{g'(c)} = \frac{f(x)}{g(x)}.$$

Agora aproximarmos x de a. Claramente, quando $x \to a$, temos $c \to a$ também, porque c deve estar no intervalo $[a, x]$. Assim,

$$\lim_{x \to a^+} \frac{f'(c)}{g'(c)} = \lim_{x \to a^+} \frac{f'(x)}{g'(x)}$$
$$\lim_{x \to a^+} \frac{f(x)}{g(x)} = \lim_{x \to a^+} \frac{f'(x)}{g'(x)}.$$

Repetimos o mesmo raciocínio para o limite pela esquerda, tomando intervalos $[x, b]$ e fazendo $x \to b$. ■

5.6.5 O Wronskiano

Suponha que queiramos determinar se um conjunto de funções é linearmente independente em um certo intervalo.

Definição 5.57 (Wronskiano)**.** Sejam $f_1, f_2, \ldots, f_n$ funções em $C^{n-1}[a, b]$, ou seja, $n - 1$ vezes diferenciáveis em um intervalo $[a, b]$. O *Wronskiano* deste conjunto de funções é o determinante

$$\det \begin{pmatrix} f_1 & f_2 & \cdots & f_n \\ f_1' & f_2' & \cdots & f_n' \\ f_1'' & f_2'' & \cdots & f_n'' \\ \vdots & & & \\ f_1^{(n-1)} & f_2^{(n-1)} & \cdots & f_n^{(n-1)} \end{pmatrix}. \qquad \blacklozenge$$

Exemplo 5.58. Sejam $f(x) = x^2$ e $g(x) = \cos(x)$. O Wronskiano das duas funções é

$$\det \begin{pmatrix} f & g \\ f' & g' \end{pmatrix} = \det \begin{pmatrix} x^2 & \cos(x) \\ 2x & -\operatorname{sen}(x) \end{pmatrix} = -x^2 \operatorname{sen}(x) - 2x \cos(x).$$

Vemos claramente que o Wronskiano, sendo obtido por soma, subtração e multiplicações de funções, também é uma função de x. ◀

Teorema 5.59. *Sejam $f_1, f_2, \ldots, f_n$ funções $n - 1$ vezes diferenciáveis em um intervalo $[a, b]$. Se o Wronskiano destas funções é diferente de zero para algum $x \in [a, b]$, então as funções são linearmente independentes nesse intervalo.*

Demonstração. Suponha que $f_1, \ldots, f_n$ sejam LD. Então existem $a_1, \ldots, a_n$ tais que

$$a_1 f_1 + a_2 f_2 + \cdots + a_n f_n = 0.$$

Derivamos ambos os lados $n-1$ vezes, obtendo

$$\begin{aligned} a_1 f_1' + a_2 f_2' + \cdots + a_n f_n' &= 0 \\ a_1 f_1'' + a_2 f_2'' + \cdots + a_n f_n'' &= 0 \\ &\vdots \\ a_1 f_1^{(n-1)} + a_2 f_2^{(n-1)} + \cdots + a_n f_n^{(n-1)} &= 0. \end{aligned}$$

Ou seja, se as funções forem LI este sistema pode ter apenas a solução trivial com todos os $a_i = 0$. Isso é o mesmo que dizer que o determinante da matriz de coeficientes do sistema – o Wronskiano – é zero, *para todo* x. ■

Exemplo 5.60. No exemplo 5.58 verificamos que o Wronskiano de $f(x) = x^2$ e $g(x) = \cos(x)$ é

$$W(x) = \det \begin{pmatrix} x^2 & \cos(x) \\ 2x & -\operatorname{sen}(x) \end{pmatrix} = -x^2 \operatorname{sen}(x) - 2x\cos(x).$$

Escolhemos, por exemplo, $x = \pi$, e obtemos

$$\begin{aligned} W(\pi) &= -\pi^2 \operatorname{sen}(\pi) - 2\pi\cos(\pi) \\ &= -2\pi(-1) \\ &= 2\pi. \end{aligned}$$

Como $W(\pi) \neq 0$, então as funções não são LI em $\mathbb{R}$. ◄

Exemplo 5.61. Considere as funções $f(x) = 2x$, $g(x) = \ln(x)$ e $h(x) = x\ln(x)$. O Wronskiano destas funções é

$$\det \begin{pmatrix} 2x & x\ln(x) & \ln(x) \\ 2 & \ln(x)+1 & 1/x \\ 0 & 1/x & -1/x^2 \end{pmatrix},$$

que é igual a

$$-\frac{2\ln(x)}{x} - \frac{2}{x} + \frac{4\ln(x)}{x}$$

Multiplicamos a expressão por x e igualamos a zero, obtendo

$$\begin{aligned} -2\ln(x) - 2 + 4\ln(x) &= 0 \\ 2\ln(x) - 2 &= 0 \\ \ln(x) &= 1 \\ x &= e. \end{aligned}$$

Assim, o Wronskiano só é zero em $x = e$, e as funções são LI em qualquer intervalo de $\mathbb{R}$. ◄

Se as funções são LD, o Wronskiano *não pode* ser diferente de zero em nenhum ponto do intervalo.

Exemplo 5.62. As funções $f(x) = x^2$ e $g(x) = -3x^2$ são evidentemente LD (uma é múltipla da outra). Calculamos seu Wronskiano:

$$W(x) = \det \begin{pmatrix} x^2 & -3x^2 \\ 2x & -6x \end{pmatrix} = -6x^3 - 6x^3 = 0,$$

e como esperávamos, o Wronskiano é zero para todo $x \in \mathbb{R}$. ◀

Observe que somente provamos que se o Wronskiano é diferente de zero em algum ponto do intervalo, as funções são LI. A recíproca não é necessariamente verdadeira: quando o Wronskiano é zero em todo o intervalo, nada podemos afirmar sobre a dependência linear das funções. Este fato é ilustrado no exemplo 5.63.

Exemplo 5.63. As funções x e $|x|$ são linearmente independentes: presuma que existem constantes a e b tais que

$$ax + b|x| = 0.$$

Para $x = -1$, teríamos $-a = b$. Para $x = 1$, teríamos $a = b$. Assim, $b = a = -a$, o que só é possível com ambos iguais a zero.

No entanto, apesar das funções serem LI, seu Wronskiano é

$$\det \begin{pmatrix} x & |x| \\ 1 & \frac{x}{|x|} \end{pmatrix} = 0.$$ ◀

5.6.6 Interpolação

Quando temos dados experimentais a respeito de algum fenômeno, mas ainda não temos um modelo matemático para ele, podemos usar esses dados para construir *Interpolar* significa determinar uma função que passe por um conjunto de pontos dados.

Se tivermos valores $(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n)$, podemos determinar um polinômio de grau menor ou igual a n passando exatamente por esses pontos.

Definição 5.64 (Matriz de Vandermonde)**.** Uma *matriz de Vandermonde* é uma matriz quadrada cujas colunas ou linhas formam uma progressão geométrica. Construímos uma matriz de Vandermonde a partir de n escalares da seguinte forma: dados $k_0, k_1, \ldots, k_n$ diferentes entre si,

$$V(k_0, k_1, \ldots, k_n) = \begin{pmatrix} 1 & k_1 & k_1^2 & \cdots & k_1^{n-1} \\ 1 & k_2 & k_2^2 & \cdots & k_2^{n-1} \\ \vdots & & & & \\ 1 & k_n & k_n^2 & \cdots & k_n^{n-1} \end{pmatrix}$$ ♦

Exemplo 5.65. As matrizes a seguir são matrizes de Vandermonde:

$$A = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 2 & 4 \\ 1 & 10 & 100 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 4 & 8 \\ 1 & 5 & 25 & 125 \\ 1 & 3 & 9 & 27 \\ 1 & 7 & 49 & 343 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & a & a^2 & a^3 & a^4 \\ 1 & a^2 & a^4 & a^6 & a^8 \\ 1 & b & b^2 & b^3 & b^4 \\ 1 & b^3 & b^6 & b^9 & b^{12} \end{pmatrix},$$

onde, na matriz C, $a \neq b$.

A matriz A tem os escalares -1, 2 e 10 elevados às potências $0, 1, 2$ em cada linha. A matriz B tem $2, 5, 3, 7$ elevados às potências $0, 1, 2, 3$. A matriz C tem a, (a^2), b, (b^3) elevados às potências $0, 1, 2, 3$. ◀

O Teorema 5.66 nos dá uma maneira simples de calcular o determinante de matrizes de Vandermonde. Sua demonstração é pedida no exercício 165.

Teorema 5.66. *Seja A uma matriz de Vandermonde $V(k_0, \dots k_n)$, ou seja,*

$$A = V(k_0, k_1, \dots, k_n) = \begin{pmatrix} 1 & k_1 & k_1^2 & \cdots & k_1^{n-1} \\ 1 & k_2 & k_2^2 & \cdots & k_2^{n-1} \\ \vdots & & & & \\ 1 & k_n & k_n^2 & \cdots & k_n^{n-1} \end{pmatrix}$$

Então

$$\det(A) = \prod_{i<j} (k_j - k_i).$$

Exemplo 5.67. O determninante da matriz A do exemplo 5.65,

$$A = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 2 & 4 \\ 1 & 10 & 100 \end{pmatrix},$$

é facilmente obtido pela regra de Sarrus:

$$\begin{aligned} \det A &= +(1)(2)(100) \quad +(-1)(4)(1) \quad +(1)(1)(10) \\ &\quad -(1)(2)(1) \quad -(10)(4)(1) \quad -(100)(1)(-1) \\ &= 264. \end{aligned}$$

Mas sabemos que esta é uma matriz de Vandermonde, com

$$\begin{aligned} k_0 &= -1 \\ k_1 &= 2 \\ k_2 &= 10 \end{aligned}$$

Seu determinante, portanto, é

$$\begin{aligned} \det A &= (k_1 - k_0)(k_2 - k_0)(k_2 - k_1) \\ &= (2 - [-1])(10 - [-1])(10 - 2) \\ &= (3)(11)(8) \\ &= 264. \end{aligned}$$

Observe que ao aplicar a regra de Sarrus, fizemos 3 somas, 3 subtrações, e 12 multiplicações. Usando o teorema 5.66, fizemos somente 3 subtrações e duas multiplicações. Para matrizes de ordem maior, o uso deste teorema é ainda mais vantajoso. ◀

Usamos a relação entre determinante e a existência de solução para um sistema linear na demonstração do teorema 5.68.

Teorema 5.68. *Dados $n+1$ pontos, existe um único polinômio de grau menor ou igual a n que passa por todos eles.*

Demonstração. Para encontrar o polinômio interpolador

$$y(x) = a_0 + a_1 x + \cdots + a_n x^n$$

escrevemos, em notação matricial,

$$\begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^n \\ \vdots & & & & \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{pmatrix}$$

Temos então um sistema linear,

$$\begin{aligned} a_3 x_0^3 + a_2 x_0^2 + a_1 x_0 + a_0 &= y_0 \\ a_3 x_1^3 + a_2 x_1^2 + a_1 x_1 + a_1 &= y_1 \\ a_3 x_2^3 + a_2 x_2^2 + a_1 x_2 + a_2 &= y_2 \\ a_3 x_3^3 + a_2 x_3^2 + a_1 x_3 + a_3 &= y_3. \end{aligned}$$

Os pares (x_i, y_i) são dados (são os pontos que usamos para interpolar), e as incógnitas são os coeficientes a_i. Como os x_i são todos distintos, o determinante da matriz de coeficientes – que é uma matriz de Vandermonde – é sempre diferente de zero, porque $\det(A)$ é o produto de diferenças entre x_i, x_j distintos, e o sistema terá uma única solução não nula que descreve o polinômio interpolador. ■

Exemplo 5.69. Os pontos a seguir poderiam ter sido obtidos de algum experimento, e acreditamos poder descrever a relação entre as duas grandezas por um polinômio.

$$\begin{aligned} &(-5, -78) \\ &(-1, -14) \\ &(1, 6) \\ &(10, -3) \end{aligned}$$

Usando o que foi exposto anteriormente, temos

$$\begin{pmatrix} 1 & -5 & (-5)^2 & (-5)^3 \\ 1 & -1 & (-1)^2 & (-1)^3 \\ 1 & 1 & 1^2 & 1^3 \\ 1 & 10 & 10^2 & 10^3 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} -78 \\ -14 \\ 6 \\ -3 \end{pmatrix}.$$

A solução do sistema é $a_0 = -3$, $a_1 = 10$, $a_2 = -1$, e $a_3 = 0$. Como $a_3 = 0$, verificamos que um dos pontos era desnecessário – ou seja, uma parábola é suficiente para descrevê-los:

$$y = -x^2 + 10x - 3$$ ◀

Exercícios

Ex. 123 — Calcule os determinantes das matrizes a seguir.

$$\begin{pmatrix} -1 & 2 & 1 \\ x & 0 & x^2 \\ 3 & 0 & -1 \end{pmatrix} \quad \begin{pmatrix} 2 & 1 & 1 & -4 \\ 4 & 5 & 3 & -2 \\ 0 & 2 & -2 & 3 \\ 1 & -1 & 1 & -2 \end{pmatrix} \quad \begin{pmatrix} a & b & c & 1 \\ b & 0 & 0 & 2 \\ c & 0 & 0 & 3 \\ d & -2 & -3 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 3 & 2 & -3 \\ 2 & 1 & 3/2 & 5 \\ 0 & 3 & 3/2 & 4 \\ -1 & 1 & 0 & -7 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 3 & 7 & -1 & 0 \\ 22 & 12 & 3/2 & 15 & -2 \\ 51 & 6 & 14 & -2 & 0 \\ 10 & 3 & 3/2 & 34 & -2 \\ -91 & 16 & 0 & 0 & 0 \end{pmatrix}$$

Ex. 124 — Determine a tal que o volume do paralelepípedo gerado pelos vetores $(0, a, 2a)^T$, $(1, 0, 1)^T$ e $(4, 4, -2)^T$ em $\mathbb{R}^3$ seja 1.

Ex. 125 — Prove o Teorema 5.49

★ **Ex. 126 —** Verifique que a fórmula que demos para determinar uma circunferência passando por dois pontos é naturalmente generalizada para quatro pontos e esferas. Depois demonstre que vale a generalização para $n + 1$ pontos e hiperesferas em $\mathbb{R}^n$.

★ **Ex. 127 —** A fórmula para determinar a circunferência passando por tres pontos dá a equação daquela circunferência a partir de um determinante

$$\det\left(\cdots\right) = A(x^2 + y^2) + Bx + Cy + D = 0,$$

que depois pode ser transformada na forma usual,

$$(x - a)^2 + (y - b)^2 = r^2.$$

Prove que aquele determinante nunca resultará em uma equação de circunferência com raio negativo.

Ex. 128 — Prove o Teorema 5.16.

Ex. 129 — Revise a notação que usamos para matrizes elementares e calcule os determinantes das matrizes a seguir. Diga também de que ordem, *no mínimo*, devem ser as matrizes para que as expressões façam sentido. A, B, C são matrizes, e k é escalar.

i) $\det[E_{2L1}\mathcal{I}]$

ii) $\det[E_{2,3}E_{3,4}E_{3L2}A]$

iii) $\det[E_{1,2}E_{3,4}E_{2L1}AE_{2,3}B(5C)]$

iv) $\det[E_{2+3L4}A(3B)E_{1,2}C]$

v) $\det\left[E_{4L1}A(kB)E_{3,1}(4C^{-1})\right]$

vi) $\det\left[k^{-1}AE_{kL2}B\right]$

Ex. 130 — Resolva usando a regra de Cramer:

$$(a)\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1 + x_2 - x_3 = 1 \\ x_1 - x_2 + x_3 = -1 \end{cases} \quad (b)\begin{cases} x_1 + x_2 = 0 \\ x_2 - x_3 = 1 \\ 2x_1 3x_3 = 2 \end{cases} \quad (c)\begin{cases} -x_1 + x_3 + x_4 = 1 \\ x_1 + 3x_2 + x_3 + x_4 = 2 \\ x_2 + x_3 = 2 \\ 2x_1 - 3x_2 - 6x_4 = 1 \end{cases}$$

Ex. 131 — Seja A uma matriz quadrada com $\det A = d$, e $A' = P_1 P_2 \dots P_k A$, onde cada P_i é uma matriz que permuta duas linhas adjacentes. Relacione o determinante de A' com k.

Ex. 132 — Demonstre o Lema 5.8.

Ex. 133 — Demonstre o Teorema 5.12.

Ex. 134 — Considere a operação de *reversão de colunas* em matrizes quadradas: a matriz $(\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n)$ tem suas colunas listadas na ordem reversa, $(\mathbf{a}_n, \mathbf{a}_{n-1}, \dots, \mathbf{a}_1)$. Diga qual é o efeito desta operação no determinante de uma matriz, e apresente uma demonstração.

Ex. 135 — A operação de reversão de colunas, exposta no exercício 134, é linear?

Ex. 136 — Sejam A e B duas matrizes quadradas de ordem n, tais que A e B não tem entradas não-nulas em comum. Em que situação é possível termos $\det A = \det B$?

Ex. 137 — Prove o Teorema 5.25

Ex. 138 — Se sempre tomarmos o módulo do determinante de uma matriz, teremos uma função que dá o volume sem sinal – seria então diferente da função determinante que desenvolvemos neste Capítulo. Explique porque esta função não é uma função determinante, e não contradiz, portanto, a unicidade da função determinante.

Ex. 139 — Seja $T(x, y, z)^T = (2x, y, y - z)$. Prove que a matriz

$$\begin{pmatrix} 1 & 0 & 3 \\ 2 & 1 & 0 \\ -2 & 0 & -6 \end{pmatrix}$$

não pode representar T, *em nenhuma base de* $\mathbb{R}^3$.

Ex. 140 — O triângulo de Pascal pode ser definido da seguinte forma:

- Na primeira linha temos "1".
- Nas linhas seguintes, cada elemento é a soma do elemento acima dele com o que está acima e à esquerda.

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & & 1 & & \\ & 1 & & 2 & & 1 & \\ 1 & & 3 & & 3 & & 1 \\ & 1 & & 4 & & 6 & & 4 & & 1 \\ & & & \vdots & & & \end{array}$$

O triângulo de Pascal pode ser naturalmente disposto na forma de matriz. Podemos, pode exemplo, definir

as matrizes B_n, C_n e P_n.

$$B_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{pmatrix} \qquad C_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad P_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{pmatrix}$$

$$B_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 \\ 1 & 3 & 3 & 1 & 0 \\ 1 & 4 & 6 & 4 & 1 \end{pmatrix} \quad C_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 3 & 6 \\ 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad P_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 6 & 10 & 15 \\ 1 & 4 & 10 & 20 & 35 \\ 1 & 5 & 15 & 35 & 70 \end{pmatrix}$$

a) Prove que $\det P_n = 1$.

b) Prove que se a matriz K tem todas as entradas iguais a um valor k, $\det(P_n + K) = 1 + k$.

c) Mostre que as matrizes P_n são parte de uma família de matrizes tais que $\det(A+K)$ pode ser calculado com apenas três operações aritméticas, desde que se conheça $\det A$.

Ex. 141 — Na definição informal de orientação em $\mathbb{R}^3$, alinhamos o último vetor da base com $\mathbf{e}_3$. Mostre que se tivéssemos alinhado com qualquer vetor não-nulo, as bases com orientação concordante seriam as mesmas.

Ex. 142 — Seja A uma matriz 3×3 com coeficientes em $\mathbb{Q}$. Mostre que se d é um inteiro positivo tal que $d|a_{11}a_{12}a_{13}$, $d|a_{21}a_{22}a_{23}$, $d|a_{31}a_{32}a_{33}$, então $d|\det(A)$.

Ex. 143 — Demonstre o teorema de Sylvester: se A é $n \times k$, e B é $k \times n$, então

$$\det(\mathcal{I}_n + AB) = \det(\mathcal{I}_k + BA).$$

Ex. 144 — O *permanente* de uma matriz é uma função semelhante ao determinante, com uma diferença: na fórmula de Leibniz, retiramos a multiplicação por $\operatorname{sgn}(\sigma)$. Que propriedades de determinante o permanente também tem? E para que matrizes reais o permanente é igual ao determinante? (Tente caracterizar as matrizes sem usar permutações.)

★ **Ex. 145 —** O permanente de uma matriz sempre será igual ao determinante quando as entradas pertencerem a um certo corpo. Qual?

Ex. 146 — Quais matrizes anti-simétricas são singulares?

Ex. 147 — Considere o conjunto das matrizes diagonais de ordem n. Defina a operação $\otimes$ como

$$A \otimes B = \det(AB)\mathcal{I}$$

O conjunto das matrizes diagonais de ordem n com as operações de soma de matrizes e $\otimes$ é um corpo? Se não for, há como impor restrições adicionais sobre as matrizes para que obtenhamos um corpo?

Ex. 148 — Determine a para que os triângulos $\triangle_1$ e $\triangle_2$, cujos vértices são dados a seguir, tenham a mesma área.

$$\triangle_1 : (3,1)^T, (0,a)^T, (2,5)^T$$
$$\triangle_2 : (1,a)^T, (-1,-4)^T, (0,0)^T$$

Ex. 149 — Considere as três funções $f(x) = x$, $g(x) = e^x$ e $h(x) = e^{-x}$ em C^0. Responda:

•Estas funções são LI ou LD em $\mathbb{R}$?

•E em algum intervalo qualquer $[a, b] \subseteq \mathbb{R}$?

Ex. 150 — Em que intervalo as funções são LI?

i) $\cos(e^x)$ e $\operatorname{sen}(e^x)$.

ii) $f(x) = 1$, $g(x) = x$, e $h(x) = e^x$.

iii) x^x e e^x.

Ex. 151 — As funções $f(x) = \operatorname{sen}^2(x)$, $g(x) = \cos^2(x)$ e $h(x) = 2$ são LD (prove!). Verifique que seu Wronskiano é zero.

Ex. 152 — Para pontos $(x_0, y_0), \ldots, (x_n, y_n)$, sempre é possível encontrar um polinômio interpolador de grau menor ou igual a n. Determine uma fórmula para os coeficientes deste polinômio (para que não seja necessário resolver o sistema linear exposto na seção 5.6.6).

★ **Ex. 153 —** Calcule o determinante da seguinte matriz, cujas entradas pertencem a $\mathbb{Z}_2$. Reveja as operações usadas no exemplo 1.22 (página 8). Lembre-se de que cada elemento é seu própio inverso aditivo, portanto $a + b = a - b$, que denotamos simplesmente por $a \oplus b$.

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Ex. 154 — Prove que se uma matriz tem todas as entradas pertencentes a um corpo, seu determinante será necessariamente um elemento do mesmo corpo.

Ex. 155 — Seja A uma matriz com entradas inteiras. Determine em que situação A pode ter inversa também com entradas inteiras (lembre-se que os inteiros não são um corpo e por isso, de maneira geral, A pode ter inversa com entradas não inteiras: tome por exemplo $\left(\begin{smallmatrix} +1 & -1 \\ +1 & +1 \end{smallmatrix}\right)$, cuja inversa é $\left(\begin{smallmatrix} +1/2 & +1/2 \\ -1/2 & +1/2 \end{smallmatrix}\right)$).

★ **Ex. 156 —** Resolva o sistema em $\mathbb{Z}_2$, usando a regra de Cramer:

$$\begin{cases} x_1 \oplus x_2 \oplus x_3 = 0 \\ x_1 \oplus x_2 = 1 \\ x_2 \oplus x_3 = 1 \end{cases}$$

Ex. 157 — No exercício 56, mostramos como representar números complexos como matrizes de ordem 2. Se $f(a + bi) = A$, quem é $\det A$?

Ex. 158 — Para que uma matriz seja totalmente unimodular, que valores ela pode ter em suas entradas?

Ex. 159 — No teorema 5.44, mostramos que se A é quadrada e totalmente unimodular, e $\mathbf{b}$ é integral, a solução para $A\mathbf{x} = \mathbf{b}$ é integral. Sabemos que se A não for quadrada, com mais colunas do que linhas, o sistema tem infinitas soluções. Reescreva o teorema para este caso. Todas as soluções serão inteiras? Parcialmente inteiras?

★ **Ex. 160 —** Há espaços vetoriais de dimensão finita onde todas as bases tem a mesma orientação. Quais são estes espaços?

Ex. 161 — Transformações lineares preservam volume?

Ex. 162 — Definimos a seguinte família de matrizes:

$$A_1 = (1)$$
$$A_2 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$
$$A_3 = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & -1 \\ 0 & 1 & 1 \end{pmatrix}$$
$$A_4 = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$
$$\vdots$$
$$A_n = \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & -1 & 0 & 0 & & 0 & 0 \\ 0 & 1 & 1 & -1 & 0 & & 0 & 0 \\ 0 & 0 & 1 & 1 & -1 & & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & & 0 & 0 \\ \vdots & & & & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 1 \end{pmatrix}$$

Ou seja, A_n tem uns na diagonal principal e imediatamente abaixo dela; e tem -1 imediatamente acima da diagonal.
Seja (a_n) a sequência definida pelos determinantes destas matrizes. Determine a forma fechada para a_n.

★ **Ex. 163 —** Prove o Teorema 5.37.

★ **Ex. 164 —** Diga se as estruturas a seguir são grupos, quando usada a operação de multiplicação de matrizes:

i) As matrizes A de ordem n com $\det A = 0$;
ii) As matrizes A de ordem n com $\det A = 1$;
iii) As matrizes A de ordem n;
iv) As matrizes A de ordem n com determinante ímpar;
v) As matrizes A de ordem n com determinante par;
vi) As matrizes A de ordem n não-singulares.

Ex. 165 — Prove o Teorema 5.66.

Ex. 166 — Os seguintes pontos foram obtidos em um experimento:

$$(-3, -8)$$

$$(1, 20)$$
$$(13, -65)$$
$$(20, 9)$$

Presumimos que estes pontos são descritos por um polinômio. Determine, portanto, um polinômio que passe por todos eles.

Capítulo 6

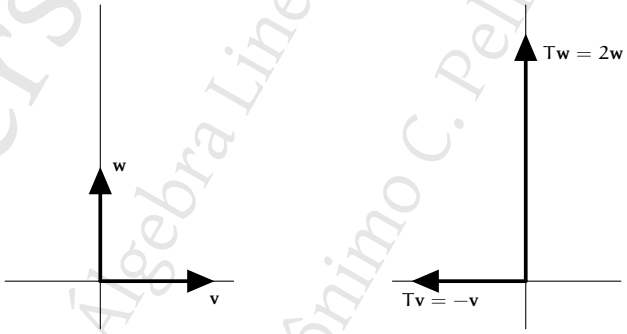
Autovalores, Autovetores e Diagonalização

Se a matriz de um operador linear T não é diagonal, muitas vezes podemos encontrar uma base diferente da canônica em que a matriz de T é diagonal. Isso traz diversas vantagens, como veremos mais adiante. O processo de determinar as matrizes de mudança de base a fim de obter uma representação diagonal de um operador é chamado de *diagonalização* – este é o tema deste Capítulo.

Considere o operador linear

$$T = \begin{pmatrix} -1 & 0 \\ 0 & 2 \end{pmatrix}.$$

Temos portanto $T(x, y)^T$ resultando no vetor $(-x, 2y)^T$. Há dois conjuntos de vetores interessantes relacionados a este operador: os que ficam na reta $x = 0$ e os que ficam na reta $y = 0$.



O operador T leva estes vetores em seus múltiplos. De maneira geral, um operador linear não leva qualquer vetor em um múltiplo seu. Quando isto acontece, dizemos que este é um *autovetor* do operador.

Os vetores da forma $(x, 0)^T$, como $\mathbf{v}$ na figura, são *autovetores* da transformação, e dizemos que eles *pertencem ao autovalor* -1, porque $T(x, 0)^T$ é igual a $-1(x, 0)^T$. Já os vetores da forma $(0, y)^T$, como o vetor

w na figura, são também autovetores da transformação, mas *pertencem* ao autovalor 2, porque $T(0,y)^T = 2(0,y)^T$.

Definição 6.1 (Autovetor e autovalor)**.** Seja A um operador linear em um espaço vetorial V sobre um corpo F. Um vetor $\mathbf{v} \neq \mathbf{0}$ é um *autovetor* de A se e somente se existe um escalar $\lambda \in F$ tal que $A\mathbf{v} = \lambda\mathbf{v}$. O escalar λ é um *autovalor* de A, associado ao autovetor $\mathbf{v}$.

O conjunto dos autovalores de um operador é o seu *espectro*. ♦

Exemplo 6.2. O operador

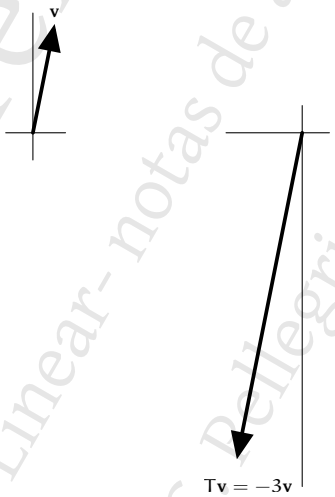
$$\begin{pmatrix} 2 & -1 \\ 0 & -3 \end{pmatrix}$$

tem autovalores -3 e 2.

Os vetores da forma $(a, 5a)^T$ são os autovetores pertencentes ao autovalor -3.

$$\begin{pmatrix} 2 & -1 \\ 0 & -3 \end{pmatrix} \begin{pmatrix} a \\ 5a \end{pmatrix} = \begin{pmatrix} 2a - 5a \\ 0 - 3(5a) \end{pmatrix} = \begin{pmatrix} -3a \\ -15a \end{pmatrix} = -3 \begin{pmatrix} a \\ 5a \end{pmatrix}.$$

A figura a seguir ilustra geometricamente a atuação de T sobre estes vetores.



Os vetores da forma $(b, 0)^T$ são os autovetores pertencentes ao autovalor 2.

$$\begin{pmatrix} 2 & -1 \\ 0 & -3 \end{pmatrix} \begin{pmatrix} b \\ 0 \end{pmatrix} = 2 \begin{pmatrix} b \\ 0 \end{pmatrix}.$$

A figura a seguir ilustra geometricamente a atuação de T sobre estes vetores.

A mesma interpretação geométrica fará sentido em $\mathbb{R}^3$, e de maneira geral, em $\mathbb{R}^n$. ◀

Da mesma forma que definimos posto e nulidade similarmente para transformações e matrizes, também o fazemos para autovalores e autovetores: os autovalores e autovetores de uma matriz são os mesmos da transformação que ela representa.

Exemplo 6.3. O operador

$$\begin{pmatrix} 4 & 0 \\ 0 & -1 \end{pmatrix}$$

tem autovalores -1 e 4. O autovetor $(0,1)^T$ é associado ao autovalor -1 e o autovetor $(1,0)^T$ associado ao autovalor 4, porque

$$\begin{pmatrix} 4 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix}, \quad \begin{pmatrix} 4 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 0 \end{pmatrix}.$$

Estes não são, no entanto, os únicos autovetores deste operador. É simples verificar que múltiplos de autovetores também serão autovetores. ◀

Exemplo 6.4. O operador

$$A = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}$$

tem somente o autovalor 1. Os autovetores associados a este autovalor são todos os vetores da forma $(x,-x)^T$:

$$A(x,-x)^T = (x,-x)^T.$$ ◀

Exemplo 6.5. O operador

$$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

não tem autovalores reais (mas tem autovalores complexos – veremos adiante que, apesar de um operador em $\mathbb{R}^n$ nem sempre ter autovalores reais, sempre terá autovalores complexos). ◀

Exemplo 6.6. Seja C^∞ o espaço das funções contínuas e infinitas vezes diferenciáveis. A derivada segunda, d^2/dx^2, é um operador linear neste espaço. Um autovetor deste operador é a função seno, já que

$$\frac{d^2}{dx^2}\operatorname{sen}(x) = -\operatorname{sen}(x),$$

e o autovalor associado a este autovetor é -1. ◀

Exemplo 6.7. No espaço C^∞, das funções reais contínuas e infinitas vezes diferenciáveis, a função $f(x) = e^x$ é um autovetor da transformação definida pela derivação, porque

$$\frac{d}{dx}e^x = e^x.$$

O autovalor de e^x neste espaço é 1.

Já a função $g(x) = e^{2x}$ é autovetor da operação de derivação, com autovalor 2, porque

$$\frac{d}{dx}e^{2x} = 2(e^{2x}).$$

A operação de derivação tem infinitos autovalores e autovetores: para todo $k \in \mathbb{R}$, k é autovalor do autovetor e^{kx}.

Como a solução geral da EDO $y' - ky = 0$ é $y = ce^{kx}$, então dado um $k \in \mathbb{R}$, para todo $c \in \mathbb{R}$,

$$y = ce^{kx}$$

é autovetor associado ao autovalor k. ◀

Exemplo 6.8. No espaço $\mathbb{R}_2[x]$, considere o operador

$$T(a_0 + a_1x + a_2x^2) = 2a_0 + 3a_1x + 2a_2x^2.$$

Este operador tem dois autovalores, 2 e 3.

- Os autovetores do autovalor 2 são os polinômios da forma $a_0 + a_2x^2$, porque T levará cada um deles ao seu dobro,
$$T(a_0 + a_2x^2) = 2a_0 + 2a_2x^2 = 2(a_0 + a_2x^2).$$
- Os autovetores do autovalor 3 são os polinômios da forma a_1x, porque T levará cada um deles ao seu triplo:
$$T(a_1x) = 3(a_1x).$$ ◀

★ **Exemplo 6.9.** Em $\mathbb{Z}_2$ temos apenas dois escalares, 0 e 1. Assim, o único autovalor que um operador pode ter é 1. Por exemplo, o operador

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

tem autovalor 1, com autovetor

$$[v] = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Verificamos:

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$ ◀

Lema 6.10. *Seja A um operador com autovetores $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ e autovalores $\lambda_1, \lambda_2, \ldots, \lambda_k$. Se os autovalores λ_i são distintos, então os autovetores são linearmente independentes.*

Definição 6.11 (subespaço próprio)**.** Sejam V um espaço vetorial, T um operador linear em V e λ um autovalor de T. Então os autovetores relacionados a λ formam um subespaço, chamado de *espaço próprio* (ou *autoespaço*) de V. ⧫

O Exercício 167 pede a demonstração de que o espaço próprio é realmente subespaço de V.

A quantidade de autovetores linearmente independentes tendo λ como autovalor associado é sua *multiplicidade geométrica*, que também podemos definir da seguinte maneira.

Definição 6.12 (multiplicidade geométrica de autovalor)**.** A *multiplicidade geométrica* de um autovalor λ é a dimensão de seu espaço próprio. ⧫

Exemplo 6.13. Considere a matriz

$$\begin{pmatrix} 1 & -2 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Esta matriz tem autovalores 3 e -1.

O autovalor 3 tem como autovetores associados os vetores da forma

$$\begin{pmatrix} a \\ -a \\ b \end{pmatrix},$$

que são combinações lineares de vetores

$$\begin{pmatrix} a \\ -a \\ 0 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 0 \\ 0 \\ b \end{pmatrix}$$

Já o autovalor -1 tem autovetores da forma,

$$\begin{pmatrix} c \\ c \\ 0 \end{pmatrix}$$

O espaço próprio do autovalor 3 é gerado por dois vetores, $(1,-1,0)^T$ e $(0,0,1)^T$, portanto sua dimensão é dois.

O espaço próprio do autovalor -1 é gerado por um vetor, $(1,1,0)^T$, portanto sua dimensão é um.

Ou, equivalentemente, a multiplicidade geométrica do autovalor 3 é dois. A multiplicidade geométrica do autovalor -1 é um. ◀

Exemplo 6.14. Como já exposto no exemplo 6.8, em $\mathbb{R}_2[x]$, o operador dado por

$$T(a_0 + a_1 x + a_2 x^2) = 2a_0 + 3a_1 x + 2a_2 x^2.$$

tem autovalores 2 e 3.

- Os autovetores do autovalor 2 são os polinômios da forma $a_0 + a_2 x^2$. Estes polinômios formam um subespaço de dimensão dois, porque são gerados pelos dois polinômios

$$(1, x^2).$$

- Os autovetores do autovalor 3 são os polinômios da forma $a_1 x$. Estes polinômios formam um subespaço de dimensão um, porque são gerados pelo polinômio x. ◀

Teorema 6.15. *Seja A com autovetor $\mathbf{v}$ e autovalor associado λ. Então $\mathbf{v}$ e λ^{-1} são autovetor e autovalor de A^{-1}.*

Demonstração. Se $A\mathbf{v} = \lambda\mathbf{v}$, então

$$\begin{aligned} A\mathbf{v} &= \lambda\mathbf{v} \\ \mathbf{v} &= A^{-1}(\lambda\mathbf{v}) && \text{(multiplique por } A^{-1}) \\ \mathbf{v} &= \lambda A^{-1}\mathbf{v} \\ \lambda^{-1}\mathbf{v} &= A^{-1}\mathbf{v}, && \text{(multiplique por } \lambda^{-1}) \end{aligned}$$

portanto $\mathbf{v}$ é autovetor de A^{-1} com autovalor λ^{-1}. ■

Corolário 6.16. *Se 0 é autovalor de A, então A é singular.*

Exemplo 6.17. Seja

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

tem autovalores $\lambda_1 = 1$ e $\lambda_2 = 3$.

- Os autovetores de $\lambda_1 = 1$ são da forma $(x, x)^T$:

$$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} x \\ x \end{pmatrix} = 1 \begin{pmatrix} x \\ x \end{pmatrix}$$

- Os autovetores de $\lambda_1 = 3$ são da forma $(x, -x)^T$:

$$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} x \\ -x \end{pmatrix} = 3 \begin{pmatrix} x \\ -x \end{pmatrix}$$

A inversa de A é

$$A^{-1} = \frac{1}{3} \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix},$$

com autovalores $\eta_1 = 1$ e $\eta_2 = 1/3$:

- Os autovetores de $\eta_1 = 1$ são da forma $(x, x)^T$:

$$\frac{1}{3} \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ x \end{pmatrix} = 1 \begin{pmatrix} x \\ x \end{pmatrix}$$

- Os autovetores de $\eta_1 = 1/3$ são da forma $(x, -x)^T$:

$$\frac{1}{3} \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ -x \end{pmatrix} = \frac{1}{3} \begin{pmatrix} x \\ -x \end{pmatrix}$$ ◀

Exemplo 6.18. A matriz singular

$$A = \begin{pmatrix} 1 & 3 \\ -2 & -6 \end{pmatrix}$$

tem autovalores $\lambda_1 = 0$ e $\lambda_2 = -5$.

- Os autovetores de $\lambda_1 = 0$ são da forma $(x, -2x)^T$:

$$\begin{pmatrix} 1 & 3 \\ -2 & -6 \end{pmatrix} \begin{pmatrix} x \\ -2x \end{pmatrix} = 0 \begin{pmatrix} x \\ -2x \end{pmatrix} = \mathbf{0}.$$

- Os autovetores de $\lambda_1 = -5$ são da forma $(x, -x/3)^T$:

$$\begin{pmatrix} 1 & 3 \\ -2 & -6 \end{pmatrix} \begin{pmatrix} x \\ -x/3 \end{pmatrix} = -5 \begin{pmatrix} x \\ -x/3 \end{pmatrix}.$$ ◀

Proposição 6.19. *Se A não é singular, os autovalores de A e A^T são os mesmos.*

O traço da matriz de um operador linear é a soma de seus autovalores. Já o determinante da matriz é o produto dos autovalores.

6.1 Polinômio característico

O polinômio característico de uma matriz nos permite determinar seus autovalores, e consequentemente seus autovetores – e é uma importante aplicação de determinantes.

Se $\mathbf{x}$ e λ são um par de autovetor e autovalor de uma transformação A, então por definição

$$A\mathbf{x} = \lambda\mathbf{x}.$$

Queremos encontrar valores para λ e $\mathbf{x}$, com $\mathbf{x} \neq \mathbf{0}$.

Podemos reescrever esta equação, já que $\lambda x = \lambda\mathcal{I}x$.

$$A\mathbf{x} = \lambda\mathcal{I}\mathbf{x}.$$

Temos então

$$\begin{aligned} \lambda\mathcal{I}\mathbf{x} - A\mathbf{x} &= \mathbf{0} \\ (\lambda\mathcal{I} - A)\mathbf{x} &= \mathbf{0}. \end{aligned}$$

Se $(\lambda\mathcal{I} - A)$ não for singular (ou seja, se seu determinante for diferente de zero), o sistema acima terá *somente* uma solução, com $\mathbf{x} = \mathbf{0}$, porque

$$\begin{aligned} (\lambda\mathcal{I} - A)\mathbf{x} &= \mathbf{0} \\ \mathbf{x} &= (\lambda\mathcal{I} - A)^{-1}\mathbf{0} && (\lambda\mathcal{I} - A \text{ não singular} \rightarrow \text{sua inversa existe}) \\ \mathbf{x} &= \mathbf{0}. \end{aligned}$$

Como queremos as outras soluções, com $\mathbf{x} \neq \mathbf{0}$, estamos procurando valores de λ para os quais a matriz $(\lambda\mathcal{I} - A)$ é singular

$$\det(\lambda\mathcal{I} - A) = 0.$$

Esta equação é chamada de *equação característica*. e seu lado esquerdo é chamado de *polinômio característico*.

Definição 6.20 (Polinômio característico)**.** Seja A um operador em $\mathbb{R}^n$ (ou uma matriz quadrada de ordem n), com elementos de um corpo F. O *polinômio característico* de A é

$$\det(x\mathcal{I} - A). \qquad \blacklozenge$$

As raízes do polinômio característico de uma matriz A são os autovalores da transformação representada por A.

Note que poderíamos ter definido o polinômio característico como $(A - \lambda\mathcal{I})$ ao invés de $(\lambda\mathcal{I} - A)$. Chegaríamos ao mesmo polinômio característico, com sinal trocado. As raízes, no entanto, seriam as mesmas.

Exemplo 6.21. O polinômio característico do operador

$$A = \begin{pmatrix} 2 & 0 & 2 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

é $\det(x\mathcal{I} - A)$, ou

$$\det\left[\begin{pmatrix} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{pmatrix} - \begin{pmatrix} 2 & 0 & 2 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}\right]$$

$$= \det \begin{pmatrix} x-2 & 0 & -2 \\ 0 & x & -1 \\ -1 & 0 & x \end{pmatrix} = x^3 - 2x^2 - 2x.$$

As raízes deste polinômio são 0, $\sqrt{3}+1$ e $1-\sqrt{3}$. Estes são também os autovalores da transformação representada pela matriz A. ◀

No último exemplo, o polinômio característico da matriz de ordem 3 era mônico (o coeficiente de x^3 era 1) e de ordem 3. Na verdade, isto sempre acontece, conforme o Lema 6.22, cuja demonstração é o objeto do Exercício 174.

Lema 6.22. *O polinômio característico para uma matriz quadrada de ordem n sempre será mônico e de grau n.*

No entanto, o polinômio característico de uma matriz de ordem n não necessariamente terá $n+1$ termos.

Exemplo 6.23. O polinômio característico da matriz

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

é $x^2 - x - 1$, com três termos. Já o polinômio característico de

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

é $x^2 - 2x$ – tem apenas dois termos. ◀

O traço e o determinante de uma matriz podem ser obtidos diretamente de seu polinômio caracetrístico, como determina o Teorema 6.24, cuja demonstração é pedida no Exercício 170.

Teorema 6.24. *Seja*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

o polinômio característico de uma matriz M. Então

$$a_{n-1} = -(-1)^n \operatorname{Tr} M$$
$$a_0 = \det M$$

Corolário 6.25. *Uma matriz é singular se e somente se o seu polinômio característico não tem termo independente.*

Exemplo 6.26. O polinômio característico da matriz

$$\begin{pmatrix} 2 & 3 \\ 4 & 6 \end{pmatrix}$$

é $x^2 - 8x$. Como a matriz é simgular (a segunda linha é obviamente múltiplo da primeira), o determinante (o termo independente do polinômio característico) da matriz é zero. ◀

Exemplo 6.27. O polinômio característico da matriz

$$A = \begin{pmatrix} 3 & 2 \\ 1 & 0 \end{pmatrix}$$

é $x^2 - 3x - 2$, e percebemos claramente também que $\operatorname{Tr} A = 3$ e $\det A = -2$.

Já o polinômio característico da matriz

$$B = \begin{pmatrix} -1 & 2 & 3 \\ -2 & 2 & 0 \\ -3 & 5 & 1 \end{pmatrix}$$

é $-x^3 - 10x - 14$. O determinande de B é 14, e seu traço é zero.

Como último exemplo, considere a matriz identidade de ordem n. Seu polinômio característico é

$$\begin{aligned} \det \begin{pmatrix} 1-x & 0 & \dots & 0 \\ 0 & 1-x & & \\ \vdots & & \ddots & \\ 0 & & & 1-x \end{pmatrix} &= (1-x)^n \\ &= (-1)^n x^n - (-1^n) n x^{n-1} + \ldots - a_1 x + 1, \end{aligned}$$

e temos portanto o traço n e o determinante 1 nos coeficientes do polinômio característico. Concretamente, o polinômio característico de $\mathcal{I}_4$ é

$$(1-x)^4 = x^4 - 4x^3 + 6x^2 - 4x + 1,$$

com $\operatorname{Tr} \mathcal{I}_4 = -(-1)^4(-4) = -(-4) = 4$, e o de $\mathcal{I}_5$ é

$$(1-x)^5 = -x^5 + 5x^4 - 10x^3 + 19x^2 - 5x + 1,$$

com $\operatorname{Tr} \mathcal{I}_5 = -(-1^5)5 = -(-1)5 = 5$. ◀

Definição 6.28 (Multiplicidade algébrica de autovalor)**.** A *multiplicidade algébrica* do autovalor λ é sua multiplicidade enquanto raiz do polinômio característico de A. ♦

Exemplo 6.29. O polinômio característico do operador

$$A = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}$$

é

$$x^2 - 6x + 9 = (x-3)^2,$$

que tem duas raízes idênticas (a parábola toca o eixo horizontal exatamente uma vez), iguais a 3. A multiplicidade algébrica do autovalor 3 é, portanto, dois. ◀

Método 6.30 (Determinação de autovalores e autovetores)**.** Para determinar os autovalores e autovetores de uma matriz A, primeiro obtenha o polinômio caractetrístico de A. As raízes deste polinômio são os autovalores de A.

Depois, resolva $A\mathbf{v} = \lambda\mathbf{v}$, para todos os autovalores λ, obtendo assim os autovetores de A. ●

Exemplo 6.31. Já calculamos no exemplo 6.29 o polinômio característico da matriz $\left(\begin{smallmatrix} 3 & 1 \\ 0 & 3 \end{smallmatrix}\right)$, que é igual a $(x-3)^2$, tendo duas raízes iguais a 3.

Para determinar os autovetores da matriz, resolvemos

$$A\mathbf{x} = 3\mathbf{x}$$
$$\begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3x_1 \\ 3x_2 \end{pmatrix}$$

O sistema que queremos resolver é

$$\begin{cases} 3x_1 + x_2 = 3x_1 \\ 3x_2 = 3x_2 \end{cases},$$

que é indeterminado e tem como soluções $x_2 = 0$, e qualquer valor para x_1. Assim, os autovetores são da forma

$$\begin{pmatrix} k \\ 0 \end{pmatrix}.$$

Como os autovetores são todos desta forma, o espaço próprio do autovalor 3 é gerado pela base

$$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}.$$ ◀

Exemplo 6.32. determinaremos os autovalores e autovetores de

$$A = \begin{pmatrix} 2 & -1 & 1 \\ 0 & 3 & 1 \\ -1 & 0 & 0 \end{pmatrix}.$$

O polinômio característoco de A é

$$\begin{aligned} \det(A - \lambda\mathcal{I}) &= \det\begin{pmatrix} 2-\lambda & -1 & 1 \\ 0 & 3-\lambda & 1 \\ -1 & 0 & -\lambda \end{pmatrix} \\ &= -x^3 + 5x^2 - 7x + 3 \\ &= -(x-3)(x-1)(x-1). \end{aligned}$$

As raízes deste polinômio – e os autovalores de A – são portanto $\lambda_1 = 1$ e $\lambda_2 = 3$. Encontramos os autovetores:

- Para $\lambda_1 = 1$,

$$A\mathbf{v} = \lambda_1\mathbf{v}$$
$$\begin{pmatrix} 2 & -1 & 1 \\ 0 & 3 & 1 \\ -1 & 0 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}.$$

Disto obtemos o sistema

$$\begin{aligned} 2a - b + c &= a, \\ 3b &= b, \end{aligned}$$

$$-a = c,$$

e temos portanto os autovetores da forma

$$\begin{pmatrix} a \\ 0 \\ -a \end{pmatrix}$$

- Para $\lambda_1 = 3$,

$$A\mathbf{v} = \lambda_1 \mathbf{v}$$
$$\begin{pmatrix} 2 & -1 & 1 \\ 0 & 3 & 1 \\ -1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = 3 \begin{pmatrix} a \\ b \\ c \end{pmatrix}.$$

Disto obtemos o sistema

$$\begin{aligned} 2a - b + c &= 3a, \\ 3b &= 3b, \\ -a &= 3c, \end{aligned}$$

e temos portanto os autovetores da forma

$$\begin{pmatrix} a \\ -4a/3 \\ -a/3 \end{pmatrix}. \quad \blacktriangleleft$$

★ **Exemplo 6.33.** Oberemos agora os autovalores e autovetores, *em* $\mathbb{Z}_2$, da matriz

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

O polinômio característico é

$$\det(A - \lambda \mathcal{I}) = \begin{pmatrix} 1-\lambda & 1 & 0 \\ 1 & -\lambda & 1 \\ 0 & 1 & 1-\lambda \end{pmatrix} = -(\lambda)(\lambda \oplus 1)(\lambda \oplus 1),$$

com raízes 0 e 1. Agora resolvemos, para $\lambda_1 = 0$,

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

ou seja,

$$\begin{aligned} a \oplus b &= 0 \\ a \oplus c &= 0 \\ b \oplus c &= 0 \end{aligned}$$

Chegamos a $a = b = c$, e os autovetores de λ_1 são da forma[1]

$$\begin{pmatrix} a \\ a \\ a \end{pmatrix}$$

Para $\lambda_2 = 1$, temos

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \end{pmatrix},$$

ou seja,

$$\begin{aligned} a \oplus b &= a \\ a \oplus c &= b \\ b \oplus c &= c \end{aligned}$$

e obtemos $b = 0$, e $a = c$, e os autovetores de λ_2 são da forma[2]

$$\begin{pmatrix} a \\ 0 \\ a \end{pmatrix}. \qquad \blacktriangleleft$$

Teorema 6.34. *Se duas matrizes quadradas de ordem n com elementos de um mesmo corpo são similares, então elas tem o mesmo polinômio característico.*

Demonstração. Se A e B são similares, então existe P tal que $B = P^{-1}AP$. Então

$$\begin{aligned} \det(x\mathcal{I} - B) &= \det(x\mathcal{I} - P^{-1}AP) \\ &= \det(x[P^{-1}\mathcal{I}]P - P^{-1}AP) \qquad (\star) \\ &= \det(P^{-1}x\mathcal{I}P - P^{-1}AP) \\ &= \det(P^{-1}(x\mathcal{I} - A)P) \\ &= \det(P^{-1})\det(x\mathcal{I} - A)\det(P) \\ &= \det(P)^{-1}\det(x\mathcal{I} - A)\det(P) \\ &= \det(x\mathcal{I} - A). \end{aligned}$$

Na passagem $(\star)$, observe que $P^{-1}\mathcal{I} = P^{-1}$, logo $(P^{-1}\mathcal{I})P = P^{-1}P = \mathcal{I}$. ■

A recíproca deste Teorema não é verdadeira (veja o Exercício 169).

Teorema 6.35. *Os valores na diagonal de uma matriz triangular são seus autovalores.*

Demonstração. Basta resolvermos $\det(\lambda\mathcal{I} - A) = 0$ para uma matriz triangular A.

$$\det \begin{pmatrix} \lambda - a_{11} & \bullet & \bullet & \bullet & \bullet \\ & \lambda - a_{22} & \bullet & \cdots & \bullet \\ & & \ddots & & \vdots \\ & & & \ddots & \bullet \\ & & & & \lambda - a_{nn} \end{pmatrix}$$

[1] Como $\mathbb{Z}_2$ é finito, o autoespaço de λ_1 só contém dois vetores, porque só há dois desta forma: $(0,0,0)^T$ e $(1,1,1)^T$. Um deles equivale a $a = 0$ e outro equivale a $a = 1$.

[2] Novamente, porque $\mathbb{Z}_2$ é finito, só há dois autovetores para λ_2: $(0,0,0)^T$ e $(1,0,1)^T$. Um para $a = 0$ e um para $a = 1$.

$$=(\lambda - a_{11})(\lambda - a_{22}) \cdots (\lambda - a_{nn}) = 0,$$

e portanto $\det(\lambda \mathcal{I} - A)$ será zero se e somente se λ for igual a um dos a_{ii} – ou seja, os elementos da diagonal são os autovalores da matriz. ■

Teorema 6.36 (de Cayley-Hamilton)**.** *Seja A uma matriz e p seu polinômio característico. Então $p(A) = 0$.*

Exemplo 6.37. Seja

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

O polinômio característico de A é

$$p(x) = x^2 - 4x + 5.$$

Calculamos então

$$\begin{aligned} p(A) &= A^2 - 4A + 5\mathcal{I} \\ &= \begin{pmatrix} -1 & 8 \\ -4 & 7 \end{pmatrix} + \begin{pmatrix} -4 & -8 \\ 4 & -12 \end{pmatrix} + \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

◀

O Teorema de Gershgorin nos dá um intervalo para os autovalores de uma matriz, sem a necessidade de calculá-los.

Teorema 6.38 (de Gershgorin, para autovalores reais)**.** *Seja A uma matriz quadrada de ordem n com entradas e autovalores reais. Seja*

$$r_i = \sum_{j \neq i} |a_{ij}|.$$

Então todos os autovalores de A pertencem ao intervalo

$$\bigcup \Big[a_{ii} - r_i, a_{ii} + r_i \Big].$$

Demonstração. Seja $\mathbf{v}$ um autovetor de A com autovalor λ – ou seja, $A\mathbf{v} = \lambda \mathbf{v}$. Se abrirmos a expressão $A\mathbf{v}$, temos

$$\sum_j a_{ij} v_j = \lambda v_i, \quad \forall i.$$

Ao retirarmos a_{ii} do somatório, obtemos

$$\begin{aligned} \sum_{j \neq i} a_{ij} v_j &= \lambda v_i - a_{ii} v_i, \quad \forall i \\ &= (\lambda - a_{ii}) v_i. \end{aligned}$$

Seja i o índice do elemento de maior valor absoluto em $\mathbf{v}$, ou seja, para todo j, $|v_i| \geq |v_j|$. Então

$$(\lambda - a_{ii}) v_i = \sum_{j \neq i} a_{ij} v_j$$

$$\begin{aligned}
\lambda - a_{ii} &= \sum_{j\neq i} a_{ij}\frac{v_j}{v_i} && \text{(dividimos por } v_i \neq 0\text{)}\\
|\lambda - a_{ii}| &= \left|\sum_{j\neq i} a_{ij}\frac{v_j}{v_i}\right| \\
&\leq \sum_{j\neq i} |a_{ij}|\left|\frac{v_j}{v_i}\right| \\
&\leq \sum_{j\neq i} |a_{ij}| && \text{(porque } |v_i| \geq |v_j|\text{)}\\
&= r_i.
\end{aligned}$$

Ou seja, a distância entre λ e a_{ii} é $\leq r_i$. Isto vale para quaisquer pares de autovetores e autovalores, e concluímos a demonstração. ■

Exemplo 6.39. Seja

$$A = \begin{pmatrix} 1 & 30 & 0 \\ 2 & -1 & 4 \\ -5 & 2 & 25 \end{pmatrix}.$$

Para esta matriz, temos

$$\begin{aligned}
r_1 &= |a_{12}| + |a_{13}| = 30\\
r_2 &= |a_{21}| + |a_{23}| = 6\\
r_3 &= |a_{31}| + |a_{32}| = 7
\end{aligned}$$

Os intervalos são

$$\begin{aligned}
a_{11} \pm 30 &= [-29, 31]\\
a_{22} \pm 6 &= [-7, 5]\\
a_{33} \pm 7 &= [18, 32]
\end{aligned}$$

A união dos intervalos é $[-29, 32]$. Os autovalores de A são

$$\begin{aligned}
\lambda_1 &= 17 - 2\sqrt{13} \approx 9.788\\
\lambda_2 &= 17 + 2\sqrt{13} \approx 24.211\\
\lambda_3 &= -9,
\end{aligned}$$

todos dentro do intervalo. ◄

Exemplo 6.40. Notamos que nada impede que os intervalos sejam desconexos. Seja

$$A = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 20 & 1 \\ 0 & 0 & -40 \end{pmatrix}.$$

Obtemos

$$r_1 = |-1| = 1$$

$$r_2 = |+1| = 1$$
$$r_3 = 0$$

Assim, os autovalores devem estar nos intervalos

$$a_{11} \pm r_1 = [-1, 2]$$
$$a_{22} \pm r_2 = [19, 21]$$
$$a_{33} \pm r_3 = [-40, -40] = \{-40\}$$

A união destes conjuntos é desconexa (não é um único intervalo), como ilustra a próxima figura.

Os autovalores de A são 1, 20 e -40 (note que A é triangular, portanto podemos inspecionar seus autovalores em sua diagonal, sem a necessidade de cálculos). ◀

Esta forma do Teorema de Gershgorin, no entanto, não vale para matrizes com autovalores complexos, porque usamos módulo para mensurar os valores $|\lambda - a_{ii}|$. Além disso, a relação $\leq$ não é definida para complexos [3]. Por exemplo, para a matriz

$$\begin{pmatrix} -1 & 1 \\ -2 & 1 \end{pmatrix}$$

teríamos

$$r_1 = |a_{12}| = 1$$
$$r_2 = |a_{21}| = 2,$$

obtendo os intervalos $[-2, 0]$ e $[-1, 3]$, mas os autovalores são $+i$ e $-i$. Não podemos dizer que $i \leq x$ ou $i \geq y$.

6.1.1 Autovalores complexos

Como os autovalores de uma matriz de elementos reais são raízes de um polinômio com coeficientes reais, pode ser que uma matriz de ordem n tenha menos de n autovalores reais. No entanto, toda matriz de ordem n sempre terá n autovalores complexos (porque todo polinômio de grau n tem n raízes complexas[4]), contando as multiplicidades. Além disso, se o polinômio tem grau ímpar, ele tem ao menos uma raiz real.

Teorema 6.41. *Um operador T em um epsaço de dimensão n, com n ímpar, sempre terá um autovalor real.*

Demonstração. Pelo Lema 6.22, o polinômio característico deste operador será

$$x^n + \underbrace{a_{n-1}x^{n-1} + \cdots + a_0}_{\text{grau menor que } n}$$

Quando $x \to \infty$, o polinômio tende a $+\infty$. Quando $x \to -\infty$, o polinômio tende a $-\infty$. Assim, pelo Teorema do Valor Intermediário, o polinômio tem pelo menos uma raiz real. ■

[3] Podemos usar a norma do número complexo, mas isto nos daria discos, e não intervalos.

[4] Como todo polinômio de grau n com coeficientes complexos tem raízes em $\mathbb{C}$, dizemos que $\mathbb{C}$ é um corpo *algebricamente fechado*. Claramente, $\mathbb{R}$ não é algebricamente fechado, já que $x^2 + 1$, com coeficientes em $\mathbb{R}$, não tem raízes em $\mathbb{R}$, mas sim em $\mathbb{C}$.

Exemplo 6.42. A matriz

$$\begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}$$

tem como polinômio característico x^2+4. Se a matriz A representar uma transformação linear de $\mathbb{R}^2$ em $\mathbb{R}^2$, então a transformação não tem autovalores ou autovetores. Se A representar uma transformação de $\mathbb{C}^2$ em $\mathbb{C}^2$, então a transformação tem os autovalores $-2i$ e $+2i$. ◀

★ 6.1.2 Matrizes complexas Hermitianas

Definição 6.43. A *matriz adjunta* de uma matriz A, denotada[5] A^H, é a transposta da matriz que tem os conjugados complexos dos elementos de A. Ou seja,

$$a^H_{ij} = \overline{a}_{ji}. \qquad \blacklozenge$$

Exemplo 6.44. A seguir mostramos tres matrizes e suas adjuntas.

$$A = \begin{pmatrix} -1 & -2i \\ 2 & 3-i \end{pmatrix} \quad B = \begin{pmatrix} 1+2i & i & 0 \\ 2-i & 3 & 1 \end{pmatrix} \quad C = \begin{pmatrix} i & 0 & 0 \\ 1 & 2i & 0 \\ 2 & 3 & 3i \end{pmatrix}$$

$$A^H = \begin{pmatrix} -1 & 2 \\ 2i & 3+i \end{pmatrix} \quad B^H = \begin{pmatrix} 1-2i & 2+1 \\ -i & 3 \\ 0 & 1 \end{pmatrix} \quad C^H = \begin{pmatrix} -i & 1 & 2 \\ 0 & -2i & 3 \\ 0 & 0 & -3i \end{pmatrix} \qquad \blacktriangleleft$$

Definição 6.45 (Matriz Hermitiana)**.** Uma matriz A é *Hermitiana* ou *auto-adjunta* se $A = A^H$. ◆

As entradas na diagonal de uma matriz Hermitiana devem necessariamente ser reais, porque devem ser iguais a seus conjugados.

Exemplo 6.46. A matriz

$$A = \begin{pmatrix} 1 & 2+i & 5 \\ 2-i & -3 & 1-i \\ 5 & 1+i & \pi \end{pmatrix}$$

é Hermitiana, porque

$$A^H = (\overline{A})^T = \begin{pmatrix} 1 & 2-i & 5 \\ 2+i & -3 & 1+i \\ 5 & 1-i & \pi \end{pmatrix}^T = \begin{pmatrix} 1 & 2+i & 5 \\ 2-i & -3 & 1-i \\ 5 & 1+i & \pi \end{pmatrix},$$

e $A = A^H$. ◀

Exemplo 6.47. A matriz

$$B = \begin{pmatrix} 1 & 2+i & 0 \\ 2-i & 1+i & 3 \\ 0 & 3 & 7 \end{pmatrix}$$

[5] Também é comum denotar a adjunta por A^* ou $A^\dagger$.

não é Hermitiana, porque não é igual a B^H:

$$B^H = (\overline{B})^T = \begin{pmatrix} 1 & 2-i & 0 \\ 2+i & 1-i & 3 \\ 0 & 3 & 7 \end{pmatrix}^T = \begin{pmatrix} 1 & 2+i & 0 \\ 2-i & 1-i & 3 \\ 0 & 3 & 7 \end{pmatrix}.$$

B e B^H diferem na posição $(2,2)$. ◀

Toda matriz real é também complexa, já que $\mathbb{R} \subset \mathbb{C}$. Desta forma, toda matriz real simétrica é também Hermitiana.

Exemplo 6.48. A matriz

$$A = \begin{pmatrix} -1 & 5 & 0 \\ 5 & 2 & 8 \\ 0 & 8 & 1 \end{pmatrix}$$

é Hermitiana, porque $A^H = A^T = A$. ◀

Teorema 6.49. *Se A é Hermitiana, seus autovalores são reais.*

Demonstração. Sejam A, λ e $\mathbf{v} \neq \mathbf{0}$, tais que $A = \lambda\mathbf{v}$.

$$\begin{aligned} A\mathbf{v} &= \lambda\mathbf{v} \\ (A\mathbf{v})^H &= (\lambda\mathbf{v})^H \\ \mathbf{v}^H A^H &= \overline{\lambda}\mathbf{v}^H \\ \mathbf{v}^H A &= \overline{\lambda}\mathbf{v}^H && (A^H = A) \\ \mathbf{v}^H A\mathbf{v} &= \overline{\lambda}\mathbf{v}^H\mathbf{v} \\ \mathbf{v}(\lambda\mathbf{v}) &= \overline{\lambda}\mathbf{v}^H\mathbf{v} && (A = \lambda v) \\ \lambda\mathbf{v}^H\mathbf{v} &= \overline{\lambda}\mathbf{v}^H\mathbf{v} \\ \lambda &= \overline{\lambda}, \end{aligned}$$

mas isto significa que $\lambda \in \mathbb{R}$. ■

Exemplo 6.50. Calculamos os autovalores da matriz

$$A = \begin{pmatrix} 1 & 2+i \\ 2-i & -3 \end{pmatrix}.$$

O polinômio característico de A é $x^2 + 2x - 8$, cujas raízes são $= -4$ e 2. ◀

Corolário 6.51. *Toda matriz Hermitiana, mesmo que com entradas complexas, tem determinante real.*

Corolário 6.52. *Toda matriz real simétrica tem autovalores reais.*

6.2 Diagonalização de operadores

Quando uma transformação linear é representada por uma matriz diagonal, sua aplicação sobre um vetor $\mathbf{v}$ consiste simplesmente na multiplicação de cada elemento da diagonal por um elemento de $\mathbf{v}$ (e não em uma multiplicação completa de matriz por vetor). Assim, ao invés de trabalharmos com uma transformação arbitrária, cuja aplicação é o mesmo que a multiplicação de matriz por vetor, trabalhamos com uma transformação da forma

$$\begin{aligned} D(x_1, x_2, \ldots, x_n)^T &= \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & d_n \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \\ &= d_1x_1 + d_2x_2 + \cdots + d_nx_n. \end{aligned}$$

Em muitas situações é útil mudar de base para realizar operações onde a transformação é diagonal, e posteriormente voltar à base anterior.

Mesmo que a matriz de uma transformação linear não seja diagonal, pode ser que a mesma transformação possa ser representada por uma matriz diagonal em alguma base diferente. Nesta seção verificamos quando um operador pode ser representado de forma diagonal, e como obter esta forma.

Definição 6.53 (Matriz diagonalizável)**.** Uma matriz quadrada A é *diagonalizável* se é similar a uma matriz diagonal – ou seja, se existe P tal que $P^{-1}AP$ é diagonal. ♦

Exemplo 6.54. Seja

$$A = \begin{pmatrix} 5 & -4 & 4 \\ -3 & 9 & -7 \\ -3 & 6 & -4 \end{pmatrix}.$$

A matriz A é diagonalizável, porque é similar a uma matriz diagonal D. Temos $D = P^{-1}AP$, onde

$$D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & -2 & 3 \\ -1 & 2 & -2 \\ 0 & -1/2 & 1/2 \end{pmatrix}, \quad P^{-1} = \begin{pmatrix} 0 & -1 & -4 \\ 1 & 1 & -2 \\ 1 & 1 & 0 \end{pmatrix}.$$

Observe que

$$P^{-1}AP = \begin{pmatrix} 0 & -1 & -4 \\ 1 & 1 & -2 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 5 & -4 & 4 \\ -3 & 9 & -7 \\ -3 & 6 & -4 \end{pmatrix} \begin{pmatrix} 1 & -2 & 3 \\ -1 & 2 & -2 \\ 0 & -1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

A matriz D é a representação de A como matriz diagonal, em base diferente.

Mais ainda, $2, 5$ e 3 são os autovalores de A. ◄

Teorema 6.55. *Uma matriz quadrada de ordem n é diagonalizável se e somente se tem n autovetores linearmente independentes.*

Demonstração. ($\Rightarrow$) Se A é diagonalizável, existe P tal que $D = P^{-1}AP$ é diagonal:

$$D = P^{-1}AP = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \ddots & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}.$$

Então $AP = PD$. Sejam $\mathbf{p}^1, \dots \mathbf{p}^n$ as colunas de P. Mas

$$AP = \begin{pmatrix} A\mathbf{p}^1 & A\mathbf{p}^2 & \cdots & A\mathbf{p}^n \end{pmatrix}$$
$$PD = \begin{pmatrix} \lambda_1\mathbf{p}^1 & \lambda_2\mathbf{p}^2 & \cdots & \lambda_n\mathbf{p}^n \end{pmatrix}$$

. Concluímos que:

i) $AP = PD$ implica que $A\mathbf{p}^i = \lambda_i\mathbf{p}^i$, e

ii) como P tem inversa, suas colunas são não-nulas e LI.

Ou seja, as colunas de P são autovetores de A, e são LI.
($\Leftarrow$) Sejam $\mathbf{p}^1, \dots, \mathbf{p}^n$ autovetores LI de A. Construa

$$P = \begin{pmatrix} \mathbf{p}^1 & \mathbf{p}^2 & \dots & \mathbf{p}^n \end{pmatrix},$$

Então, para cada coluna $\mathbf{p}^i$, $A\mathbf{p}^i$ é a multiplicação de A por um de seus autovetores, que sabemos ser igual a $\lambda_i\mathbf{p}^i$. Assim, $AP = PD$, onde D é a matriz diagonal com os autovalores $\lambda_1, \dots \lambda_n$. Como as colunas de P são LI, P tem inversa, e podemos multiplicar "$AP = PD$" à esquerda por P^{-1}, obtendo $D = P^{-1}AP$. ■

Método 6.56 (Diagonalização de matriz)**.** Encontre n autovetores LI de A (denote-os $v_1, v_2, \dots, v_n$). Seja P a matriz tendo as colunas iguais a estes vetores – ou seja, $P = (v_1 \;\; v_2 \;\; \dots \;\; v_n)$. A matriz $B = P^{-1}AP$ é diagonal e similar a A. ●

Exemplo 6.57. Seja

$$A = \begin{pmatrix} -3 & -\sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix}.$$

Primeiro obtemos dois de seus autovetores LI, que são

$$\begin{pmatrix} 1 \\ 1/\sqrt{3} \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -\sqrt{3} \end{pmatrix}.$$

Construímos então a matriz P e sua inversa:

$$P = \begin{pmatrix} 1 & 1 \\ 1/\sqrt{3} & -\sqrt{3} \end{pmatrix}, P^{-1} = \begin{pmatrix} 3/4 & \sqrt{3}/4 \\ 1/4 & -\sqrt{3}/4 \end{pmatrix}.$$

Temos então

$$P^{-1}AP = \begin{pmatrix} -4 & 0 \\ 0 & 0 \end{pmatrix}.$$ ◄

Podemos escolher qualquer conjunto de autovetores LI para diagonalizar uma matriz. Cada conjunto diferente nos dará uma base diferente onde o operador pode ser escrito como matriz diagonal. observe que o que poderá mudar é a *base*, e consequentemente as *matrizes de mudança de base* – mas a matriz diagonal que representa o operador é sempre a mesma, contendo em sua diagonal os autovalores do operador.

Exemplo 6.58. Seja

$$A = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 1 & 1 \\ 0 & 0 & -1 \end{pmatrix}.$$

A matriz A tem autovalores 0, -1 e 2. Os autovetores pertencentes a 0 são da forma $(x, x, 0)^T$; os pertencentes a -1 são da forma $(y, y, -y)^T$; os pertencentes a 2 são da forma $(z, -z, 0)^T$.

Escolhemos então autovetores para as colunas da matriz de mudança de base: $(1, 1, 0)^T$ $(1, 1, -1)^T$ $(1, -1, 0)^T$. Portanto,

$$P = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 0 & -1 & 0 \end{pmatrix}, \quad P^{-1} = \begin{pmatrix} 1/2 & 1/2 & 1 \\ 0 & 0 & -1 \\ 1/2 & -1/2 & 0 \end{pmatrix},$$

e

$$P^{-1}AP = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix},$$

Agora escolhemos autovetores diferentes para as colunas da matriz de mudança de base: $(-2, -2, 0)^T$ $(3, 3, -3)^T$ $(-1, 1, 0)^T$. Temos desta vez

$$Q = \begin{pmatrix} -2 & 3 & -1 \\ -2 & 3 & 1 \\ 0 & -3 & 0 \end{pmatrix}, \quad Q^{-1} = \begin{pmatrix} -1/4 & -1/4 & -1/2 \\ 0 & 0 & -1/3 \\ -1/2 & 1/2 & 0 \end{pmatrix}.$$

E finalmente,

$$Q^{-1}AQ = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix}. \quad \blacktriangleleft$$

Exemplo 6.59. A matriz

$$A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$$

tem polinômio característico $(2-x)^2$, e com duas raízes iguais: o autovalor 2 tem multiplicidade algébrica igual a dois. Este autovalor tem somente autovetores da forma

$$\begin{pmatrix} a \\ 0 \end{pmatrix}$$

e não podemos obter, portanto, dois autovetores linearmente independentes para construir uma matriz de mudança de base. A matriz *não* é diagonalizável.

Na verdade, qualquer matriz da forma

$$\begin{pmatrix} k & 1 & 0 & \cdots & 0 \\ 0 & k & 1 & & 0 \\ 0 & 0 & k & & \vdots \\ \vdots & & & \ddots & 1 \\ 0 & 0 & \cdots & 0 & k \end{pmatrix},$$

com a constante k na diagonal e uns acima da diagonal terá n autovalores iguais a k, e o autoespaço de todos terá dimensão um. Nenhuma destas matrizes é diagonalizável. $\blacktriangleleft$

Teorema 6.60. *Autovetores pertencentes a diferentes autovalores são linearmente independentes.*

6.3 Transformações lineares e matrizes não quadradas

Até o momento tratamos de operadores lineares e suas representações como matrizes quadradas. Nesta seção mostramos um fato a respeito do espectro do produto de matrizes retangulares.

Teorema 6.61. *Sejam* A *e* B *duas transformações lineares,*

$$A : \mathbb{R}^m \to \mathbb{R}^n$$
$$B : \mathbb{R}^n \to \mathbb{R}^m.$$

As duas transformações são representadas por matrizes A, $n \times m$ *e* B $m \times n$. *Assim, estão bem definidos os produtos*

- AB, *matriz quadrada de ordem* n, *e*
- BA, *matriz quadrada de ordem* m.

Os autovalores não nulos de AB *e* BA *são os mesmos.*

Demonstração. Seja $\mathbf{v} \neq \mathbf{0}$ autovetor de AB pertencente a um autovalor não nulo, ou seja,

$$AB\mathbf{v} = \lambda\mathbf{v}, \text{ com } \lambda \neq 0.$$

Então

$$(B)AB\mathbf{v} = B\lambda\mathbf{v}$$
$$(BA)B\mathbf{v} = \lambda(B\mathbf{v}),$$

e temos $B\mathbf{v} \neq 0$, porque $AB\mathbf{v} = \lambda\mathbf{v} \neq \mathbf{0}$. Assim, $B\mathbf{v}$ é autovetor de BA pertencente ao mesmo autovalor λ. ■

Exemplo 6.62. Sejam

$$A = \begin{pmatrix} 1 & 3 & -1 \\ -2 & 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & -2 \\ 2 & 5 \\ 0 & -1 \end{pmatrix}$$

Temos

$$AB = \begin{pmatrix} 5 & 14 \\ 2 & 2 \end{pmatrix}, \quad BA = \begin{pmatrix} 3 & -3 & -3 \\ -8 & 6 & 8 \\ 2 & 0 & -2 \end{pmatrix}$$

Os autovalores de AB são $9, -2$. Os de BA são $0, -2, 9$. ◄

★ 6.4 Diagonalização simultânea de dois operadores

Diagonalizar um operador é o mesmo que encontrar uma base na qual este operador é representado como uma matriz diagonal. Podemos eventualmente precisar representar *dois* (ou mais) operadores na forma diagonal, *na mesma base*.

Definição 6.63 (Operadores simultaneamente diagonalizáveis)**.** Um conjunto de operadores $\{A_i\}$ é simultaneamente diagonalizável se existe uma *única* matriz de mudança de base P tal que para todo operador A_i do conjunto, $P^{-1}A_iP$ é diagonal.

Em particular, dois operadores A e B são *simultaneamente diagonalizáveis* se existe P não singular tal que tanto $P^{-1}AP$ como $P^{-1}BP$ são diagonais. ♦

Lema 6.64. *Sejam A e B dois operadores lineares em um mesmo espaço vetorial (de dimensão finita ou infinita). Se $AB = BA$, então o operador B é um operador linear no autoespaço de A (ou seja, se $\mathbf{v}$ está no autoespaço de A, $B\mathbf{v}$ também está).*

Demonstração. Se $\mathbf{v}$ é autovetor de λ para o operador A, então

$$\begin{aligned} A\mathbf{v} &= \lambda\mathbf{v} \\ BA\mathbf{v} &= B\lambda\mathbf{v} \\ A(B\mathbf{v}) &= \lambda(B\mathbf{v}), \end{aligned}$$

portanto $B\mathbf{v}$ também é autovetor de λ. ■

Teorema 6.65. *Dois operadores A e B em $\mathbb{R}^n$ (e em qualquer espaço vetorial de dimensão finita) são diagonalizáveis simultaneamente se e somente se $AB = BA$.*

Demonstração. ($\Rightarrow$) Se A e B são simultaneamente diagonalizáveis, então podemos escrever

$$\begin{aligned} A &= P^{-1}A_DP \\ B &= P^{-1}B_DP \end{aligned}$$

O produto AB é, portanto,

$$\begin{aligned} AB &= P^{-1}A_DPP^{-1}B_DP \\ &= P^{-1}A_DB_DP \\ &= P^{-1}B_DA_DP && \text{(produto de diagonais é comutativo (Exercício 87))} \\ &= P^{-1}B_D(PP^{-1})A_DP \\ &= (P^{-1}B_DP)(P^{-1}A_DP) \\ &= BA. \end{aligned}$$

($\Leftarrow$) Sejam $\lambda_1, \lambda_2, \ldots, \lambda_k$ os autovalores de A. Seja $\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d_n}$ uma base β formada por autovetores de A, *ordenada por autovalor* – ou seja, os primeiros vetores pertencem ao primeiro autovalor λ_1, em seguida temos os vetores do autovalor λ_2, e assim por diante. Pelo Lema 6.64, a matriz que representa B nesta base é diagonal por blocos (leva autovetores de um autoespaço de A neste mesmo autoespaço):

$$[B]_\beta = \begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B_k \end{pmatrix}.$$

Cada bloco i é uma matriz quadrada cuja ordem é a multiplicidade geométrica do autovalor λ_i de A.

Temos portanto uma base em que B é descrito por uma matriz *diagonal por blocos*. Para obter uma matriz diagonal, observamos que podemos diagonalizar cada bloco separadamente. Para isso, basta tomar cada

bloco A_i e obter m vetores LI (m é a multiplicidade geométrica de λ_i, todos no autoespaço de λ_i em A, *que também sejam autovetores de* B. Estes vetores serão autovetores tando de B como de A (e em A, eles pertencerão a λ_i). ■

Exemplo 6.66. Começamos com um exemplo onde as duas matrizes já tem os mesmos autoespaços, portanto não precisamos diagonalizar blocos. Sejam

$$A = \begin{pmatrix} -2 & 1 \\ 1 & -2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

os produtos AB e BA são iguais:

$$AB = BA = \begin{pmatrix} -3 & 3 \\ 3 & -3 \end{pmatrix}$$

Os autovalores e autovetores de A e B são

$$\begin{aligned} A &: -1, (x,x)^T; -3, (x,-x)^T \\ B &: \ \ 0, (x,x)^T; \ \ \ 2, (x,-x)^T \end{aligned}$$

Assim, se usarmos os vetores

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

para construir a matriz de mudança de base, teremos diagonalizado os dois operadores! Construímos

$$P = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad P^{-1} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix},$$

e temos finalmente

$$\begin{aligned} A = P^{-1} A_D P &= \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -3 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \\ B = P^{-1} B_D P &= \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \end{aligned}$$

Os dois operadores são diagonais quando descritos na base ordenada

$$\left((1,1)^T, (1,-1)^T\right).$$ ◄

Exemplo 6.67. Sejam A e B dois operadores em $\mathbb{R}^4$:

$$A = \begin{pmatrix} 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \\ 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \end{pmatrix}, \quad B \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Estes operadores comutam:

$$AB = BA = \begin{pmatrix} 0 & 0 & 0 & 3 \\ 0 & 0 & 3 & 0 \\ 0 & 3 & 0 & 0 \\ 3 & 0 & 0 & 0 \end{pmatrix}.$$

Diagonalizamos A primeiro: seus autovalores são -3 e $+3$, cada um com multiplicidade algébrica 2.

Os autoespaços são:

$$E(-3) = \left[\begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ -1 \end{pmatrix} \right], \quad E(+3) = \left[\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \right].$$

Temos então uma base β onde A é diagonal,

$$P = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix},$$

e

$$P^{-1}AP = \begin{pmatrix} -3 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

O operador B, descrito nsta base, é

$$P^{-1}BP = \left(\begin{array}{cc:cc} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right) = \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix}$$

Os dois blocos são

$$B_1 = B_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

e cada bloco tem autovalores -1 e 1. Os autovetores de B_1 (e de B_2) são

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} -1 \\ 1 \end{pmatrix}.$$

O primeiro autovetor tem as coordenadas 1 e -1, indicando que posemos tomar os dois primeiros autovetores $\mathbf{d_1}$ e $\mathbf{d_2}$ e usar $\mathbf{d_1} - \mathbf{d_2}$ deve ser usado.

De acordo com o segundo autovetor, $\mathbf{d_1} + \mathbf{d_2}$ deve ser usado em seguida.

O terceiro e quarto autovetores (de B_2) nos dão $\mathbf{d_3} \pm \mathbf{d_4}$, portanto temos

$$Q = \begin{pmatrix} \mathbf{d_1} - \mathbf{d_2}, & \mathbf{d_1} + \mathbf{d_2}, & \mathbf{d_3} - \mathbf{d_4}, & \mathbf{d_3} + \mathbf{d_4} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Temos

$$Q^{-1} = \frac{1}{4} \begin{pmatrix} 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Nesta base, tanto A como B são diagonais:

$$[A]_\gamma = Q^{-1}AQ = \frac{1}{4}\begin{pmatrix} 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \\ 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} -3 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

$$[B]_\gamma = Q^{-1}BQ = \frac{1}{4}\begin{pmatrix} 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Notamos que, como os autovalores são os mesmos em qualquer base (matrizes similares tem os mesmos autovalores), podemos ver os autovalores de A e B nas suas representações diagonais na base γ. ◀

O Teorema 6.65 pode ser generalizado para espaços de dimensão infinita. Não o faremos aqui.

6.5 Cálculo de autovalores e autovetores

Os métodos que apresentamos para determinar os autovalores e autovetores de uma transformação são úteis e eficientes para matrizes pequenas. Observe que se o polinômio característico de uma matriz tem grau elevado, não temos sequer fórmula para obter suas raízes.

Teorema 6.68. *Qualquer método para a obtenção do valor exato dos autovalores de matrizes de ordem n pode ser usado para obter as raízes de qualquer polinômio de grau n.*

A relevância deste Teorema se faz clara quando consideramos também o Teorema de Abel-Ruffini, que apresentamos sem demonstração.

Teorema 6.69 (Abel-Ruffini)**.** *Não existe como descrever as raízes de polinômios de grau cinco ou mais alto, usando apenas as operações aritméticas básicas (soma, subtração, multiplicação, divisão e extração de raiz n-ésima).*

Isto *não* significa, no entanto:

- que seja impossível encontrar autovalores para famílias específicas de matrizes (o exemplo mais simples é o das matrizes triangulares, onde sequer precisamos de "método", já que o sautovalores ficam expostos na diagonal);
- que não haja método para aproximar autovalores. Na verdade há muitos deles;
- que não haja método para a obtenção de autovalores exatos (o Teorema apenas diz que não podem ser obtidos usando apenas aquelas operações).

Para grandes matrizes há diversos métodos de obtenção de autovalores, cujas descrições o leitor encontrará na literatura de Cálculo Numérico [Fra07].

6.6 Aplicações

Damos aqui uma pequena quantidade de aplicações dos conceitos apresentados neste Capítulo. No início da seção 6.2, dissemos que "*em muitas situações é útil mudar de base para realizar operações onde a transformação é diagonal, e posteriormente voltar à base anterior*". Grande parte das aplicações nesta Seção resume-se a isto.

6.6.1 Potência de matriz [diagonalização]

O cálculo da potência A^n é muito simples quando A é diagonal:

$$\operatorname{diag}(a_1, a_2, \ldots, a_k)^n = \operatorname{diag}(a_1^n, a_2^n, \ldots, a_k^n).$$

Se A não é diagonal, é necessário realizar uma grande quantidade de operações[6],

$$A^n = \overbrace{AAA\cdots A}^{n-1 \text{ operações}}$$

Teorema 6.70. *Seja A diaginalizável com $A = PDP^{-1}$, e $n \in \mathbb{N}$. Então*

$$A^n = PD^nP^{-1}.$$

Demonstração. Para demonstrar, simplesmente reescrevemos A^n como produto de n matrizes:

$$\begin{aligned} A^n &= \overbrace{AAA\cdots A}^{n-1 \text{ operações}} \\ &= (PDP^{-1})(PDP^{-1})\cdots(PDP^{-1}) \\ &= PD(P^{-1}P)D(P^{-1}P)D\cdots DP^{-1} \\ &= PDIDI\cdots DP^{-1} \\ &= PD^nP^{-1}. \end{aligned}$$

■

Se A é diagonalizável e n é muito grande, é vantajoso calcular a sua potência na base em que é diagonal, fazendo assim uma quantidade fixa (e pequena) de operações.

Exemplo 6.71. Seja

$$A = \begin{pmatrix} 3 & 1/3 \\ 15 & -1 \end{pmatrix}.$$

A matriz A é diagonalizável:

$$A = QDQ^{-1} = \begin{pmatrix} 1 & 1 \\ -15 & 3 \end{pmatrix}\begin{pmatrix} -2 & 0 \\ 0 & 4 \end{pmatrix}\frac{1}{6}\begin{pmatrix} 1 & -\frac{1}{3} \\ 5 & \frac{1}{3} \end{pmatrix}.$$

Calculamos A^2 e A^{10}.

$$A^2 = A.A = \begin{pmatrix} 14 & 2/3 \\ 30 & 6 \end{pmatrix}.$$

Poderíamos também ter calculado

$$A^2 = QD^2Q^{-1} = \begin{pmatrix} 1 & 1 \\ -15 & 3 \end{pmatrix}\begin{pmatrix} 4 & 0 \\ 0 & 16 \end{pmatrix}\frac{1}{6}\begin{pmatrix} 1 & -\frac{1}{3} \\ 5 & \frac{1}{3} \end{pmatrix} = \begin{pmatrix} 14 & 2/3 \\ 30 & 6 \end{pmatrix}$$

Para calcular A^{10}, podemos computar as nove multiplicações $A.A\cdots A$, mas é mais simples calcular

$$A^{10} = QD^{10}Q^{-1} = \begin{pmatrix} 1 & 1 \\ -15 & 3 \end{pmatrix}\begin{pmatrix} 2^{10} & 0 \\ 0 & 4^{10} \end{pmatrix}\frac{1}{6}\begin{pmatrix} 1 & -\frac{1}{3} \\ 5 & \frac{1}{3} \end{pmatrix} = \begin{pmatrix} 2^9 & 1707 & \frac{2^9\ 341}{3} \\ 2^9 & 5115 & 2^9\ 343 \end{pmatrix}.$$

◀

[6] na verdade podemos calcular A^2, depois $A^2A^2 = A^4$, depois $A^4A^4 = A^8$, depois $A^8A^8 = A^{32}$, etc, acelerando o processo, mas ainda assim a quantidade de operações pode ser arbitrariamente grande.

6.6.2 Relações de recorrência [polinômio característico; diagonalização]

Definição 6.72 (Relação de recorrência)**.** Uma *relação de recorrência de ordem* k é uma definição de uma sequência que descreve o n-ésimo termo como função dos k anteriores:

$$\begin{aligned} a_1 &= z_1, \\ a_2 &= z_2, \\ &\vdots \\ a_k &= z_k \\ a_n &= f(a_{n-1}, a_{n-2}, \ldots, a_{n-k}), \end{aligned}$$

onde os *valores iniciais* z_i são constantes. A definição da sequência deve incluir também k valores iniciais, além da equação recursiva.

Uma recorrência é *linear* se é da forma

$$a_n = c_1 a_{n-1} + \cdots + c_k a_{n-k} + g(n),$$

e é *homogênea* se $g(n) = 0$. ♦

Exemplo 6.73. A função fatorial é dada pela recorrência

$$\begin{aligned} f_0 &= 1, \\ f_n &= n f_{n-1}, \end{aligned}$$

que é linear e homogênea. ◀

Exemplo 6.74. Como visto no Exemplo 1.36, a sequência de Fibonacci pode ser definida pela recorrência

$$\begin{aligned} F_1 &= 1, \\ F_2 &= 1, \\ F_n &= F_{n-1} + F_{n-2}, \end{aligned}$$

e seus primeiros termos são

$$\begin{aligned} F_1 &= 1 \quad F_5 = 5 \\ F_2 &= 1 \quad F_6 = 8 \\ F_3 &= 2 \quad F_7 = 13 \\ F_4 &= 3 \quad F_8 = 21 \end{aligned}$$

◀

Estamos interessados no problema de, dada uma definição de sequência como recorrência, encontrar uma forma fechada para ela.

Exemplo 6.75. Considere a sequência (a_n) definida recursivamente a seguir.

$$\begin{aligned} a_0 &= 1 \\ a_n &= 2a_{n+1} \end{aligned}$$

Os primeiros termos desta sequência são

$$\begin{aligned} a_0 &= 1, \\ a_1 &= 2, \\ a_2 &= 4, \\ a_3 &= 8, \\ &\vdots \end{aligned}$$

A forma fechada para o n-ésimo termo da sequência é

$$a_n = 2^n,$$

que percebemos imediatamente apenas porque a sequência é familiar e muito simples. ◀

Teorema 6.76. *Uma equação recorrente de ordem k acompanhada de k valores iniciais define unicamente uma sequência.*

Se a equação estiver acompanhada de menos do que k valores iniciais, há mais de uma sequência que satisfaz a relação.

Se a equação estiver acompanhada de menos do que k valores iniciais, uma de duas situações ocorrerá: ou a recorrência definirá uma única sequência, ou nenhuma sequência satisfará a definição.

Definição 6.77 (Matriz associada a uma equação de recorrência linear)**.** Uma equação de recorrência linear de ordem k

$$a_n = c_1 a_{n-1} + c_2 a_{n-1} + \cdots + c_k a_{n-k}$$

pode ser descrita em forma matricial como

$$\overbrace{\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ 0 & 0 & 0 & \ddots & \\ \vdots & & & & 1 \\ c_k & c_{k-1} & c_{k-2} & \cdots & c_1 \end{pmatrix}}^{C} \begin{pmatrix} a_n \\ a_{n+1} \\ a_{n+2} \\ \vdots \\ a_{n+k} \end{pmatrix} = \begin{pmatrix} a_{n+1} \\ a_{n+2} \\ a_{n+3} \\ \vdots \\ a_{n+k+1} \end{pmatrix}$$

A matriz C é chamada de *matriz associada* à equação de recorrência (a_n). ◆

Exemplo 6.78. Para ilustrar a construção da matriz associada usamos a seguinte equação de recorência:

$$a_n = 2a_{n-1} - 3a_{n-2} + \frac{1}{2}a_{n-3} - a_{n-4}.$$

Os coeficientes da equação são $(1, -3, 1/2, -1)$, e a matriz associada a esta equação é

$$C = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 1/2 & -3 & 2 \end{pmatrix},$$

de forma que

$$C\begin{pmatrix} a_n \\ a_{n+1} \\ a_{n+2} \\ a_{n+3} \end{pmatrix} = \begin{pmatrix} a_{n+1} \\ a_{n+2} \\ a_{n+3} \\ a_{n+4} \end{pmatrix},$$

com $a_{n+4} = 2a_{n+3} - 3a_{n_2} + (1/2)a_{n+1} - a_n$, como esperado. ◀

Vemos que C transforma $a_n, \ldots, a_{n+k}$ em outro vetor coluna, com $a_{n+1}, \ldots a_{n+k+1}$. Se aplicarmos C novamente, obteremos os próximos k valores, e assim por diante.

$$\begin{pmatrix} a_n \\ a_{n+1} \\ a_{n+2} \\ \vdots \\ a_{n+k} \end{pmatrix} \xrightarrow{C} \begin{pmatrix} a_{n+1} \\ a_{n+2} \\ a_{n+3} \\ \vdots \\ a_{n+k+1} \end{pmatrix} \xrightarrow{C} \begin{pmatrix} a_{n+2} \\ a_{n+3} \\ a_{n+4} \\ \vdots \\ a_{n+k+2} \end{pmatrix} \xrightarrow{C} \cdots$$

Assim, se pudermos calcular C^n e aplicar no vetor com os valores iniciais, teremos um valor com o valor de a_n na primeira posição.

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_k \end{pmatrix} \xrightarrow{C^n} \begin{pmatrix} a_{n+1} \\ a_{n+2} \\ a_{n+3} \\ \vdots \\ a_{n+k} \end{pmatrix}$$

Calcular C^n é fácil se pudermos diagonalizá-la: determinamos a base em que C é diagonal, e calculamos PD^nP^{-1}.

Assim, temos o seguinte método.

Método 6.79. Seja C uma matriz associada a uma relação de recorrência de ordem k. Se D é diagonalizáve, sejam P e P^{-1} as matrizes de mudança de base tais que $D = P^{-1}CP$ é diagonal. Seja Z o vetor coluna com os valores iniciais da recorrência,

$$Z = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ \vdots \\ z_k \end{pmatrix}.$$

A forma fechada para o n-ésimo termo da recorrência é dada pela primeira entrada do vetor

$$PD^{n-1}P^{-1}Z.$$ ●

Antes de exemplificarmos este método, apresentamos alguns Teoremas que tornam sua aplicação mais fácil.

Teorema 6.80. *Seja C a matriz associada à equação de recorrência de uma sequência a_n. O polinômio característico de C é*

$$\lambda^k + c_k\lambda^{k-1} + c_{k-1}\lambda^{k-2} + \cdots + c_2\lambda + c_1.$$

C não tem autovalores zero, e para qualquer autovalor λ de C, $a_n = \lambda^n$ é solução da recorrência $\mathbf{a}_n = C\mathbf{a}_{n-1}$.

Teorema 6.81. *Seja λ o autovalor de uma matriz associada a uma relação de recorrência linear de ordem k. Então*

$$(1, \lambda, \lambda^2, \ldots, \lambda^{k-1})^T$$

é autovetor pertencente a λ.

Exemplo 6.82. Considere a equação recorrente

$$\begin{aligned} a_0 &= 1, \\ a_1 &= 2, \\ a_n &= -2a_{n-1} + 3a_{n-2}. \end{aligned}$$

A matriz associada a ela é

$$\begin{pmatrix} 0 & 1 \\ 3 & -2 \end{pmatrix}$$

com autovalores -3 e 1, e autovetores gerados por

$$\begin{pmatrix} 1 \\ -3 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

A matriz de mudança de base e sua inversa são

$$P = \begin{pmatrix} 1 & 1 \\ -3 & 1 \end{pmatrix}, \quad P^{-1} = \frac{1}{4}\begin{pmatrix} 1 & -1 \\ 3 & 1 \end{pmatrix}.$$

O n-ésimo termo da sequência será dado por

$$\begin{aligned} \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix} &= PD^{n-1}P^{-1}Z \\ &= \begin{pmatrix} 1 & 1 \\ -3 & 1 \end{pmatrix}\begin{pmatrix} -3 & 0 \\ 0 & 1 \end{pmatrix}^n \frac{1}{4}\begin{pmatrix} 1 & -1 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ -3 & 1 \end{pmatrix}\begin{pmatrix} (-3)^n & 0 \\ 0 & 1 \end{pmatrix}\frac{1}{4}\begin{pmatrix} 1 & -1 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 2 \end{pmatrix} \\ &= \frac{1}{4}\begin{pmatrix} 5 - (-3)^n \\ 5 - (-3)^{n+1}. \end{pmatrix} \end{aligned}$$

e temos a forma fechada para o n-ésimo termo da sequência:

$$a_n = \frac{5 - (-3)^n}{4}.$$ ◀

6.6.3 Solução de sistemas de equações de diferença [diagonalização]

Uma *equação de diferenças* é como uma equação diferencial, mas discreta. Uma equação de diferença, da forma $x(t) = \alpha x(t-1)$ representa a evolução de um processo em tempo discreto, e é muito usada em biologia, economia, engenharia e diversas outras áeras. Por exemplo, $x(t)$ poderia representar a quantidade

de animais de uma certa espécie em um ecossistema, a quantidade de dinheiro em um fundo de investimento ou empréstimo, ou qualquer outra quantidade que evolua ao longo do tempo, e que dependa da quantidade em um momento anterior.

Considere o sistema de equações de diferença

$$\begin{aligned} x_1(t) &= 2x_1(t-1) \\ x_2(t) &= (1/5)x_2(t-1) \end{aligned}$$

Como as duas equações são independentes, podem ser resolvidas separadamente.

A primeira equação significa que a quantidade x_1 sempre dobra a cada unidade de tempo. Após t unidades de tempo, teremos portanto $x_1(0)$ multiplicado por 2^t.

De acordo com a segunda equação, x_2 cai para um quinto a cada unidade de tempo. No tempo t, portanto, teremos $x_2(0)$ multiplicado por 5^{-t}.

Já podemos agora calcular $x_1(t)$ e $x_2(t)$ a partir de seus valores iniciais:

$$\begin{aligned} x_1(t) &= 2^t x_1(0) \\ x_2(t) &= 5^{-t} x_2(0) \end{aligned}$$

Este sistema foi resolvido facilmente porque as equações são independentes – ou seja, se o representarmos como uma matriz, na forma $\mathbf{x}(t) = A\mathbf{x}(t-1)$, então A será diagonal:

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1/5 \end{pmatrix}$$

Sabemos que 2 e 5 são os autovalores desta matriz, e que seus autovetores são da forma $(ax_1, 0)^T$ e $(0, bx_2)^T$. Cada uma das duas equações é a expressão de $A\mathbf{x} = \lambda\mathbf{x}$ para um dos autovalores e um dos autovetores:

Quando as equações não são independentes, a matriz dos coeficientes do sistema não é diagonal. Tomamos agora como exemplo o sistema a seguir.

$$\begin{aligned} x_1(t) &= 2x_1(t-1) + 2x_2(t-1) \\ x_2(t) &= 2x_1(t-1) + 5x_2(t-1) \end{aligned}$$

Não conseguimos resolver as equações isoladamente, como fizemos antes, porque elas dependem uma da outra. Se o descrevermos na forma matricial, a matriz dos coeficientes será

$$A = \begin{pmatrix} 2 & 2 \\ 2 & 5 \end{pmatrix}.$$

Notamos, no entanto, que A é diagonalizável: seus autovalores são 6 e 1, com autovetores da forma $(a, 2a)^T$ e $(b, -b/2)^T$.

A matriz A descreve o sistema na base canônica C. Obtemos agora a matriz diagonal similar a A, ou seja, a matriz diagonal $D = [A]_\delta$, que descreve o sistema em uma base δ, e as matrizes de mudança de base:

$$P^{-1}AP = \begin{pmatrix} 1/5 & 2/5 \\ 4/5 & -2/5 \end{pmatrix} \begin{pmatrix} 2 & 2 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & -1/2 \end{pmatrix} = \begin{pmatrix} 6 & 0 \\ 0 & 1 \end{pmatrix}.$$

Isso significa que as matrizes P e P^{-1}, de mudança de base, nos permitem levar vetores para a base δ onde A é diagonal. Como usaremos a matriz na base δ, precisamos também descrever o vetor $\mathbf{x}$ nesta base. Seja

$$\mathbf{y} = [\mathbf{x}]_\delta.$$

Determinamos agora como escrever $\mathbf{x}$ em função de $\mathbf{y}$ e $\mathbf{y}$ em função de $\mathbf{x}$. Para isso, aplicamos as matrizes de mudança de base em ambos. Começamos por $\mathbf{y} = P^{-1}\mathbf{x}$:

$$\mathbf{y} = \begin{pmatrix} 1/5 & 2/5 \\ 4/5 & -2/5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} (x_1 + 2x_2)/5 \\ (4x_1 - 2x_2)/5 \end{pmatrix}$$

Assim,

$$\begin{aligned} y_1 &= (x_1 + 2x_2)/5 \\ y_2 &= (4x_1 - 2x_2)/5 \end{aligned}$$

Agora calculamos $P\mathbf{y}$:

$$\mathbf{x} = \begin{pmatrix} 1 & 1 \\ 2 & -1/2 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} y_1 + y_2 \\ 2y_1 - y_2/2 \end{pmatrix}$$

Ou seja,

$$\begin{aligned} x_1 &= y_1 + y_2 \\ x_2 &= 2y_1 - y_2/2 \end{aligned}$$

Agora resolvemos o sistema

$$\begin{aligned} y_1(t) &= 6y_1(t-1) \\ y_2(t) &= y_2(t-1). \end{aligned}$$

Este segundo sistema consiste de duas equações independentes, e verificamos facilmente que

$$\begin{aligned} y_1(t) &= 6^t y_1(0) \\ y_2(t) &= y_2(0). \end{aligned}$$

Finalmente, conseguimos escrever $x_1(t)$ e $x_2(t)$ em função de $x_1(0)$ e $x_2(0)$:

$$\begin{aligned} x_1(t) &= y_1(t) + y_2(t) \\ &= 6^t y_1(0) + y_2(0) \\ &= 6^t \left(\frac{x_1(0) - 2x_2(0)}{5} \right) + \left(\frac{4x_1(0) - 2x_2(0)}{5} \right) \\ x_2(t) &= 2y_1(t) - y_2(t)/2 \\ &= 2(6^t y_1(0)) - (1/2)y_2(0) \\ &= 2\left[6^t \left(\frac{x_1(0) + 2x_2(0)}{5} \right) \right] - \frac{1}{2} \left(\frac{4x_1(0) - 2x_2(0)}{5} \right) \end{aligned}$$

6.6.4 Exponencial de matriz [diagonalização]

Da mesma forma que a exponencial e^x surge na solução de equações diferenciais, a exponencial e^A, onde A é uma matriz, também tem papel importante na solução de *sistemas* de equações diferenciais.

A exponencial e^x para números x reais e complexos é definida como[7]

$$e^x = \sum_{i=0}^{\infty} \frac{x^i}{i!}.$$

A exponencial de uma matriz é definida exatamente da mesma forma, porque a definição só depende de podermos calcular a n-ésima potência da matriz.

Definição 6.83 (Exponencial de matriz)**.** Seja A uma matriz quadrada. A exponencial de A é definida como

$$e^A = \sum_{i=0}^{\infty} \frac{A^i}{i!}.$$ ♦

Primeiro observamos que é fácil calcular e^D para qualquer matriz diagonal D.

Teorema 6.84. *Seja D uma matriz diagonal. Então*

$$e^D = \operatorname{diag}(e^{d}_{11}, e^{d}_{22}, \ldots, e^{d}_{nn}).$$

Demonstração.

$$\begin{aligned}
e^D &= \sum_{i=0}^{\infty} \frac{D^i}{i!} \\
&= \sum_{i=0}^{\infty} \frac{1}{i!} \begin{pmatrix} d_{11} & & & \\ & d_{22} & & \\ & & \ddots & \\ & & & d_{nn} \end{pmatrix}^i \\
&= \sum_{i=0}^{\infty} \begin{pmatrix} \frac{d_{11}^i}{i!} & & & \\ & \frac{d_{22}^i}{i!} & & \\ & & \ddots & \\ & & & \frac{d_{nn}^i}{i!} \end{pmatrix} \\
&= \begin{pmatrix} \sum_{i=0}^{\infty} \frac{d_{11}^i}{i!} & & & \\ & \sum_{i=0}^{\infty} \frac{d_{22}^i}{i!} & & \\ & & \ddots & \\ & & & \sum_{i=0}^{\infty} \frac{d_{nn}^i}{i!} \end{pmatrix} \\
&= \begin{pmatrix} e^{d_{11}} & & & \\ & e^{d_{22}} & & \\ & & \ddots & \\ & & & e^{d_{nn}} \end{pmatrix}.
\end{aligned}$$ ■

[7] Esta é a expansão de Taylor no zero (a série de Maclaurin),

$$\begin{aligned}
e^x &= \frac{\exp(0)(x^0)}{0!} + \frac{\exp'(0)x^1}{1!} + \frac{\exp''(0)x^2}{2!} + \frac{\exp'''(0)x^3}{3!} + \cdots \\
&= 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots
\end{aligned}$$

Exemplo 6.85. Seja

$$D = \text{diag}(2,4,1) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Então

$$e^D = \begin{pmatrix} e^2 & 0 & 0 \\ 0 & e^4 & 0 \\ 0 & 0 & e \end{pmatrix}. \qquad \blacktriangleleft$$

Agora tratamos de matrizes não diagonais, mas diagonalzáveis.

Teorema 6.86. *Se A é diagonalizável, com $A = PDP^{-1}$, então $e^A = Pe^DP^{-1}$.*

Demonstração. Usaremos o teorema 6.70, que nos garante que $A^n = PD^nP^{-1}$.

Calculamos agora

$$e^A = \sum_{i=0}^{\infty} \frac{A^i}{i!} = \sum_{i=0}^{\infty} \frac{(PDP^{-1})^i}{i!} = P\left(\sum_{i=0}^{\infty} \frac{D^i}{i!}\right)P^{-1} = Pe^DP^{-1}. \qquad \blacksquare$$

Exemplo 6.87. Seja

$$A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}.$$

Calculamos e^A a seguir. A matriz tem autovalores 4 e 2, e é diagonalizável: $D = P^{-1}AP$ é diagonal, com

$$P = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad D = \begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}, \quad P^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Assim,

$$e^D = \begin{pmatrix} e^4 & 0 \\ 0 & e^2 \end{pmatrix}.$$

Como $A = PDP^{-1}$, temos

$$\begin{aligned} e^A &= Pe^DP^{-1} \\ &= \begin{pmatrix} \frac{e^4+e^2}{2} & \frac{e^4-e^2}{2} \\ \frac{e^4-e^2}{2} & \frac{e^4+e^2}{2} \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} e^4+e^2 & e^4-e^2 \\ e^4-e^2 & e^4+e^2 \end{pmatrix}. \end{aligned} \qquad \blacktriangleleft$$

Exemplo 6.88. Mencionamos que podemos precisar trabalhar com autovalores complexos, mesmo que nossa matriz seja real. Este exemplo ilustra tal situação.

Seja

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Calculamos e^A a seguir. A matriz tem autovalores $-i$ e i, e é diagonalizável: $D = P^{-1}AP$ é diagonal, com

$$P = \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix}, D = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

Assim,

$$e^D = \begin{pmatrix} e^{-i} & 0 \\ 0 & e^i \end{pmatrix}$$

Finalmente, $A = PDP^{-1}$, portanto

$$e^A = Pe^D P^{-1} = \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix} \begin{pmatrix} e^{-i} & 0 \\ 0 & e^i \end{pmatrix} \begin{pmatrix} 1/2 & i/2 \\ 1/2 & -i/2 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} e^i + e^{-i} & ie^{-i} - ie^i \\ ie^i - ie^{-i} & e^i + e^{-i} \end{pmatrix}$$ ◀

Teorema 6.89. *Se A é uma matriz quadrada diagonalizável com autovalores $\lambda_1, \lambda_2, \ldots, \lambda_n$, então os autovalores de e^A são $e^{\lambda_1}, e^{\lambda_2}, \ldots, e^{\lambda_n}$.*

Demonstração. Sabemos que se A é diagonalizável, $A = PDP^{-1}$, onde D é diagonal, e os elementos d_{ii} são os autovalores de A. Também sabemos que

$$e^D = \operatorname{diag}(e^{d_{11}}, \ldots, e^{nn}).$$

P e P^{-1} são matrizes de mudança de base e não modificam os autovalores, e como

$$e^A = Pe^D P^{-1},$$

os autovalores de e^A são os mesmos que os de A. ■

Exemplo 6.90. Seja

$$A = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}.$$

Seus autovalores são 1 e 2. A exponencial de A é

$$e^A = \begin{pmatrix} e & 3e^2 - 3e \\ 0 & e^2 \end{pmatrix},$$

com autovalores $e^1 = e$ e e^2.

Seja

$$B = \begin{pmatrix} -1 & 2 \\ 2 & -1 \end{pmatrix}.$$

Seus autovalores são 1 e -3. A exponencial de B é

$$e^B = \frac{1}{2} \begin{pmatrix} e^{-3}(e^4 + 1) & e^{-3}(e^4 - 1) \\ e^{-3}(e^4 - 1) & e^{-3}(e^4 + 1) \end{pmatrix},$$

com autovalores e e e^{-3}. ◀

6.6.5 Solução de sistemas de equações diferenciais [diagonalização]

Na seção 6.6.3 descrevemos um método para resolver sistemas de equações de diferença. Nesta seção tratamos de sistemas de equações diferenciais. Uma resumida introdução às Equações Diferenciais é dada no Apêndice δ.

Definição 6.91 (Sistema de equações diferenciais)**.** Um *sistema de equações diferenciais* é um conjunto de equações diferenciais. ♦

Dado um sistema de equações diferenciais, que contém equações envolvendo derivadas de várias funções diferentes, possivelmente compartilhando argumentos, queremos determinar a forma fechada para estas funções em função de valores iniciais para elas.

Precisaremos neste exemplo do conceito de derivada de um vetor, que definimos a seguir. Também definimos, por completude, integração de vetores.

Definição 6.92 (Derivação e integração de vetor)**.** Seja $\mathbf{y}$ um vetor de funções, ou seja,

$$\mathbf{y} = \begin{pmatrix} y_1(x) \\ y_2(x) \\ \vdots \\ y_n(x) \end{pmatrix}.$$

Denotamos por y_i a i-ésima função. A derivada de $\mathbf{y}$, que denotamos $\mathbf{y}'$, é

$$\mathbf{y}' = \begin{pmatrix} y_1' \\ y_2' \\ \vdots \\ y_n' \end{pmatrix}.$$

Consequentemente, temos que definir a integral de $\mathbf{y}$ em um dado intervalo como

$$\int_a^b \mathbf{y}\,dx = \begin{pmatrix} \int_a^b y_1\,dx \\ \int_a^b y_2\,dx \\ \vdots \\ \int_a^b y_n\,dx \end{pmatrix}.$$

Integrais indefinidas são obtidas e forma semelhante. ♦

Exemplo 6.93. Seja

$$\mathbf{v} = \begin{pmatrix} x^2 + y \\ \operatorname{sen}(x) \\ xy \end{pmatrix},$$

onde y é uma constante (o vetor $\mathbf{v}$ contém funções de uma variável x). Temos

$$\frac{d}{dx}\mathbf{v} = \begin{pmatrix} \frac{d}{dx}(x^2 + y) \\ \frac{d}{dx}\operatorname{sen}(x) \\ \frac{d}{dx}xy \end{pmatrix} = \begin{pmatrix} 2x \\ \cos(x) \\ y \end{pmatrix}.$$

Também podemos integrar o vetor:

$$\int \mathbf{v}\,dx = \begin{pmatrix} \int x^2 + y\,dx \\ \int \operatorname{sen}(x)\,dx \\ \int xy\,dx \end{pmatrix} = \begin{pmatrix} \frac{x^3}{3} + xy \\ -\cos(x) \\ \frac{x^2 y}{2} \end{pmatrix}. \quad ◀$$

Considere o sistema de equações diferenciais lineares a seguir.

$$\begin{cases} y_1' = & a_{11}y_1 + a_{12}y_2 + \cdots + a_{1n}y_n \\ y_2' = & a_{21}y_1 + a_{22}y_2 + \cdots + a_{2n}y_n \\ \quad \vdots & \\ y_n' = & a_{11}y_1 + a_{22}y_2 + \cdots + a_{nn}y_n \end{cases}$$

Este sistema pode ser descrito em forma matricial, tendo as funções y_i como incógnitas:

$$A\mathbf{y} = \mathbf{y}',$$

onde

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & a_{2n} \\ \vdots & & \ddots & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, \quad \mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}, \quad \mathbf{y}' = \begin{pmatrix} y_1' \\ y_2' \\ \vdots \\ y_n' \end{pmatrix}.$$

Lema 6.94. *Seja $x \in \mathbb{R}$ e A uma matriz quadrada. Então*

$$\frac{d}{dx}e^{xA} = Ae^{xA}.$$

Demonstração.

$$\begin{aligned} \frac{d}{dx}e^{xA} &= \frac{d}{dx}\left(\mathcal{I} + \frac{xA}{1!} + \frac{x^2A^2}{2!} + \cdots\right) \\ &= A + \frac{xA^2}{1!} + \frac{x^2A^3}{2!} + \cdots \\ &= A\left(\mathcal{I} + \frac{xA}{1!} + \frac{x^2A^2}{2!} + \cdots\right) \\ &= Ae^{xA}. \end{aligned}$$

■

Teorema 6.95. *A solução geral para o sistema*

$$\frac{d}{dt}\mathbf{y}(t) = A\mathbf{y}(t)$$

com n variáveis e n é

$$\mathbf{y}(t) = e^{tA}\mathbf{y}(0).$$

Demonstração. Suponha que

$$\mathbf{y}(t) = e^{tA}\mathbf{y}(0).$$

Derivamos ambos os lados da equação, obtendo

$$\begin{aligned} \mathbf{y}'(t) &= \frac{d}{dt}e^{tA}\mathbf{y}(0) \\ &= Ae^{tA}\mathbf{y}(0) \\ &= A\mathbf{y}(t), && \text{(porque presumimos que } \mathbf{y}(t) = e^{tA}\mathbf{y}(0)) \end{aligned}$$

o que conclui a demonstração. ■

Para determinar a solução para um sistema de equações diferenciais lineares, calculamos e^{tA} da forma descrita na seção 6.6.4.

Exemplo 6.96. Considere o sistema dinâmico

$$\begin{aligned} y_1'(t) &= 2y_1(t) + 3y_2(t) \\ y_2'(t) &= 2y_1(t) + y_2(t). \end{aligned}$$

A matriz de coeficientes é

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

Os autovalores de A são 4 e -1, com autovetores $(1, 2/3)^T$ e $(1, -1)^T$, respectivamente. Já podemos diagonalizar A:

$$A = \begin{pmatrix} 1 & 1 \\ 2/3 & -1 \end{pmatrix} \begin{pmatrix} 4 & 0 \\ 0 & -1 \end{pmatrix} \frac{1}{5} \begin{pmatrix} 3 & 3 \\ 2 & -3 \end{pmatrix}.$$

A solução para $\frac{d}{dt}\mathbf{y}(t)A\mathbf{y}(t)$ é $\mathbf{y}(t) = e^{tA}\mathbf{y}(0)$, que calculamos agora:

$$\begin{aligned} e^{tA}\mathbf{y}(0) &= P^{-1}e^{tD}P\mathbf{y}(0) \\ &= \begin{pmatrix} 1 & 1 \\ 2/3 & -1 \end{pmatrix} \begin{pmatrix} e^{4t} & 0 \\ 0 & e^{-t} \end{pmatrix} \begin{pmatrix} 3/5 & 3/5 \\ 2/5 & -3/5 \end{pmatrix} \mathbf{y}(0) \\ &= \frac{1}{5} \begin{pmatrix} e^{-t}(3e^{5t} + 2) & e^{-t}(3e^{5t} - 3) \\ e^{-t}(2e^{5t} - 2) & e^{-t}(2e^{5t} + 3) \end{pmatrix} \mathbf{y}(0) \\ &= \frac{1}{5e^t} \begin{pmatrix} (3e^{5t} + 2)y_1(0) + (3e^{5t} - 3)y_2(0) \\ (2e^{5t} - 2)y_1(0) + (2e^{5t} + 3)y_2(0) \end{pmatrix} \end{aligned}$$

◀

O livro de Luiz Henrique Alves Monteiro [Mon02] é uma excelente introdução aos sistemas dinâmicos.

6.6.6 Cadeias de Markov [autovalor; autovetor]

Há uma descrição simplificada de Cadeias de Markov no apêndice α. Esta seção dá um tratamento mais rigoroso ao assunto.

Um *processo estocástico* é uma maneira de descrever a evolução de diversas variáveis aleatórias ao longo do tempo. Pode-se, por exemplo, descrever a evolução do DNA de uma população; do estado futuro de máquinas em uma indústria; do crescimento de populações, e diversos outros sistemas.

Usaremos como exemplo a modelagem, extremamente simplificada, da evolução de uma doença. Suponha que

Representamos o estado de um sistema em um processo estocástico como um vetor de estado. A evolução do sistema é descrita por uma sequencia de vetores de estado, onde cada um pode depender, probabilisticamente, dos anteriores.

Definição 6.97 (cadeia de Markov)**.** Se um sistema pode ser descrito em um dado momento t por um vetor de estados, e o estado no momento $t + 1$ depende apenas do estado no momento t e de probabilidades de transição entre estados, então a sequência de vetores de estado desse sistema é uma *cadeia de Markov*. ♦

Definição 6.98 (matriz de transição)**.** Se, para cada par de estados i, j, a probabilidade de transição de i para j é p_{ij}, então a *matriz de transição* da cadeia de Markov é dada por $(p_{i,j})$, ou

$$P = \begin{pmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{pmatrix}$$ ♦

Exemplo 6.99. A matriz

$$P = \begin{pmatrix} 0.2 & 0.1 & 0.7 \\ 0.1 & 0.5 & 0.4 \\ 0.6 & 0.2 & 0.2 \end{pmatrix}$$

representa as probabilidades de transição em uma cadeia de Markov com tres estados. ◀

Um *vetor estocástico* é um vetor que representa uma distribuição de probabilidades.

Definição 6.100 (vetor estocástico)**.** Um vetor $\mathbf{v} \in \mathbb{R}^n$ é *estocástico* se $\sum_i v_i = 1$, e todos os v_i são não-negativos. ♦

Exemplo 6.101. Os vetores $(1, 0, 0)^T$, $(1/2, 1/2, 0)^T$ e $(1/4, 0, 3/4, 0)^T$ são estocásticos. ◀

Definição 6.102 (matriz estocástica)**.** Uma matriz é *estocástica* se todas as suas linhas ou todas as suas colunas forem vetores estocásticos.

Se tanto as linhas como as colunas de uma matriz são vetors estocásticos, dizemos que a matriz é *duplamente estocástica.* ♦

Exemplo 6.103. A matriz de transição de qualquer cadeia de Markov é estocástica. Por exemplo, a matriz do exemplo 6.99 é uma matriz estocástica, porque só tem entradas positivas e a soma de cada linha é um. ◀

As matrizes de transição são operadores lineares, e o teorema 6.104 nos mostra como podemos usá-las.

Teorema 6.104. *Sejam A e B duas matrizes estocásticas, e $\mathbf{p}$ um vetor estocástico tais que os produtos AB e $A\mathbf{p}$ são bem definidos. Então AB também é uma matriz estocástica e $A\mathbf{p}$ é um vetor estocástico.*

O teorema 6.105 nos dá a interpretação da multiplicação de uma matriz de transição por um vetor estocástico.

Teorema 6.105. *Seja T a matriz de transição de uma cadeia de Markov, e $\mathbf{p}$ um vetor estocástico representando uma distribuição de probabilidades sobre os estados da cadeia. A matriz T, quando usada como operador linear em $\mathbf{p}$, leva à distribuição de probabilidades depois de um estágio.*

Demonstração. Seuponha que T seja estocástica nas colunas. A coluna j, portanto contém as probabilidades de, estando no estado j, haver transição para cada um dos outros estados – ou seja, a_{ij} é a probabilidade de haver transição para i quando o estado anterior era j. Então

$$\begin{aligned} T\mathbf{p} &= \begin{pmatrix} t_{11} & t_{12} & \cdots & t_{1n} \\ t_{21} & t_{22} & & t_{2n} \\ \vdots & & \ddots & \\ t_{n1} & t_{n2} & & t_{nn} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix} \\ &= \begin{pmatrix} t_{11}p_1 + t_{21}p_2 + \cdots + t_{n1}p_n \\ t_{12}p_1 + t_{22}p_2 + \cdots + t_{n2}p_n \\ \vdots \\ t_{n1}p_1 + t_{n2}p_2 + \cdots + t_{nn}p_n \end{pmatrix} \end{aligned}$$

$$= \begin{pmatrix} p_1(t_{11} + t_{21} + \cdots + t_{n1}) \\ p_2(t_{12} + t_{22} + \cdots + t_{n2}) \\ \vdots \\ p_n(t_{1n} + t_{2n} + \cdots + t_{nn}) \end{pmatrix}$$

Se a matriz é estocástica nas linhas, pode-se repetir o argumento com o operador à direita, $\mathbf{p}T = \mathbf{p}'$. ■

Fica claro então que podemos aplciar a matriz de transição T iteradamente para obter a distribuição de probabilidade sobre os estados após k estágios:

$$\underbrace{(T(T \cdots T(T\mathbf{p}) \cdots))}_{k \text{ aplicações}} = (TT \cdots T)\mathbf{p} = T^k\mathbf{p}.$$

Teorema 6.106. *Toda matriz estocástica tem um autovalor igual a um, e todos os outros autovalores são menores ou iguais a um.*

O vetor estocástico cuja existência o teorema 6.106 garante é chamado de *distribuição estacionária.*
De maneira geral, uma cadeia de Markov pode ter mais de uma distribuição estacionária

Exemplo 6.107. Se uma cadeia de Markov tem a matriz de transição

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

verificamos facilmente que há dois autovalores iguais a um, e que seus autovetores são

$$(1,0)^T \quad \text{e} \quad (0,1)^T.$$

Assim, as duas distribuições estacionárias são

$$\left(\frac{1}{2}, 0\right)^T \quad \text{e} \quad \left(0, \frac{1}{2}\right)^T. \qquad \blacktriangleleft$$

Exemplo 6.108. Na matriz de transição

$$\begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{3} & 0 & 0 \\ 0 & \frac{3}{4} & \frac{1}{4} \\ 0 & \frac{1}{5} & \frac{4}{5} \end{pmatrix}$$

o autovalor 1 tem multiplicidade algébrica dois, com os autovetores

$$(1,1,0,0)^T \quad \text{e} \quad (0,0,1,1)^T.$$

Assim, as duas distribuições estacionárias são

$$\left(\frac{1}{2}, \frac{1}{2}, 0, 0\right)^T \quad \text{e} \quad \left(0, 0, \frac{1}{2}, \frac{1}{2}\right)^T. \qquad \blacktriangleleft$$

Cadeias de Markov são descritas na literatura de probabilidade e processos estocásticos – por exemplo, o livro de Robert Ash [Ash08] dá uma breve introdução; os livros de Erhan Çinlar [Çin13] e de Pierre Bremaud [Bre08] tratam extensivamente do assunto.

6.6.7 Classificação de relevância (pagerank) [autovalor; autovetor]

Nos primeiros anos da Internet, havia uma grande quantidade de páginas disponíveis ao público, e muitos mecanismos de busca que indexavam estas páginas. Usuários podiam buscar palavras-chave e obter uma lista de páginas relacionadas com tais palavras.

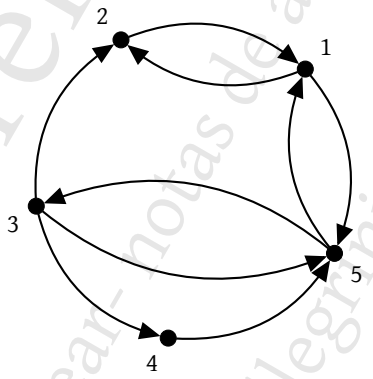
Um problema importante para aqueles mecanismos de busca era o de decidir em que ordem apresentar a lista – idealmente, as páginas mais relevantes seriam apresentadas primeiro, mas não era fácil definir a relevância de cada página.

O primeiro método a oferecer resultado satisfatório a este problema foi o algoritmo *pagerank*, cujo fundamento descrevemos a seguir.

Conceitualmente, a Internet pode ser vista como um *grafo dirigido* – ou seja, um grafo onde as arestas tem direção. Neste tipo de grafo, não definimos arestas como conjuntos de dois nós, e sim como par ordenado: a aresta (a, b) é diferente da aresta (b, a).

No grafo que representa a rede cada página é um nó, e uma aresta indo do nó a ao nó b significa que a página a tem um link para a página b.

Uma página relevante deve receber muitos links, portanto sua pontuação deve, de alguma forma, depender da quantidade de arestas que chegam a ela no grafo. O grafo a seguir é um exemplo, em pequena escala.



No entanto, não queremos que uma página tenha grande influência sobre a relevância das outras somente porque tem uma grande lista de links. Resolvemos isso determinando que, se uma página i tem k links para outras, cada um deles contribuirá com $n_i = 1/k$ para as páginas para onde estiverem apontando. Para o grafo mostrado na figura, temos

$$\begin{aligned} n_1 &= 1/2, \\ n_2 &= 1, \\ n_3 &= 1/3, \\ n_4 &= 1, \\ n_5 &= 1/2. \end{aligned}$$

A classificação de cada página i será dada então por um valor x_i, que é composto pela soma das influências das outras páginas: a_{i1} é a influência da página 1 sobre i; a_{i2} é a influência da página 2 sobre i, e assim

por diante. Para determinar a classificação das páginas, precisamos resolver o sistema a seguir.

$$\begin{array}{rcrcrcl} a_{11}x_1 + & & a_{12}x_2 + & \cdots + & a_{1n}x_n = & x_1 \\ a_{21}x_2 + & & a_{22}x_2 + & \cdots + & a_{2n}x_n = & x_2 \\ & & \vdots & & & \vdots \\ a_{n1}x_1 + & & a_{n2}x_2 + & \cdots + & a_{nn}x_n = & x_n, \end{array}$$

onde a_{ij} pode ser zero ou n_j. Usando a representação do sistema como matriz, podemos perceber que o que procuramos é um vetor $\mathbf{x}$ que satisfaça $A\mathbf{x} = \mathbf{x}$ – ou seja, um autovetor que pertença ao autovalor 1. Sabemos determinar autovalores e autovetores, portanto só nos resta definir o que fazer se a matriz não tiver o atovalor 1. Esta questão se resolve observando que cada coluna da matriz tem somatório igual a um.

O teorema 6.106 nos garante que sempre encontraremos o autovetor que contém a classificação (a demonstração é pedida no exercício 192).

A matriz de coeficientes do sistema para nosso exemplo é

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1/2 \\ 1/2 & 0 & 1/3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 1/3 & 0 & 0 \\ 1/2 & 0 & 1/3 & 1 & 0 \end{pmatrix}.$$

O autovalor 1 de A tem o autovetor $\frac{1}{8}(8, 5, 3, 1, 6)^T$. Este é o vetor de relevâncias.

$$\begin{aligned} x_1 &= 1, \\ x_2 &= 5/8 = 0.625, \\ x_3 &= 3/8 = 0.375, \\ x_4 &= 1/8 = 0.127, \\ x_5 &= 6/8 = 0.75. \end{aligned}$$

O nó mais relevante é o de número um; o segundo mais relevante, o de número cinco. Observe que ao contrário do que acontece com cadeias de Markov, não é necessário que o vetor de relevância seja estocástico: queremos apenas uma ordem de relevância entre os nós.

O algoritmo PageRank foi desenvolvido por Sergey Brin e Lawrence Page, fundadores da empresa Google [Pag+99]. Há diversas modificações e ajustes feitas posteriormente para que o método funcione bem na prática.

6.6.8 Cálculo de polinômio de matriz [polinômio característico; teorema de Cayley-Hamilton]

Suponha que precisemos calcular o valor de um polinômio t cujo argumento é uma matriz,

$$t(A),$$

e com grau menor que o do polinômio característico de A.

Seja p o polinômio característico de A. Podemos usar o algoritmo de Euclides para dividir t por p, obtendo q e r tais que

$$t(A) = p(A)q(A) + r(A).$$

Como $p(A) = 0$, temos

$$t(A) = r(A),$$

mas o grau de r é necessariamente menor que o de t. Repetindo este procedimento, obteremos o resultado mais rapiamente do que se tentássemos o cálculo direto.

Exemplo 6.109. Seja

$$t(x) = x^6 - 6x^5 + 15x^4 - 13x^3 + x.$$

e

$$A = \begin{pmatrix} 1 & -1 \\ 4 & 3 \end{pmatrix},$$

Para calcularmos $t(A)$, determinamos seu polinômio característico,

$$p(x) = \det(A - x\mathcal{I}) = x^2 - 4x + 7.$$

Agora dividimos t por p, e obtemos

$$t(x) = p(x)(x^4 - 2x^3) + x^3 + x,$$

e portanto

$$t(A) = A^3 + A.$$

Podemos dividir mais uma vez, e obtemos

$$t(A) = p(A)(A + 4) + 10A - 28\mathcal{I}.$$

Assim,

$$\begin{aligned} t(A) &= 10A - 28\mathcal{I} \\ &= \begin{pmatrix} -18 & -10 \\ 40 & 2 \end{pmatrix}. \end{aligned}$$

◀

6.6.9 Inversão de matrizes [polinômio característico; teorema de Cayley-Hamilton]

O teorema de Cayley-Hamilton nos permite, em algumas situações, encontrar a inversa de uma matriz de maneira rápida, se pudermos facilmente isolar A^{-1}.

Exemplo 6.110. Seja

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

com poliômio característico

$$p(x) = x^2 + x + 4.$$

Pelo Teorema de Cayley-Hamilton, temos

$$\begin{aligned} A^2 + A + 4\mathcal{I} &= 0 \\ A^2 + A &= -4\mathcal{I} \end{aligned}$$

$$A + \mathcal{I} = -4A^{-1}$$
$$-\frac{1}{4}(A + \mathcal{I}) = A^{-1}.$$

Calculamos

$$-\frac{1}{4}(A + \mathcal{I}) = -\frac{1}{4}\begin{pmatrix} 1 & 2 \\ -3 & -2 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$= -\frac{1}{4}\begin{pmatrix} 2 & 2 \\ -3 & -1 \end{pmatrix}.$$

E de fato, verificamos que

$$-\frac{1}{4}\begin{pmatrix} 1 & 2 \\ -3 & -2 \end{pmatrix}\begin{pmatrix} 2 & 2 \\ -3 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

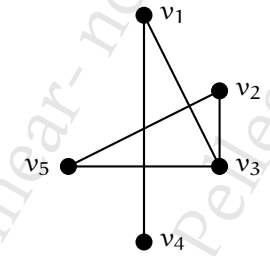
◀

★ 6.6.10 Grafos [autovalores]

A partir da descrição matricial de um grafo é possível extrair uma grande quantidade de informações a respeito dele. O polinômio característico, autovalores e autovetores do grafo, particularmente importantes, são objeto de estudo da *Teoria Espectral de Grafos* [Mie11; CDS80]. Nesta Seção apresentamos a matriz Laplaciana, fundamental na Teoria espectral de Grafos, e mostramos uma de suas aplicações mais elementares.

Definição 6.111 (Matriz de adjacência de grafo)**.** Seja $G = (V, E)$ um grafo. A *matriz de ajdacência* de G é a matriz A tal que $a_{ij} = 1$ se e somente se existe aresta entre os vértices i e j. ♦

Exemplo 6.112. Considere o grafo a seguir.



A matriz de ajdacencia deste grafo é

$$\begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

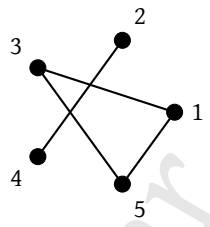
Como o grafo não é dirigido, a matriz é simétrica, já que (i, j) e (j, i) representam a mesma aresta. ◀

Definição 6.113 (Matriz Laplaciana de grafo)**.** Seja $G = (V, E)$ um grafo. A *matriz Laplaciana* de G é

$$L_G = D - A,$$

onde D é a matriz diagonal com d_{ii} igual ao grau do vértice i e A é a matriz de adjacência de G. ♦

Exemplo 6.114. A seguir temos um exemplo de grafo.



A matriz de adjacência deste grafo é

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

A diagonal com os graus é

$$D = \operatorname{diag}(2,1,2,1,2) = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

A matriz Laplaciana é, portanto,

$$L = D - A = \begin{pmatrix} 2 & 0 & -1 & 0 & -1 \\ 0 & 1 & 0 & -1 & 0 \\ -1 & 0 & 2 & 0 & -1 \\ 0 & -1 & 0 & 1 & 0 \\ -1 & 0 & -1 & 0 & 2 \end{pmatrix}$$ ◀

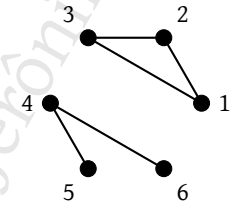
Teorema 6.115. *Todos os autovalores de qualquer grafo são não-negativos.*

Teorema 6.116. *A matriz Laplaciana de um grafo sempre tem zero como autovalor.*

Demonstração. Cada linha i contém o grau do vértice i, $d(i)$, na diagonal, mas também tem -1 repetido $d(i)$ vezes (uma para cada vizinho). Assim, a soma de cada linha é zero, e o Lema 4.27 nos garante que há linhas LD, e consequentemente $\det L_G = 0$, nos garantindo que zero é autovalor. ■

Definição 6.117 (Componente conexo)**.** Seja $G = (V, E)$ um grafo. Um *componente conexo* de G é um subgrafo de G onde, para quaisquer dois vértices diferentes $v, w \in V$, existe um caminho de v até w formado por arestas neste subgrafo. ♦

Exemplo 6.118. Considere o grafo a seguir.



Este grafo tem dois componentes conexos: um formado pelos vértices 1, 2, 3 e o outro pelos vértices 4, 5, 6. ◀

Definição 6.119 (Grafo conexo)**.** Um grafo é conexo se tem somente um componente conexo. ♦

Teorema 6.120. *Seja* G *um grafo. A quantidade de componentes conexos de* G *é igual à multiplicidade algébrica do autovalor zero de* L_G.

Demonstração. Os vértices podem ser reordenados de forma que a matriz de adjacência seja diagonal por blocos, onde cada bloco é a matriz de adjacência de um componente conexo.

$$A = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{pmatrix}$$

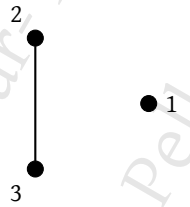
Cada A_k é a matriz de adjacência de um componente. A construção da Laplaciana não altera a estrutuda dos blocos.

$$L = \begin{pmatrix} L_1 & & & \\ & L_2 & & \\ & & \ddots & \\ & & & L_k \end{pmatrix}$$

Cada um dos blocos da matriz Laplaciana é, ele mesmo, uma matriz Laplaciana $L_i = D_i - A_i$ de um grafo conexo, e portanto cada bloco tem o autovalor zero com multiplicidade um. ■

Corolário 6.121. *Se* G *é um grafo conexo, a multiplicidade algébrica do autovalor zero em* L_G *é um.*

Exemplo 6.122. O grafo a seguir tem um vértice isolado e dois outros ligados por uma aresta. Tem, portanto, dois componentes conexos.



A matriz Laplaciana deste grafo é

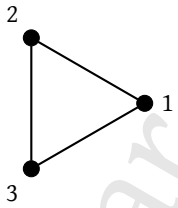
$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix},$$

e seus autovalores são

0 (multiplicidade 2)
2 (multiplicidade 1).

A multiplicidade do autovalor zero é dois, como esperávamos, já que o grafo tem dois componentes conexos. ◀

Exemplo 6.123. O grafo a seguir, chamado de K_3, é completo (ou seja, há arestas ligando cada vértice a todos os outros) e portanto tem um único componente conexo:



A matriz Laplaciana deste grafo é

$$\begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix},$$

e seus autovalores são

$$\begin{array}{l} 0 \text{ (multiplicidade 1)} \\ 3 \text{ (multiplicidade 2).} \end{array}$$

A multiplicidade do autovalor zero é um, já que o grafo tem um único componente conexo. ◀

Exercícios

Ex. 167 — Prove que o subespaço próprio da Definição 6.11 é de fato um subespaço de V.

Ex. 168 — Encontre os autovetores da matriz do exemplo 6.42.

Ex. 169 — Refute a recíproca do Teorema 6.34.

Ex. 170 — Demonstre o Teorema 6.24.

Ex. 171 — Identifique famílias de matrizes de ordem n cujos polinômios característicos tenham *exatamente*:

i) $n + 1$ termos

ii) n termos

iii) $n - 1$ termos

Ex. 172 — Quais as matrizes de ordem 2 que tem autovalores reais?

Ex. 173 — Quando matrizes de rotação são diagonalizáveis com autovalores reais?

Ex. 174 — Prove o Lema 6.22.

Ex. 175 — Quais são os autovalores de uma matriz quadrada anti-simétrica de ordem 2, com pelo menos uma entrada não-nula?

Ex. 176 — Calcule os autovalores e autovetores das matrizes. Para cada uma, diga se (ou quando) é diagonalizável.

$$\begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & k \\ -k & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix}, \quad \begin{pmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & b \end{pmatrix}, \quad \begin{pmatrix} a & 0 & 0 \\ 1 & a & 0 \\ 0 & 1 & b \end{pmatrix},$$

$$\begin{pmatrix} a & b & 0 \\ b & a & 0 \\ 0 & 0 & a-b \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 2 \\ 1 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 1 \\ 2 & 2 & 0 \\ 1 & 0 & -1 \end{pmatrix}.$$

Ex. 177 — Encontre uma matriz com autovalores -5 e 7, sendo que o autovalor -5 deve ter autovetores da forma $(1, -3/2)^T$, e o autovalor 7 deve ter autovetores da forma $(1, 3/2)^T$.

Ex. 178 — Diga para que ângulos θ a matriz a seguir tem autovalores reais. Comente o significado geométrico da matriz e dos autovalores reais que calculou.

$$\begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{pmatrix}$$

Ex. 179 — Para cada matriz do exercício 176, diagonalize ou mostre porque não é possível.

★ **Ex. 180 —** Calcule os autovalores, os autovetores e diagonalize (se possível) os seguintes operadores lineares. A primeira é em $\mathbb{Z}_2^2$, e o segundo é em $\mathbb{Z}_2^3$.

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

Ex. 181 — Diga se os operadores são simultaneamente diagonalizáveis, e quando forem, mostre a base que os torna diagonais.

i)

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & -4 \\ 0 & -1 \end{pmatrix}$$

ii)

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 5 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & -4 \\ 0 & -1 \end{pmatrix}$$

Ex. 182 — Determine x e y para que A e B sejam simultaneamente diagonalizáveis.

$$A = \begin{pmatrix} -2 & 2 \\ 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & x \\ 1 & y \end{pmatrix}$$

Ex. 183 — Calcule os autovalores, os autovetores e diagonalize (se possível) os seguintes operadores lineares. A primeira é em $\mathbb{C}^2$, e o segundo é em $\mathbb{Q}[\sqrt{2}]^2$.

$$A = \begin{pmatrix} i & -1 \\ -i & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & -\sqrt{2} \\ 0 & 2+2\sqrt{2} \end{pmatrix}$$

Ex. 184 — Considere a sequência definida pela recorrência

$$\begin{aligned} a_0 &= 1, \\ a_1 &= 2, \\ a_2 &= 5, \\ a_n &= a_{n-1} - 2a_{n-2} + 2a_{n-3} \end{aligned}$$

Mostre a matriz associada a esta recorrência, o polinômio característico, e os autovetores.

Ex. 185 — Para cada sistema de equações de diferença, escreva $\mathbf{x}(t)$ em função de $\mathbf{x}(0)$:

$$\begin{aligned} x_1(t) &= 3x_1(t-1) - x_2(t-1) \\ x_2(t) &= -x_2(t-1) + 3x_2(t-1) \end{aligned}$$

$$\begin{aligned} x_1(t) &= -2x_1(t-1) + x_2(t-1) \\ x_2(t) &= 3x_2(t-1) - 2x_2(t-1) \end{aligned}$$

Ex. 186 — Dê a solução geral para os sistemas de equações diferenciais a seguir.

$$\begin{aligned} y_1' &= 2y_1 - 2y_2 \\ y_2' &= -3y_2 + y_2 \end{aligned}$$

$$\begin{aligned} y_1' &= 2y_1 - 2y_2 \\ y_2' &= -3y_1 + y_2 - y_3 \\ y_3' &= -y_1 - y_2 - y_3 \end{aligned}$$

Ex. 187 — Prove o teorema 6.104.

Ex. 188 — Prove (usando exemplos pequenos) que uma matriz estocástica pode ter:

i) Determinante zero

ii) Autovalores zero

iii) Determinante negativo

iv) Autovalores complexos

Ex. 189 — Prove que uma matriz estocástica pode não ser diagonalizável.

Ex. 190 — Prove que uma matriz estocástica de ordem 2 com entradas estritamente positivas sempre tem um autovalor menor que um (ou seja, a multiplicidade do autovalor um é exatamente um).

Ex. 191 — Fixado n, o conjunto das matrizes complexas de ordem n formam um espaço vetorial sobre $\mathbb{C}$? E sobre $\mathbb{R}$?

Ex. 192 — Prove o teorema 6.106.

Ex. 193 — Prove que se a matriz de transição de uma cadeia de Markov é simétrica, a distribuição uniforme é estacionária.

Ex. 194 — Considere a cadeia de Markov com tres estados onde não acontecem transições de um estadoa outro: a probabilidade de se permanecer no mesmo estado é sempre 1. A matriz de transição desta cadeia é $\mathcal{I}_3$, que tem somente o autovalor 1, com multiplicidade 3. Os autovetores são

$$(1,0,0)^T$$
$$(0,1,0)^T$$
$$(0,0,1)^T,$$

que são três distribuições estacionárias. No entanto, como a matriz de transição é igual à identidade, *qualquer* outra distribuição também será estacionária. Explique porque só encontramos três distribuições quando calculamos os autovetores.

Ex. 195 — A matriz usada no *pagerank* (na seção 6.6.7) é uma matriz "estocástica". Isso significa que deve haver alguma interpretação probabilística para o vetor obtido pelo algoritmo. Descreva esta interpretação, e diga o que teria que ser feito com os vetores de relevância.

Ex. 196 — Prove que se o maior grau de vértice um grafo G é k, então k é maior que o módulo do maior autovalor da matriz de adjacência de G.

★ **Ex. 197 —** Prove que o conjunto de autovalores e uma base de autovetores determina completamente e unicamente um grafo.

★ **Ex. 198 —** suponha que um grafo G seja regular (todos os vértices tem o mesmo grau). Prove que o vetor $(1,1,\ldots,1)^T$ é autovetor de G, e diga a que autovalor ele pertence.

★ **Ex. 199 —** Tente diagonalizar o operador do exemplo 4.14, e explicite as dificuldades que encontrar.

★ **Ex. 200 —** Escolha um operador linear no espaço de ciclos de um grafo com pelo menos 5 ciclos diferentes, e tente diagonalizá-lo. Que semelhança este exercício tem com o exercício 199?

Ex. 201 — Prove que

i) Se Z é a matriz zero, $e^Z = \mathcal{I}$.

ii) $e^A e^{-A} = \mathcal{I}$.

iii) Se A e B são de mesma ordem e $AB = BA$, então $e^A e^B = e^B e^A = e^{(A+B)}$.

iv) Para toda matriz quadrada A, e^A tem inversa.

v) Para toda matriz quadrada A, $(e^A)^{-1} = e^{-A}$.

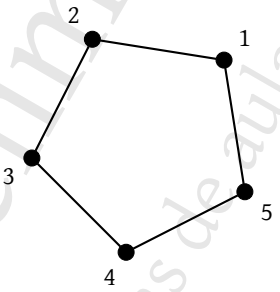
Ex. 202 — Mostre que para qualquer matriz A complexa, $\det e^A = e^{\mathrm{Tr}(A)}$.

Ex. 203 — Mostre que para qualquer matriz real A, $\mathrm{Tr}\, A = \log(\det(e^A))$.

★ **Ex. 204 —** Mostre que os autovalores de A^H são os conjugados dos autovalores de A.

★ **Ex. 205 —** Seja G um grafo com n vértices. Mostre que a soma dos autovalores de L_G é menor ou igual a n.

★ **Ex. 206 —** Denotamos por C_n o grafo que consiste somente de um ciclo com n vértices. Por exemplo, C_5 é mostrado a seguir.



Como é, de maneira geral, a matriz Laplaceana de C_n? O que se pode dizer sobre seus autovalores?

Capítulo 7

Produto Interno

Nos outros Capítulos trabalhamos com espaços vetoriais sobre corpos quaisquer. Neste Capítulo nos restringimos a espaços sobre o corpo dos números reais (há uma seção que discorre muito brevemente sobre a extensão dos conceitos abordados aqui para espaços complexos).

7.1 Produto interno e norma

Definição 7.1 (Produto interno)**.** Um *produto interno* em um espaço vetorial V *sobre* $\mathbb{R}$ é uma função de $V \times V$ em $\mathbb{R}$, que denotamos por[1] $\langle \mathbf{u}, \mathbf{v} \rangle$, com as propriedades a seguir.

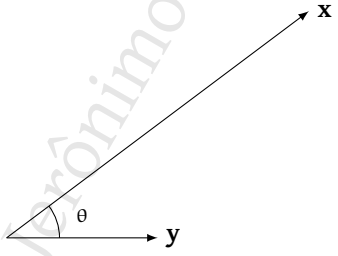
- **comutatividade** (ou **simetria**): $\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle$
- **positividade:** $\langle \mathbf{v}, \mathbf{v} \rangle \geq 0$, e $\langle \mathbf{0}, \mathbf{0} \rangle = 0$.
- **bilinearidade:** o produto interno é linear em seu primeiro argumento (e como é comutativo, é também linear no segundo argumento) – para todo escalar k e vetores $\mathbf{u}, \mathbf{v}, \mathbf{w}$,

$$\langle \mathbf{u} + \mathbf{w}, \mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{w}, \mathbf{v} \rangle$$
$$\langle k\mathbf{v}, \mathbf{w} \rangle = k \langle \mathbf{v}, \mathbf{w} \rangle$$ ♦

Exemplo 7.2. Em $\mathbb{R}^2$, é usual definir o produto de dois vetores como

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + x_2 y_2,$$

que geometricamente é o produto das magnitudes de $\mathbf{x}$ e $\mathbf{y}$, e do cosseno do ângulo entre eles.



[1] Também é comum denotar o produto interno por $(\mathbf{u}, \mathbf{v})$, ou por $\langle \mathbf{u} | \mathbf{v} \rangle$.

$$\langle \mathbf{x}, \mathbf{y} \rangle = \|\mathbf{x}\| \, \|\mathbf{y}\| \cos\theta$$

Assim, o produto de $(1,-2)^T$ com $(-1,1)^T$ é

$$\left\langle (1,-2)^T, (-1,1)^T \right\rangle = (1)(-1) + (-2)(1) = -3.$$

Podemos verificar que $\langle \mathbf{x}, \mathbf{y} \rangle$ definido desta forma é realmente produto interno:

- Claramente, $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$.
- $\langle \mathbf{x}, \mathbf{y} \rangle$ é positivo:

  $$\langle \mathbf{0}, \mathbf{0} \rangle = 0 \times 0 + 0 \times 0 = 0.$$

  e

  $$\langle \mathbf{x}, \mathbf{x} \rangle = x_1 x_1 + x_2 x_2 = x_1^2 + x_2^2 \geq 0.$$

- É bilinear. Verificamos a multiplicação por escalar,

  $$\begin{aligned} \langle a\mathbf{x}, \mathbf{y} \rangle &= (ax_1, ax_2)^T (y_1, y_2)^T \\ &= ax_1 y_1 + ax_2 y_2 \\ &= a(x_1 y_1 + x_2 y_2 \\ &= a \langle \mathbf{x}, \mathbf{y} \rangle , \end{aligned}$$

  e a soma,

  $$\begin{aligned} \langle \mathbf{x} + \mathbf{z}, \mathbf{y} \rangle &= (x_1 + z_1, x_2 + z_2)^T (y_1, y_2)^T \\ &= (x_1 + z_1) y_1 + (x_2 + z_2) y_2 \\ &= x_1 y_1 + z_1 y_1 + x_2 y_2 + z_2 y_2 \\ &= \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{z}, \mathbf{y} \rangle . \end{aligned}$$

  ◀

Este não é o único produto interno em $\mathbb{R}^2$.

Exemplo 7.3. Em $\mathbb{R}^2$, $\langle \mathbf{x}, \mathbf{y} \rangle = 2x_1 y_1 + 3x_2 y_2$ também é produto interno.

i) é comutativo

ii) é positivo:

$$\begin{aligned} \langle \mathbf{x}, \mathbf{x} \rangle &= 2x_1 x_1 + 3x_2 x_2 \\ &= 2x_1^2 + 3x_2^2 \\ &\geq 0. \end{aligned}$$

Além disso, $\langle \mathbf{0}, \mathbf{0} \rangle = 0$.

iii) é bilinear:

$$\begin{aligned} \langle k\mathbf{v}, \mathbf{w} \rangle &= 2kv_1 w_1 + 3kv_2 w_2 \\ &= k(2kv_1 w_1 + 3kv_2 w_2) \\ &= k \langle \mathbf{v}, \mathbf{w} \rangle . \end{aligned}$$

E

$$\begin{aligned}\langle \mathbf{u}+\mathbf{v}, \mathbf{w}\rangle &= 2(u_1+v_1)w_1 + 3(u_2+v_2)w_2 \\ &= 2u_1w_1 + 2v_1w_1 + 3u_2w_2 + 3v_2w_2 \\ &= \left(2u_1w_1 + 3u_2w_2\right) + \left(2v_1w_1 + 3v_2w_2\right) \\ &= \langle \mathbf{u}, \mathbf{w}\rangle + \langle \mathbf{v}, \mathbf{w}\rangle .\end{aligned}$$ ◀

Exemplo 7.4. Em $\mathbb{R}^n$, uma função usual de produto interno é

$$\langle \mathbf{u}, \mathbf{v}\rangle = \mathbf{u}^T\mathbf{v} = \sum_i u_i v_i.$$

Pode-se verificar facilmente que este produto é comutativo, bilinear e positivo. ◀

Exemplo 7.5. Em $\mathbb{R}^2$, $\langle \mathbf{v}, \mathbf{w}\rangle = (v_1+w_1)(v_2+w_2)$ *não* é produto interno.

i) é comutativo:

$$\begin{aligned}\langle \mathbf{v}, \mathbf{w}\rangle &= (v_1+w_1)(v_2+w_2) \\ &= (w_1+v_1)(w_2+v_2) \\ &= \langle \mathbf{w}, \mathbf{v}\rangle\end{aligned}$$

ii) *não* é positivo:

$$\begin{aligned}\langle \mathbf{v}, \mathbf{v}\rangle &= (v_1+v_1)(v_2+v_2) \\ &= 4v_1v_2,\end{aligned}$$

que pode ser menor que zero.

iii) *não* é bilinear:

$$\langle k\mathbf{v}, \mathbf{w}\rangle = (kv_1+w_1)(kv_2+w_2),$$

que de maneira geral não é igual a $k\langle \mathbf{v}, \mathbf{w}\rangle$. ◀

Exemplo 7.6. Obteremos neste exemplo um produto interno para espaço de funções. Embora possamos escolher qualquer produto interno que satisfaça a definição 7.1, construiremos uma definição de produto interno particularmente interessante para espaços de funções – uma definição análoga à de produto interno em $\mathbb{R}^n$. Escolhemos para o exemplo o espaço $C^0[0,1]$, embora seja claro que o desenvolvimento é também válido para outros espaços de funções.

Sejam f e g funções em $C^0[0,1]$, o espaço das funções contínuas no intervalo $[0,1]$. Podemos dividir o intervalo $[0,1]$ em n subintervalos iguais, como em uma soma de Riemann, e sabemos que quando $n \to \infty$

$$\sum_{i=0}^{n} f(i)g(i)\Delta x \to \int_0^1 f(x)g(x)dx,$$

com $\Delta x = 1/n$.

Podemos reescrever $f(i) = a_i$ e $g(i) = b_i$, e teremos dois vetores com os valores das funções em $1, 1+\delta, 1+2\delta, \ldots$.

$$f^* : (a_1, a_2, \ldots, a_n)^T$$
$$g^* : (b_1, b_2, \ldots, b_n)^T$$

O produto interno destes dois vetores é $\sum a_i b_i$, que é semelhante à soma de Riemann que resulta na integral de $f(x)g(x)$:

$$\Delta x \sum_{i=1}^{n} a_i b_i \to \int_0^1 f(x)g(x)dx.$$

Por isso seria interessante definir o produto interno em $C^0[0,1]$ como

$$\langle f, g\rangle = \int_0^1 f(x)g(x)dx.$$

No entanto, esta integral pode ser divergente (por exemplo, se $f(x) = x^{-1}$ e $g(x) = 1$, temos $\langle f, g\rangle = \int_0^1 \frac{1}{x}dx$, que é divergente.

Podemos usar este produto para o subespaço de $C^0[0,1]$ composto pelas funções f tais que

$$\int_0^1 f(x)dx$$

não diverge. Este é de fato um subespaço, porque (i) a função constante zero é integrável em qualquer intervalo; (ii) a multiplicação por escalar não pode fazer uma integral divergir, e (iii) se tanto f como g são integráveis em algum intervalo, $f + g$ também é. ◀

Exemplo 7.7. As funções $f(x) = 2x$ e $g(x) = \cos(x)$ são definidas no espaço de funções contínuas $C[0,\pi]$. O produto interno destas funções neste espaço é

$$\begin{aligned}\langle f, g\rangle &= \int_0^{\pi} 2x\cos(x)dx \\ &= 2(x\,\mathrm{sen}\,x + \cos x)\Big|_0^{\pi} \\ &= -4.\end{aligned}$$

Veja que se mudarmos o intervalo para, por exemplo, $C[0,\pi/2]$, teremos mudado o espaço vetorial em que trabalhamos, e o produto interno também muda:

$$\begin{aligned}\langle f, g\rangle &= \int_0^{\pi/2} 2x\cos(x)dx \\ &= 2(x\,\mathrm{sen}\,x + \cos x)\Big|_0^{\pi/2} \\ &= \pi - 2.\end{aligned}$$ ◀

Exemplo 7.8. No espaço $M_{n\times n}$, o produto de Frobenius, denotado $A : B$, é um produto interno:

$$\langle A, B\rangle = A : B = \sum_i \sum_j a_{ij} b_{ij}.$$

Se

$$A = \begin{pmatrix} 1 & -2 \\ 3 & 3 \end{pmatrix} B = \begin{pmatrix} 1 & 1 \\ 0 & -2 \end{pmatrix}$$

então

$$\langle A, B \rangle = A : B = (1)(1) + (-2)(1) + (3)(0) + (3)(-2) = -7. \quad \blacktriangleleft$$

★ **Exemplo 7.9.** No espaço $M_{n\times n}$,

$$\langle A, B \rangle = \text{maior autovalor de } A^T B$$

é produto interno:

i) *comutatividade:* os autovalores de A^T e A são os mesmos, assim como os de B^T e B. Desta forma, os autovalores de $A^T B$ e de $B^T A$ também são os mesmos

ii) *positividade:* seja Z a matriz zero. Então $Z^T Z = Z$, que só tem autovalores zero. Além disso, os autovalores de $A^T A$ são todos positivos.

iii) *bilinearidade:* vemos claramente que como

$$(A + C)^T B = A^T B + C^T B,$$

e os autovalores da soma de dois operadores são as somas dos autovalores, temos

$$\langle A + C, B \rangle = \langle A, B \rangle + \langle C, B \rangle .$$

Também observamos que

$$(kA)^T B = k(A^T B).$$

Como a multiplicação do operador por k também multiplica todos seus autovalores por k, temos $\langle kA, B \rangle = k \langle A, B \rangle$. $\blacktriangleleft$

Exemplo 7.10. No espaço $M_{n\times n}$, a multiplicação de matrizes *não* é produto interno, porque (i) não é função de $M_{n\times n} \times M_{n\times n}$ em $\mathbb{R}$; e (ii) porque a operação não é comutativa. $\blacktriangleleft$

Exemplo 7.11. No espaço $M_{n\times n}$, a função $f(A, B) = \det(AB)$ *não* é produto interno. Verificamos as propriedades:

i) vale a comutatividade: $\det(AB) = \det(A)\det(B) = \det(BA)$.

ii) vale a positividade: $\det(AA) = \det(A)\det(A) = [\det(A)]^2 > 0$, e $\det(0 \cdot 0) = 0$.

iii) a função *não* é bilinear:

$$\begin{aligned} \langle kA, B \rangle &= \det(kAB) \\ &= \det(kA)\det(B) \\ &= k^n \det(A)\det(B) \\ &= k^n \langle A, B \rangle . \end{aligned}$$ $\blacktriangleleft$

Exemplo 7.12. Damos agora um exemplo de dois produtos internos diferentes no mesmo espaço vetorial.

No espaço $\mathbb{R}_n[x]$, de polinômios com grau menor ou igual a n, sejam

$$p(x) = a_n x^n + a_{n-1}x_{n-1} + \cdots + a_1 x_1 + a_0$$
$$q(x) = b_n x^n + b_{n-1}x_{n-1} + \cdots + b_1 x_1 + b_0.$$

Definimos os dois produtos

$$\langle p, q\rangle_1 = \sum_{i=0}^{n} a_i b_i$$
$$\langle p, q\rangle_2 = \int_0^1 p(x)q(x)dx$$

Os dois são de fato produtos internos, porque são comutativos, positivos e bilineares, mas são completamente diferentes.

Exemplificamos com dois polinômios em $\mathbb{R}_2[x]$:

$$p = x^2 - x$$
$$q = 4x^2 + 2$$

Então,

$$\langle p, q\rangle_1 = (0)(2) + (-1)(0) + (1)(4) = 4$$
$$\langle p, q\rangle_2 = \int_0^1 p(x)q(x)dx = -\frac{8}{15}.$$ ◀

★ **Exemplo 7.13.** Considere o conjunto de todas as sequências (a_n) tais que

$$\sum_{i=1}^{\infty} |a_i|^2$$

converge (observe que usamos $|a_i|^2$, e não simplesmente a_i^2, porque a_i pode ser complexo). Chamamos este espaço de ℓ_2. Este conjunto é um subespaço do espaço de sequencias. Por exemplo, considere a sequencia

$$a_n = 1/n.$$

Podemos verificar facilmente que $|(a_n)|^2$ converge:

$$\sum_{i=1}^{\infty} |a_i|^2 = \frac{\pi^2}{6},$$

portanto $(a_n) \in \ell_2$.

ℓ_2 tem dimensão infinita, porque as sequências tem comprimento (quantidade de termos) infinito. Apesar disso, podemos identificar uma base para este espaço: o conjunto (infinito) de sequências

$$(1, 0, 0, \ldots)$$

$$(0,1,0,\ldots)$$
$$(0,0,1,\ldots)$$
$$\vdots$$

ou seja, as sequências onde somente um termo é igual a um, e os outros são zero.

A sequência $a_n = x^2$, por exemplo, pode ser expressa como a combinação linear infinita

$$\begin{aligned} &1\ (1,0,0,0,\ldots)\\ &+4\ (0,1,0,0,\ldots)\\ &+9\ (0,0,1,0,\ldots)\\ &+\vdots \end{aligned}$$

Em ℓ_2, definimos

$$\langle (a_n), (b_n) \rangle = \sum_{i=1}^{\infty} a_i b_i,$$

que é produto interno.

Exemplificamos com duas sequências:

$$(a_n) = \frac{1}{n!}$$
$$(b_n) = \frac{1}{2^n}$$

O produto interno das duas sequências é

$$\langle (a_n), (b_n) \rangle = \sum_{i=1}^{\infty} a_i b_i = \sum_{i=1}^{\infty} \frac{1}{n!2^n} = \sqrt{e} - 1. \qquad \blacktriangleleft$$

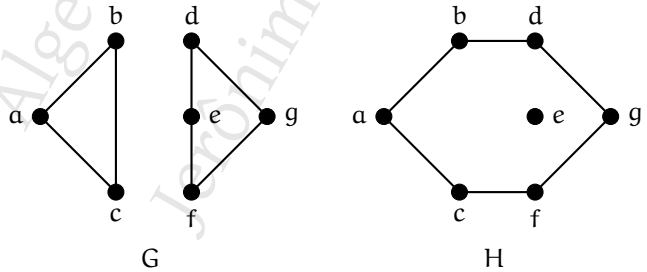
★ **Exemplo 7.14.** No espaço de ciclos de um grafo (definido no exemplo 1.41, página 20), definimos o produto interno de dois grafos de ciclos disjuntos da seguinte maneira. Sejam **c** e **d** os vetores característicos dos dois grafos. Então

$$\langle C, D \rangle = \sum c_i \wedge d_i,$$

onde a soma é em $\mathbb{R}$, não em $\mathbb{Z}_2$. Claramente, f dá o número de arestas em comum dos dois grafos.

Sejam G e H os grafos a seguir.

$$V = \{a, b, c, d, e, f, g\}$$
$$E(G) = \{(a,b), (b,c), (c,a), (d,e), (e,f), (f,g), (g,d)\}$$
$$E(H) = \{(a,b), (b,d), (d,g), (g,f), (f,c), (c,a)\}$$



Os vetores característicos de arestas de G, H, e o valor de $g_i \wedge h_i$ são

aresta	G	H	$g_i \wedge h_i$
$\{a, b\}$	1	1	1
$\{a, c\}$	1	1	1
$\{a, d\}$	0	0	0
$\{a, e\}$	0	0	0
$\{a, f\}$	0	0	0
$\{a, g\}$	0	0	0
$\{b, c\}$	1	0	0
$\{b, d\}$	0	1	0
$\{b, e\}$	0	0	0
$\{b, f\}$	0	0	0
$\{b, g\}$	0	0	0
$\{c, d\}$	0	0	0
$\{c, e\}$	0	0	0
$\{c, f\}$	0	1	0
$\{c, g\}$	0	0	0
$\{d, e\}$	1	0	0
$\{d, f\}$	0	0	0
$\{d, g\}$	1	1	1
$\{e, f\}$	1	0	0
$\{e, g\}$	0	0	0
$\{f, g\}$	1	1	1

O produto de G com H é, portanto,

$$\langle G, H \rangle = \sum_i g_i \wedge h_i = 4. \qquad \blacktriangleleft$$

Teorema 7.15 (Desigualdade de Cauchy-Schwarz-Bunyakovsky)**.** *Seja V um espaço vetorial com produto interno, e $\mathbf{u}, \mathbf{v} \in V$. Então*

$$\langle \mathbf{u}, \mathbf{w} \rangle^2 \leq \langle \mathbf{u}, \mathbf{u} \rangle \langle \mathbf{w}, \mathbf{w} \rangle .$$

Demonstração. Seja k um escalar. Então

$$\langle k\mathbf{u} + \mathbf{w}, k\mathbf{u} + \mathbf{w} \rangle \geq 0$$

Mas

$$\begin{aligned} \langle k\mathbf{u} + \mathbf{w}, k\mathbf{u} + \mathbf{w} \rangle &= \langle k\mathbf{u}, k\mathbf{u} + \mathbf{w} \rangle + \langle \mathbf{w}, k\mathbf{u} + \mathbf{w} \rangle \\ &= \big(\langle k\mathbf{u}, k\mathbf{u} \rangle + \langle k\mathbf{u}, \mathbf{w} \rangle \big) + \big(\langle \mathbf{w}, k\mathbf{u} \rangle + \langle \mathbf{w}, \mathbf{w} \rangle \big) \\ &= k^2 \langle \mathbf{u}, \mathbf{u} \rangle + 2k \langle \mathbf{u}, \mathbf{w} \rangle + \langle \mathbf{w}, \mathbf{w} \rangle . \end{aligned}$$

Temos então

$$\langle \mathbf{u}, \mathbf{u} \rangle k^2 + 2 \langle \mathbf{u}, \mathbf{w} \rangle k + \langle \mathbf{w}, \mathbf{w} \rangle \geq 0.$$

O lado esquerdo da equação define um polinômio do segundo grau, com $a = \langle \mathbf{u}, \mathbf{u} \rangle$, $b = 2\langle \mathbf{u}, \mathbf{w} \rangle$ e $c = \langle \mathbf{w}, \mathbf{w} \rangle$. Como a desigualdade determina que este polinômio tenha valor maior que zero, ele não pode ter soluções diferentes (a parábola pode tocar o eixo das abscissas, mas não pode ter pontos abaixo dele). Assim, seu discriminante, $b^2 - 4ac$, não pode ser positivo:

$$\begin{aligned} (2\langle \mathbf{u}, \mathbf{w} \rangle)^2 - 4(\langle \mathbf{u}, \mathbf{u} \rangle \langle \mathbf{w}, \mathbf{w} \rangle) &\leq 0 \\ \langle \mathbf{u}, \mathbf{w} \rangle^2 - \langle \mathbf{u}, \mathbf{u} \rangle \langle \mathbf{w}, \mathbf{w} \rangle &\leq 0 \\ \langle \mathbf{u}, \mathbf{w} \rangle^2 &\leq \langle \mathbf{u}, \mathbf{u} \rangle \langle \mathbf{w}, \mathbf{w} \rangle . \end{aligned}$$ ■

Proposição 7.16. *A desigualdade de Cauchy-Schwarz-Bunyakovsky se reduz a uma igualdade se os vetores são LI.*

Definição 7.17 (Norma)**.** A *norma* de um vetor[2] $\mathbf{v}$, denotada por $\|\mathbf{v}\|$, é igual a $\sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}$. ♦

Exemplo 7.18. Em $\mathbb{R}^n$, se usarmos o produto usual, $\langle \mathbf{x}, \mathbf{y} \rangle$, a norma será

$$\begin{aligned} \|\mathbf{x}\| &= \sqrt{\mathbf{x}^T \mathbf{x}} \\ &= \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}. \end{aligned}$$ ◀

Exemplo 7.19. No espaço $C^0[0, 1]$ de funções contínuas com o produto definido no exemplo 7.6, a norma de uma função é

$$\|f\| = \sqrt{\int_0^1 (f(x))^2 dx}.$$ ◀

Exemplo 7.20. Se o produto for dado por $\langle A, B \rangle = \sum_i \sum_j a_{ij} b_{ij}$ como no exemplo 7.8, temos a *norma de Frobenius*,

$$\|A\| = \sqrt{\sum_i \sum_j a_{ij}^2}.$$ ◀

★ **Exemplo 7.21.** No espaço de matrizes quadradas com entradas complexas, se usarmos o produto interno

$$\langle A, B \rangle = \text{maior autovalor de } A^H B,$$

teremos a norma

$$\|A\|_2 = \sqrt{\text{maior autovalor de } A^H A}.$$

Para matrizes reais podemos usar A^T ao invés de A^H. ◀

Exemplo 7.22. Sejam

$$A = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 1 \\ 3 & 1 \end{pmatrix}$$

Os autovalores das matrizes são:

$$\begin{aligned} A &: -1, 1 \\ B &: -2, 2 \end{aligned}$$

[2] Na verdade esta é apenas *uma* norma. Pode-se definir várias outras, como por exemplo $\|\mathbf{x}\|_p = \sqrt[p]{\sum_1^n |x_i|^p}$, para $p > 0$.

Para calcular a norma de Frobenius, temos

$$\|A\| = \sqrt{1^2 + 2^2 + (-1)^2} = \sqrt{6}.$$
$$\|B\| = \sqrt{(-1)^2 + 1^2 + 3^2 + 1^2} = \sqrt{12} = 2\sqrt{3}.$$

As normas são, portanto,

$$\|A\|_2 = 1 \qquad \|A\| = \sqrt{6}$$
$$\|B\|_2 = 2 \qquad \|B\| = 2\sqrt{3}$$ ◀

★ **Exemplo 7.23.** Usando o produto interno do exemplo 7.14, facilmente verificamos que a norma nos dá a quantidade de arestas no grafo de ciclos. ◀

★ **Exemplo 7.24.** Em ℓ_2, usaremos o produto interno

$$\langle (a_n), (b_n) \rangle = \sum_{i=1}^{\infty} a_i b_i.$$

Calculamos a norma da sequência (b_n) do exemplo 7.13.

$$(b_n) = \frac{1}{2^n}$$

A norma de (b_n) é

$$\sqrt{\sum_{i=1}^{\infty} b_i^2} = \sqrt{\sum_{i=1}^{\infty} (2^{-i})^2} = \frac{1}{\sqrt{3}}.$$ ◀

Definição 7.25 (Distância entre vetores)**.** A *distância* entre dois vetores $\mathbf{v}$ e $\mathbf{w}$, é $d(\mathbf{v}, \mathbf{w}) = \|\mathbf{v} - \mathbf{w}\|$. ♦

Fica evidente que $d(\mathbf{v}, \mathbf{v}) = 0$.

Exemplo 7.26. Usando o produto usual em $\mathbb{R}^n$, a distância é dada por

$$d(\mathbf{x}, \mathbf{y}) = \sqrt{(\mathbf{x} - \mathbf{y})^T (\mathbf{x} - \mathbf{y})}.$$ ◀

Exemplo 7.27. No espaço $C^0[0, 1]$ de funções contínuas com o produto definido no exemplo 7.6, a distância entre duas funções é

$$\begin{aligned} d(f, g) &= \sqrt{\langle f - g, f - g \rangle} \\ &= \sqrt{\int_0^1 (f(x) - g(x))^2 dx}. \end{aligned}$$

Mais concretamente, se $f(x) = x$ e $g(x) = e^x$, então

$$d(f, g) = \sqrt{\int_0^1 (f(x) - g(x))^2 dx}$$

$$= \sqrt{\int_0^1 (x - e^x)^2 dx}$$
$$= \sqrt{\frac{3e^2 - 13}{6}}$$
$$= 1.2360669006160 86\ldots$$ ◀

Exemplo 7.28. Com o produto $(A, B) = A : B = \sum_i \sum_j a_{ij} b_{ij}$ do exemplo 7.8, a distância entre duas matrizes é

$$d(A, B) = \sqrt{(A - B) : (A - B)}$$
$$= \sqrt{\sum_i \sum_j (a_{ij} - b_{ij})^2}.$$

Para um exemplo concreto, tomemos

$$A = \begin{pmatrix} 1 & 0 & 4 \\ -3 & 1 & 0 \\ 2 & 1 & 5 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 0 & 3 \\ 2 & 0 & 1 \\ -5 & 1 & 5 \end{pmatrix}.$$

Primeiro calculamos

$$\sum_i \sum_j (a_{ij} - b_{ij})^2 = (1-3)^2 + (4-3)^2 + (-3-2)^2 + (1-0)^2 + (0-1)^2 + (2+5)^2$$
$$= 4 + 1 + 25 + 1 + 1 + 49 = 81.$$

A distância entre A e B é, portanto,

$$\sqrt{\sum_i \sum_j (a_{ij} - b_{ij})^2} = \sqrt{81} = 9.$$ ◀

★ **Exemplo 7.29.** Sejam

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 1 \\ 1 & -1 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 1 \\ -1 & -2 & -3 \end{pmatrix}$$

Calculamos $A - B$:

$$C = A - B = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix}$$

Com o produto $(A, B) = A : B = \sum_i \sum_j a_{ij} b_{ij}$ do exemplo 7.8, calculamos a distância entre A e B, que é a norma de C:

$$d(A, B) = \|A - B\| = \sqrt{\langle A - B, A - B \rangle}$$
$$= \sqrt{\sum_i \sum_j c_{ij}^2}$$
$$= \sqrt{1 + 0 + 0 + (-2)^2 + 1 + 0 + 2^2 + 1 + 0}$$

$$= \sqrt{1+4+1+4+1}$$
$$= \sqrt{11}.$$

Agora calculamos a distância novamente, mas usando outro produto interno: temos

$$C^T C = \begin{pmatrix} 9 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

os autovalores de $C = A - B$ são portanto 0, 2 e 9. A distância é

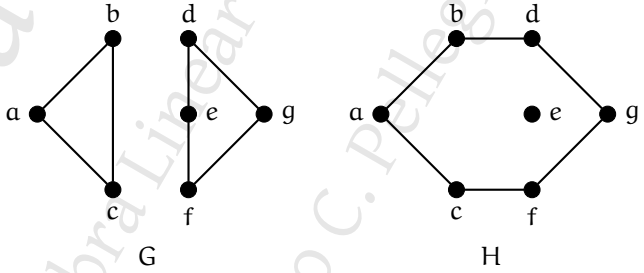
$$\begin{aligned} d(A,B) = \|A-B\|_2 &= \sqrt{\langle A-B, A-B\rangle} \\ &= \sqrt{\max\{0,2,9\}} \\ &= \sqrt{9} = 3. \end{aligned}$$

◀

★ **Exemplo 7.30.** No espaço de ciclos de um grafo, a distância entre dois grafos é a raiz quadrada da quantidade de arestas *não comuns* dos grafos.

Usamos os mesmos grafos G e H do exemplo 7.14, cuja descrição apresentamos novamente a seguir.

$$\begin{aligned} V &= \{a,b,c,d,e,f,g\} \\ E(G) &= \{(a,b),(b,c),(c,a),(d,e),(e,f),(f,g),(g,d)\} \\ E(H) &= \{(a,b),(b,d),(d,g),(g,f),(f,c),(c,a)\} \end{aligned}$$



A distância entre G e H é

$$\begin{aligned} d(G,H) &= \|G-H\| \\ &= \sqrt{\langle G-H, G-H\rangle} \end{aligned}$$

O grafo $G - H$ é formado subtraindo os vetores característico das arestas – ou seja, uma aresta está em

$G - H$ se está em um grafo mas não no outro. Os vetores característicos de arestas de G, H e $G - H$ são

aresta	G	H	$G - H$
$\{a, b\}$	1	1	0
$\{a, c\}$	1	1	0
$\{a, d\}$	0	0	0
$\{a, e\}$	0	0	0
$\{a, f\}$	0	0	0
$\{a, g\}$	0	0	0
$\{b, c\}$	1	0	1
$\{b, d\}$	0	1	1
$\{b, e\}$	0	0	0
$\{b, f\}$	0	0	0
$\{b, g\}$	0	0	0
$\{c, d\}$	0	0	0
$\{c, e\}$	0	0	0
$\{c, f\}$	0	1	1
$\{c, g\}$	0	0	0
$\{d, e\}$	1	0	1
$\{d, f\}$	0	0	0
$\{d, g\}$	1	1	0
$\{e, f\}$	1	0	1
$\{e, g\}$	0	0	0
$\{f, g\}$	1	1	0

Como em $\mathbb{Z}_2$, tanto a soma como a subtração são o ou exclusivo,

$$\begin{aligned}\sqrt{\langle G - H, G - H\rangle} &= \sqrt{\sum_i (gh)_i \wedge (gh)_i} \\ &= \sqrt{5}.\end{aligned}$$

◀

Definição 7.31 (matriz de Gram)**.** Seja $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ um conjunto de vetores. A *matriz de Gram* deste conjunto é a matriz G de ordem n tal que

$$g_{ij} = \langle \mathbf{v}_i, \mathbf{v}_j \rangle ,$$

ou seja,

$$G = \begin{pmatrix} \langle \mathbf{v}_1, \mathbf{v}_1\rangle & \langle \mathbf{v}_1, \mathbf{v}_2\rangle & \cdots & \langle \mathbf{v}_1, \mathbf{v}_n\rangle \\ \langle \mathbf{v}_2, \mathbf{v}_1\rangle & \langle \mathbf{v}_2, \mathbf{v}_2\rangle & \cdots & \langle \mathbf{v}_2, \mathbf{v}_n\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle \mathbf{v}_n, \mathbf{v}_1\rangle & \langle \mathbf{v}_n, \mathbf{v}_2\rangle & \cdots & \langle \mathbf{v}_n, \mathbf{v}_n\rangle \end{pmatrix}.$$

♦

Se os vetores pertencem a $\mathbb{R}^n$ são dispostos como colunas de uma matriz V, então a matriz de Gram é $V^T V$. Se pertencem a $\mathbb{C}^n$, a matriz de Gram é $V^H V$.

Exemplo 7.32. Em $\mathbb{R}^3$, usando o produto interno usual, a matriz de Gram dos vetores

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} -1 \\ 0 \\ 3 \end{pmatrix}, \quad \mathbf{v}_3 = \begin{pmatrix} 4 \\ 4 \\ 8 \end{pmatrix}$$

é

$$G = \begin{pmatrix} \langle \mathbf{v}_1, \mathbf{v}_1 \rangle & \langle \mathbf{v}_1, \mathbf{v}_2 \rangle & \langle \mathbf{v}_1, \mathbf{v}_3 \rangle \\ \langle \mathbf{v}_2, \mathbf{v}_1 \rangle & \langle \mathbf{v}_2, \mathbf{v}_2 \rangle & \langle \mathbf{v}_2, \mathbf{v}_3 \rangle \\ \langle \mathbf{v}_3, \mathbf{v}_1 \rangle & \langle \mathbf{v}_3, \mathbf{v}_2 \rangle & \langle \mathbf{v}_3, \mathbf{v}_3 \rangle \end{pmatrix} = \begin{pmatrix} 5 & -1 & 12 \\ -1 & 10 & 20 \\ 12 & 20 & 96 \end{pmatrix}. \qquad \blacktriangleleft$$

Exemplo 7.33. Em $\mathcal{F}$, no intervalo $[-\pi, +\pi]$ e usando o produto interno usual ($\int_{-\pi}^{\pi} f(x)g(x)dx$), a matriz de Gram de

$$f_1(x) = \operatorname{sen}(x), \quad f_2(x) = \cos(x), \quad , f_3(x) = x$$

é

$$G = \begin{pmatrix} \langle \mathbf{v}_1, \mathbf{v}_1 \rangle & \langle \mathbf{v}_1, \mathbf{v}_2 \rangle & \langle \mathbf{v}_1, \mathbf{v}_3 \rangle \\ \langle \mathbf{v}_2, \mathbf{v}_1 \rangle & \langle \mathbf{v}_2, \mathbf{v}_2 \rangle & \langle \mathbf{v}_2, \mathbf{v}_3 \rangle \\ \langle \mathbf{v}_3, \mathbf{v}_1 \rangle & \langle \mathbf{v}_3, \mathbf{v}_2 \rangle & \langle \mathbf{v}_3, \mathbf{v}_3 \rangle \end{pmatrix} = \begin{pmatrix} \int_{-\pi}^{\pi} \operatorname{sen}^2(x)dx & \int_{-\pi}^{\pi} \operatorname{sen}(x)\cos(x)dx & \int_{-\pi}^{\pi} x\operatorname{sen}(x)dx \\ \int_{-\pi}^{\pi} \operatorname{sen}(x)\cos(x)dx & \int_{-\pi}^{\pi} \cos^2(x)dx & \int_{-\pi}^{\pi} x\cos(x)dx \\ \int_{-\pi}^{\pi} x\operatorname{sen}(x)dx & \int_{-\pi}^{\pi} x\cos(x)dx & \int_{-\pi}^{\pi} x^2dx \end{pmatrix}$$

$$= \begin{pmatrix} \pi & 0 & 2\pi \\ 0 & \pi & 0 \\ 2\pi & 0 & 2\pi^3/3 \end{pmatrix}. \qquad \blacktriangleleft$$

Exemplo 7.34. A seguir temos três matrizes 2×2.

$$A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} -2 & 0 \\ 1 & 1 \end{pmatrix}$$

Se usarmos o produto de Frobenius, a matriz de Gram destas matrizes é

$$G = \begin{pmatrix} A:A & A:B & A:C \\ B:A & B:B & B:C \\ C:A & C:B & C:C \end{pmatrix} = \begin{pmatrix} 4 & -4 & -2 \\ -4 & 8 & 2 \\ -2 & -2 & 6 \end{pmatrix}$$

$\blacktriangleleft$

Teorema 7.35. *Um conjunto de vetores é LI se e somente se sua matriz de Gram tem determinante diferente de zero.*

7.2 Ângulos e ortogonalidade

O produto interno de dois vetores pode ser arbitrariamente grande. Podemos obter valores em um intervalo limitado se dividirmos o produto interno pelo produto das normas dos vetores. Com isso temos o *cosseno* do ângulo destes vetores, que sempre estará entre -1 e 1.

Definição 7.36 (Ângulo entre dois vetores)**.** O *ângulo* entre dois vetores $\mathbf{v}$ e $\mathbf{w}$ é o número θ tal que

$$\cos\theta = \frac{\langle \mathbf{v}, \mathbf{w} \rangle}{||\mathbf{v}||\,||\mathbf{w}||},$$

ou

$$\theta = \arccos\left(\frac{\langle \mathbf{v}, \mathbf{w} \rangle}{||\mathbf{v}||\,||\mathbf{w}||}\right). \qquad \blacklozenge$$

Exemplo 7.37. Em $\mathbb{R}^2$, o ângulo entre os vetores $(0,1)^T$ e $(1,0)$ é

$$\begin{aligned}\theta &= \arccos\left(\frac{\langle (1,0)^T, (0,1)^T\rangle}{\|(1,0)^T\|\,\|(0,1)^T\|}\right)\\ &= \arccos\langle (1,0)^T, (0,1)^T\rangle\\ &= \arccos(0) = \frac{\pi}{2}.\end{aligned}$$

Já entre os vetores $(3,5)$ e $(-1,0)$ o ângulo é

$$\begin{aligned}\theta &= \arccos\left(\frac{\langle (3,5)^T, (-1,0)^T\rangle}{\|(3,5)^T\|\,\|(-1,0)^T\|}\right)\\ &= \arccos\frac{-3}{\sqrt{34}} = 2.11121582706548\ldots\end{aligned}$$ ◀

Exemplo 7.38. O ângulo entre os vetores $\mathbf{v} = (2,4,1,-5)^T$ e $\mathbf{w} = (1,0,-3,-3)^T$ é

$$\begin{aligned}\theta &= \arccos\left(\frac{\langle \mathbf{v}, \mathbf{w}\rangle}{\|\mathbf{v}\|\,\|\mathbf{w}\|}\right)\\ &= \arccos\left(\frac{(2,4,1,-5)(1,0,-3,-3)^T}{\|(2,4,1,-5)^T\|\,\|(1,0,-3,-3)^T\|}\right)\\ &= \arccos\left(\frac{14}{\sqrt{46}\sqrt{19}}\right)\\ &= 1.07747129721464\ldots\end{aligned}$$ ◀

Exemplo 7.39. No espaço $C^0[0,1]$ das funções contínuas definidas no intervalo $[0,1]$, o ângulo entre as funções $f(x) = x^3 - x$ e $g(x) = x^2 - x$ é

$$\begin{aligned}\theta &= \arccos\left(\frac{\langle f, g\rangle}{\|f\|\,\|g\|}\right)\\ &= \arccos\left(\frac{\int_0^1 f(x)g(x)dx}{\sqrt{\int_0^1 f(x)^2dx\int_0^1 g(x)^2dx}}\right)\\ &= \arccos\left(\frac{\int_0^1 (x^3-x)(x^2-x)dx}{\sqrt{\int_0^1 (x^3-x)^2dx\int_0^1 (x^2-x)^2dx}}\right)\\ &= \arccos\left(\frac{1/20}{2/15\sqrt{7}}\right)\\ &= \arccos\left(\frac{3\sqrt{7}}{8}\right)\\ &= 0.12532783116806\ldots\end{aligned}$$ ◀

Teorema 7.40 (Teorema de Pitágoras generalizado)**.** *Em um espaço vetorial com produto interno, para quaisquer dois vetores* $\mathbf{v}$ *e* $\mathbf{w}$ *com ângulo* θ*,*

$$\|\mathbf{v}+\mathbf{w}\|^2 = \|\mathbf{v}\|^2 + \|\mathbf{w}\|^2 + 2\|\mathbf{v}\|\,\|\mathbf{w}\|\cos\theta.$$

Exemplo 7.41. No exemplo 7.39 calculamos o ângulo entre as funções $f(x) = x^3 - x$ e $g(x) = x^2 - x$ no espaço $C^0[0, 1]$, cujo cosseno é $\frac{3\sqrt{7}}{8}$. A norma de $(f + g)(x) = x^2 + x^3 - 2x$ é, portanto,

$$\begin{aligned}
\|\mathbf{f} + \mathbf{g}\|^2 &= \|\mathbf{f}\|^2 + \|\mathbf{g}\|^2 + 2\|\mathbf{f}\|\,\|\mathbf{g}\|\cos\theta \\
&= \|x^3 - x\|^2 + \|x^2 - x\|^2 + 2\|x^3 - x\|\,\|x^2 - x\|\left(\frac{3\sqrt{7}}{8}\right) \\
&= \left(\sqrt{\int_0^1 (x^3 - x)^2 dx}\right)^2 + \left(\sqrt{\int_0^1 (x^2 - x)^2 dx}\right)^2 + 2\sqrt{\int_0^1 (x^3 - x)^2 dx}\sqrt{\int_0^1 (x^2 - x)^2 dx}\left(\frac{3\sqrt{7}}{8}\right)
\end{aligned}$$

Calculamos as integrais, e obtemos

$$\begin{aligned}
\int_0^1 (x^3 - x)^2 dx &= 8/105 \\
\int_0^1 (x^2 - x)^2 dx &= 1/30
\end{aligned}$$

Continuamos:

$$\begin{aligned}
\|\mathbf{f} + \mathbf{g}\|^2 &= \left(\sqrt{\frac{8}{105}}\right)^2 + \left(\sqrt{\frac{1}{30}}\right)^2 + 2\sqrt{\left(\frac{8}{105}\right)\left(\frac{1}{30}\right)}\left(\frac{3\sqrt{7}}{8}\right) \\
&= \frac{23}{210} + \frac{6}{8}\sqrt{\frac{8}{105}\frac{1}{30}}\sqrt{7} \\
&= \frac{23}{210} + \frac{6}{8}\frac{\sqrt{(8)(7)}}{\sqrt{(30)(105)}} \\
&= \frac{23}{210} + \frac{6}{8}\frac{\sqrt{4}}{\sqrt{225}} \\
&= \frac{23}{210} + \frac{6}{8}\frac{2}{15} \\
&= \frac{22}{105}
\end{aligned}$$

Sem o Teorema de Pitágoras, calculamos o mesmo valor:

$$\begin{aligned}
\|\mathbf{f} + \mathbf{g}\|^2 &= \|x^2 + x^3 - 2x\|^2 \\
&= \left(\sqrt{\int_0^1 (x^2 + x^3 - 2x)^2 dx}\right)^2 \\
&= \left(\sqrt{\frac{22}{105}}\right)^2 \\
&= \frac{22}{105}.
\end{aligned}$$

◀

Há uma noção de ortogonalidade em $\mathbb{R}^2$ e $\mathbb{R}^3$, que aqui estendemos para todos os espaços vetoriais com produto interno.

Definição 7.42 (Vetores ortogonais)**.** Dois vetores $\mathbf{v}$ e $\mathbf{w}$ em um espaço com produto interno são *ortogonais* se $\langle \mathbf{v}, \mathbf{w} \rangle = 0$. ♦

Claramente, o ângulo entre vetores ortogonais é $\pi/2$, porque é $\arccos[0/(\|x\| \, \|y\|)] = \arccos(0) = \pi/2$.

Exemplo 7.43. Em $\mathbb{R}^3$ com o produto usual, os vetores $(2, 3, 4)^T$ e $(1, -2, 1)^T$ são ortogonais. ◀

Exemplo 7.44. Em $\mathbb{R}^n$ com o produto usual, quaisquer dois vetores da base canônica são ortogonais. ◀

Exemplo 7.45. Em $C[-\pi, \pi]$, o espaço de funções contínuas definidas entre $-\pi$ e π, o produto interno pode ser dado por

$$\langle f, g \rangle = \int_{-\pi}^{\pi} f(x) g(x) \, dx.$$ ◀

Neste espaço, os vetores (funções) $\cos(x)$ e $\operatorname{sen}(x)$ são ortogonais, porque

$$\int_{-\pi}^{\pi} \cos(x) \operatorname{sen}(x) \, dx = 0.$$

Exemplo 7.46. Em $M_{2\times 2}$ as matrizes

$$A = \begin{pmatrix} 2 & 3 \\ -1 & 0 \end{pmatrix} \quad e \quad B = \begin{pmatrix} 1 & -2 \\ -4 & -2 \end{pmatrix}$$

são ortogonais se usarmos o produto de Frobenius, porque $A : B = 0$. ◀

★ **Exemplo 7.47.** Usando o produto interno definido no exemplo 7.14, está claro que dois grafos de ciclos são ortogonais quando não há arestas comuns entre os dois grafos. ◀

Teorema 7.48. *Em um espaço com produto interno, se n vetores $\mathbf{v}_1, \ldots, \mathbf{v}_n$ diferentes de $\mathbf{0}$ são ortogonais entre si, então também são LI.*

Demonstração. Suponha que $\mathbf{v}_1, \ldots, \mathbf{v}_n$ diferentes de $\mathbf{0}$ são ortogonais e LD. Então existem a_i tais que

$$a_1 \mathbf{v}_1 + \cdots + a_n \mathbf{v}_n = \mathbf{0}$$

com $a_1 \neq 0$. Tomamos o produto da equação por $\mathbf{v}_1$:

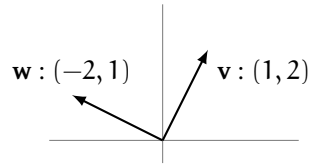
$$\begin{aligned} \langle \mathbf{v}_1, a_1 \mathbf{v}_1 + \cdots + a_n \mathbf{v}_1 \mathbf{v}_n \rangle &= \mathbf{v}_1 \mathbf{0} \\ \langle \mathbf{v}_1, a_1 \mathbf{v}_1 \rangle &= \mathbf{0} \\ a_1 \langle \mathbf{v}_1, \mathbf{v}_1 \rangle &= \mathbf{0}, \end{aligned}$$

e como presumimos que $a_1 \neq 0$, concluímos que $\mathbf{v}_1 = \mathbf{0}$. ■

Corolário 7.49. *Em um espaço de dimensão n, quaisquer n vetores ortogonais formam uma base.*

Corolário 7.50. *Em um espaço de dimensão n, há no máximo n vetores ortogonais entre si.*

Exemplo 7.51. Em $\mathbb{R}^2$, quaisquer dois vetores ortogonais são LI, e não há como obter mais de dois vetores ortogonais em $\mathbb{R}^2$.



Na figura acima, $\mathbf{v} = (1,2)^T$ e $\mathbf{w} = (-2,1)^T$. Os dois vetores são ortogonais, e claramente LI (não são colineares). Além disso, não se pode obter um terceiro vetor no plano que não seja combinação linear destes. ◀

Exemplo 7.52. Os vetores dos exemplos 7.43 e 7.44, que ali mostramos serem ortogonais, são claramente LI.

Os vetores do exemplo 7.45 também são LI: não há como descrever seno como múltiplo de cosseno.

As matrizes do exemplo 7.46 são LI: podemos verificar que $aA + bB = 0$ implica em $a = b = 0$:

$$a\begin{pmatrix} 2 & 3 \\ -1 & 0 \end{pmatrix} + b\begin{pmatrix} 1 & -2 \\ -4 & -2 \end{pmatrix} = 0$$

implica em

$$\begin{cases} 2a + b = 0 \\ 3a - 2b = 0 \\ -a - 4b = 0 \\ -2b = 0 \end{cases},$$

cuja única solução é $a = b = 0$. ◀

Exemplo 7.53. Damos um contraexemplo para a recíproca do teorema 7.48. Os vetores $(1,2)^T$ e $(1,3)^T$ em $\mathbb{R}^2$ são LI, mas não são ortogonais, porque $(1,2)^T(1,3) = 1 + 6 = 7$. ◀

Observe que de acordo com o teorema 7.48 é necessário que haja *algum* produto interno para os quais os vetores sejam ortogonais, como mostra o próximo exemplo.

Exemplo 7.54. Considere o espaço $\mathbb{R}_2[x]$ com o produto interno $\langle p, q\rangle = \int_{-1}^{+1} p(x)q(x)dx$. Os polinômios $p(x) = x^2 - 2/6$, $q(x) = x$ e $r(x) = 1$ são ortogonais:

$$\int_{-1}^{+1} p(x)q(x)dx = \int_{-1}^{+1} \left(x^2 - \frac{2}{6}\right) x dx = 0$$
$$\int_{-1}^{+1} p(x)r(x)dx = \int_{-1}^{+1} x dx = 0$$
$$\int_{-1}^{+1} q(x)r(x)dx = \int_{-1}^{+1} x^2 - \frac{2}{6} dx = 0.$$

Pelo teorema 7.48 os tres polinômios são também LI, e portanto uma base para $\mathbb{R}_2[x]$.

Suponha que

$$p(x) = a_2x^2 + a_1x + a_0$$
$$q(x) = b_2x^2 + b_1x + b_0$$

$$r(x) = c_2x^2 + c_1x + c_0$$

Neste mesmo espaço, com o produto interno $\langle p(x), q(x)\rangle = a_2b_2 + a_1b_1 + a_0b_0$, temos

$$\langle p(x), r(x)\rangle = (1, 0, -2/6)^T(0, 0, 1)^T = -\frac{2}{6} \neq 0,$$

e os vetores não são ortogonais. Ainda assim, são LI. ◀

Exemplo 7.55. Considere o espaço $C[-\pi, \pi]$, com o produto interno $\langle f, g\rangle = \int_{-\pi}^{+\pi} f(x)g(x)dx$. As funções $f(x) = x$ e $g(x) = \text{sen}^2(x)$ são ortogonais neste espaço, e portanto LI:

$$\int_{-\pi}^{+\pi} x\,\text{sen}^2(x)dx = 0$$

Estas funções são base para um subespaço de $C[-\pi, +\pi]$. Neste subespaço estão as funções $ax + b\,\text{sen}^2(x)$.

Se incluirmos $h(x) = x + \cos^2(x) - 1$ teremos o conjunto $\left\{ x, \text{sen}^2(x), x + \cos^2(x) - 1 \right\}$. Este conjunto não é LI, porque

$$\text{sen}^2(x) + (x + \cos^2(x) - 1) = x.$$

De acordo com o teorema 7.48, as funções não podem ser todas ortogonais. E realmente, $\text{sen}^2(x)$ e $x + \cos^2(x) - 1$ não são ortogonais com o produto interno dado:

$$\int_{-\pi}^{+\pi} \text{sen}^2(x)(x + \cos^2(x) - 1)dx = -\frac{3\pi}{4}.$$ ◀

Teorema 7.56. *Em um espaço com produto interno, se n vetores $\mathbf{v}_1, \ldots, \mathbf{v}_n$ são ortogonais a um outro vetor $\mathbf{w}$, então todas as combinações lineares dos vetores $\mathbf{v}_i$ também são ortogonais a $\mathbf{w}$.*

Demonstração. As combinações lineares dos $\mathbf{v}_i$ são $\alpha_1\mathbf{v}_1 + \cdots + \alpha_2\mathbf{v}_n$. O produto de uma combinação linear dos $\mathbf{v}_i$ com $\mathbf{w}$ é

$$\begin{aligned} &\langle \alpha_1\mathbf{v}_1 + \cdots + \alpha_2\mathbf{v}_n, \mathbf{w}\rangle \\ &= \langle \alpha_1\mathbf{v}_1, \mathbf{w}\rangle + \cdots + \langle \alpha_n\mathbf{v}_n, \mathbf{w}\rangle \\ &= \alpha_1 \langle \mathbf{v}_1, \mathbf{w}\rangle + \cdots + \alpha_n \langle \mathbf{v}_n, \mathbf{w}\rangle \end{aligned}$$

que é zero, porque todos os produtos são zero. ■

Exemplo 7.57. Em $\mathbb{R}^3$ com o produto interno usual, os vetores

$$\begin{aligned} \mathbf{v_1} &= (2, 0, 0)^T \\ \mathbf{v_2} &= (0, 1, 0)^T \end{aligned}$$

são ortogonais ao vetor $\mathbf{v_3}$:

$$\mathbf{v_3} = (0, 0, 3)^T.$$

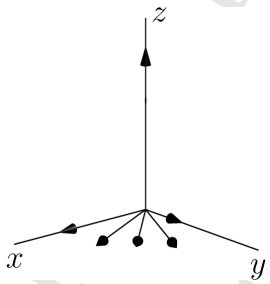
Qualquer combinação linear de $\mathbf{v_1}$ e $\mathbf{v_2}$ também será ortogonal a $\mathbf{v_3}$:

$$a\mathbf{v_1} + b\mathbf{v_2} = (2a, b, 0)^T.$$

Verificamos que o produto interno de $\mathbf{v_3}$ com $(2a, b, 0)^T$ é zero:

$$\begin{aligned}\left\langle (0,0,3)^T, (2a,b,0)^T \right\rangle &= (0,0,3)^T\ (2a,b,0)^T \\ &= (0)(2a) + (0)(b) + (3)(0) \\ &= 0.\end{aligned}$$

Geometricamente, temos $\mathbf{v_1}$ e $\mathbf{v_2}$ no plano por onde passam os eixos **x** e **y**:



O vetor $\mathbf{v_3}$ está sobre o eixo **z**. Algumas combinações lineares de $\mathbf{v_1}$ e $\mathbf{v_2}$ são mostradas na figura – são os vetores tracejados. Claramente, todas ficam no mesmo plano, perpendicular a $\mathbf{v_3}$. ◀

Definição 7.58 (Base ortogonal)**.** Uma base para um espaço vetorial com produto interno é *ortogonal* se seus vetores são todos ortogonais entre si. ♦

Exemplo 7.59. Os vetores $(-2, 1)^T$ e $(2, 4)^T$ formam uma base ortogonal para $\mathbb{R}^2$. ◀

Definição 7.60 (Base ortonormal)**.** Uma base para um espaço vetorial com produto interno é *ortonormal* se é ortogonal e todos os seus vetores tem norma igual a um. ♦

Exemplo 7.61. A base canônica em $\mathbb{R}^n$ é ortonormal. ◀

A base canônica não é a única base ortonormal, como mostra o exemplo a seguir.

Exemplo 7.62. Os vetores

$$\begin{pmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

são claramente LI (e portanto base para $\mathbb{R}^2$).

Os dois vetores são ortogonais:

$$\left(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right) \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = 0$$

Finalmente, a norma de ambos é igual a um:

$$\sqrt{\left(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right) \begin{pmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}} = 1$$

$$\sqrt{\left(\frac{1}{\sqrt{2}},\ \frac{1}{\sqrt{2}}\right)\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}} = 1,$$

e portanto os dois vetores formam uma base ortonormal. ◀

Teorema 7.63. *Se* $B = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ *é uma base ortonormal para um espaço* V*, então para todo* $\mathbf{v} \in V$*,*

$$\mathbf{v} = \sum_i \langle \mathbf{v}, \mathbf{b}_i \rangle \mathbf{b}_i.$$

Exemplo 7.64. Seja $B = \{(0,0,1)^T, (0,1,0)^T, (0,0,1)^T\}$. Então o vetor $(2,4,5)^T$ é

$$\begin{aligned}(2,4,5)^T &= \left\langle (0,0,1)^T, (2,4,5)^T \right\rangle (0,0,1)^T \\ &\quad + \left\langle (0,1,0)^T, (2,4,5)^T \right\rangle (0,1,0)^T \\ &\quad + \left\langle (1,0,0)^T, (2,4,5)^T \right\rangle (1,0,0)^T \\ &= (5,0,0)^T + (0,4,0)^T + (1,0,0)^T.\end{aligned}$$ ◀

Exemplo 7.65. Seja

$$B = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}-1\\1\end{pmatrix} \right\}.$$

Então o vetor $(-2,5)^T$ é

$$\begin{aligned}(-2,5)^T &= \left\langle \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)^T, (-2,5)^T \right\rangle \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)^T \\ &\quad + \left\langle \left(\frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)^T, (-2,5)^T \right\rangle \left(\frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)^T \\ &= \left(\frac{3}{2}, \frac{3}{2}\right)^T + \left(-\frac{7}{2}, \frac{7}{2}\right)^T.\end{aligned}$$ ◀

7.3 Projeções

Em Geometria Analítica definimos a projeção de um vetor $\mathbf{v}$ sobre uma reta r como o vetor $\mathbf{v}'$ tal que $\mathbf{u} = \mathbf{v} - \mathbf{v}'$ é perpendicular a r (ou ainda, o vetor $\mathbf{u}$ é paralelo a uma reta s perpendicular a r).

Mas sabemos que uma reta é um subespaço de $\mathbb{R}^2$, e que nessa definição de projeção, vetores de r e s são ortogonais entre si (o ângulo entre eles será sempre $\pi/2$). Como cada um desses subespaços tem dimensão um, e a interseção deles é somente a origem, concluímos que $\mathbb{R}^2$ é soma direta desses dois subespaços.

Assim, revisamos o conceito de projeção: falamos agora de projeção de um vetor de um espaço V em um subespaço de V.

Definição 7.66 (Projeção)**.** Sejam U, V e W espaços vetoriais tais que $V = U \oplus W$. Um operador linear em T é uma *projeção em* U se e somente se, para todo $\mathbf{v} = \mathbf{u} + \mathbf{w}$, com $\mathbf{u} \in U$ e $\mathbf{w} \in W$, $T(\mathbf{v}) = \mathbf{u}$. ♦

Exemplo 7.67. ◀

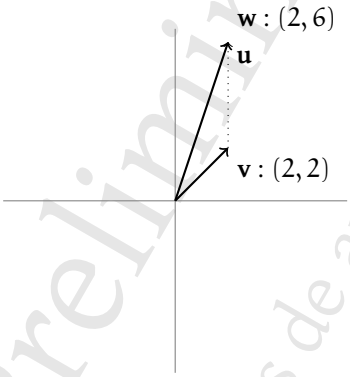
Exemplo 7.68. Em $\mathbb{R}^2$, o operador linear

$$T(x, y)^T = (x, 3x)^T$$

é uma projeção no subespaço igual à reta $y = 3x$. Todo vetor em $\mathbb{R}^2$ pode ser escrito como soma

$$(x, 3x)^T + (0, a)^T,$$

e o operador T sempre nos dará o componente $(x, 3x)^T$. Geometricamente: temos um vetor qualquer, por exemplo, $(2, 2)^T$. A transformação levará em $(2, 6)^T$, que fica sobre a reta $(x, 3x)^T$:



◀

Exemplo 7.69. Em $\mathbb{R}^4$, O operador $T(x_1, x_2, x_3, x_4)^T = (x_1, x_2, 0, 0)^T$ é uma projeção no subespaço de $\mathbb{R}^4$ gerado por $(a, b, 0, 0)^T$. ◀

Exemplo 7.70. Em $\mathbb{R}_4[x]$, o de polinômios de grau 4, o operador T que elimina o termo com coeficiente x^4 é uma projeção. Sabemos que

$$\mathbb{R}_4[x] = \mathbb{R}_3[x] \oplus \{ax^4 : a \in \mathbb{R}\},$$

e o operador descrito leva qualquer polinômio de grau 4 no componente em $\mathbb{R}^3$. Por exemplo,

$$3x^4 - 2x^3 + 1 = \left(3x^4\right) + \left(-2x^3 + 1\right).$$

O operador T leva o polinômio à sua componente de grau 3:

$$T(3x^4 - 2x^3 + 1) = -2x^3 + 1.$$ ◀

Uma vez que um vetor tenha sido projetado em um subespaço, o operador de projeção não mais o modificará. Similarmente, se um vetor não é modificado pelo operador de projeção, ele já deve pertencer ao subespaço onde o operador projeta.

Teorema 7.71. *Um operador linear* T *é uma* projeção *se e somente se* $T = T \circ T$ *(ou, na forma matricial,* $T = T^2$*). Também dizemos que* T *é* idempotente.

Exemplo 7.72. O operador

$$T = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

é idempotente:

$$T^2 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

Também podemos verificar que T é uma projeção: seja $\mathbf{v} = (x_1, x_2)^T$. Então

$$T\mathbf{v} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_1 \end{pmatrix},$$

e vetores são projetados por T na reta $(x, x)^T$. ◀

Exemplo 7.73. O operador definido no espaço $\mathbb{R}_4[x]$, no Exemplo 7.70 é, em forma matricial,

$$T = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Para aplicar T em um polinômio $a_4x^4 + a_3x^3 + a_2x^2 + a_1x + x_0$, usamos suas coordenadas:

$$\begin{aligned} T(a_4x^4 + a_3x^3 + a_2x^2 + a_1x + x_0) &= T(a_4, a_3, a_2, a_1, a_0)^T \\ &= \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} a_4 \\ a_3 \\ a_2 \\ a_1 \\ a_0 \end{pmatrix} = \begin{pmatrix} 0 \\ a_3 \\ a_2 \\ a_1 \\ a_0 \end{pmatrix}, \end{aligned}$$

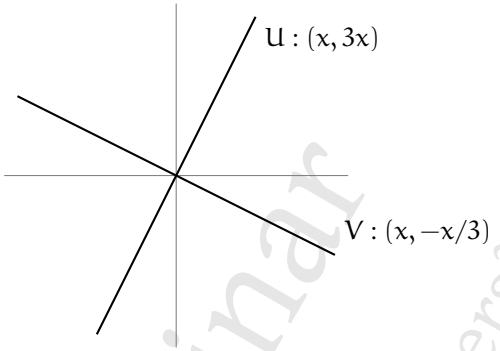
que são as coordenadas de $\mathbf{0x^4} + a_3x^3 + a_2x^2 + a_1x + x_0$.

Verificamos que a matriz do operador é idempotente:

$$T^2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = T.$$ ◀

Definição 7.74 (Complemento ortogonal)**.** Seja V um espaço vetorial e W um subespaço de V. O *complemento ortogonal* de W é o subespaço denotado $W^\perp$ tal que todo vetor de W é ortogonal a todo vetor de $W^\perp$. ♦

Exemplo 7.75. Em $\mathbb{R}^2$, o subespaço U gerado por $(x, 3x)^T$ é uma reta. Seu complemento ortogonal é o subespaço V gerado por $(x, -x/3)^T$ – que é a reta perpendicular a U.



Quaisquer duas retas perpendiculares em $\mathbb{R}^2$ passando pela origem formam um exemplo de subespaço com complemento ortogonal. ◀

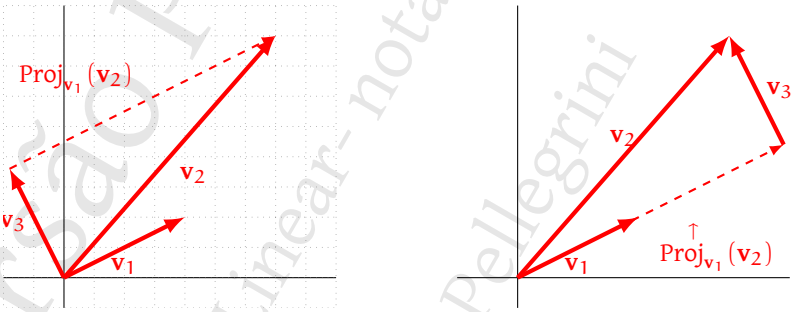
Exemplo 7.76. Em $\mathbb{R}^3$, o complemento ortogonal de uma reta é um plano, e o de um plano é uma reta. ◀

Definição 7.77 (Projeção ortogonal)**.** Seja $\mathbf{v}$ um vetor em um espaço vetorial. Se

$$\mathbf{v} = \mathbf{p} + k\mathbf{w},$$

com $\mathbf{p}$ e $\mathbf{w}$ ortogonais, dizemos $\mathbf{p}$ é a *projeção ortogonal* de $\mathbf{v}$ em $\mathbf{w}$. ♦

Exemplo 7.78. Na figura a seguir, $\mathbf{v}_1 = (4,2)^T$ e $\mathbf{v}_2 = (7,8)^T$.



O vetor tracejado, exibido como se indo de $\mathbf{v}_3$ até $\mathbf{v}_2$ na figura da esquerda, é a projeção ortogonal de $\mathbf{v}_2$ em $\mathbf{v}_1$. Ele pertence ao mesmo subespaço que $\mathbf{v}_1$, embora esteja representado de forma paralela a ele, longe da origem – a figura da direita mostra que este vetor é de fato a projeção de $\mathbf{v}_2$ em $\mathbf{v}_1$, formando um ângulo reto. Observe que

- $\mathbf{v}_3 = \mathbf{v}_2 - \frac{11}{5}\mathbf{v}_1$, e
- $\langle \mathbf{v}_1, \mathbf{v}_3 \rangle = 0$ (são ortogonais). ◀

Teorema 7.79. *Para todo* $\mathbf{v}$ *e* $\mathbf{w} \neq \mathbf{0}$ *em um espaço vetorial, existe uma projeção ortogonal de* $\mathbf{v}$ *em* $\mathbf{w}$*, dada* unicamente *por*

$$\text{Proj}_{\mathbf{w}}(\mathbf{v}) = \frac{\langle \mathbf{w}, \mathbf{v} \rangle}{\langle \mathbf{w}, \mathbf{w} \rangle}\mathbf{w}.$$

Demonstração. Primeiro verificamos que $\mathbf{v} - \text{Proj}_{\mathbf{w}}(\mathbf{v})$ de fato resulta em vetor ortogonal a $\mathbf{w}$.

$$\begin{aligned}
\mathbf{u} &= \mathbf{v} - \text{Proj}_{\mathbf{w}}(\mathbf{v}) \\
&= \mathbf{v} - \frac{\langle \mathbf{w}, \mathbf{v} \rangle}{\langle \mathbf{w}, \mathbf{w} \rangle} \mathbf{w} \\
\langle \mathbf{w}, \mathbf{u} \rangle &= \langle \mathbf{w}, \mathbf{v} \rangle - \frac{\langle \mathbf{w}, \mathbf{v} \rangle}{\langle \mathbf{w}, \mathbf{w} \rangle} \langle \mathbf{w}, \mathbf{w} \rangle \qquad \text{(produto interno com } \mathbf{w}\text{)} \\
&= \langle \mathbf{w}, \mathbf{v} \rangle - \langle \mathbf{w}, \mathbf{v} \rangle = 0.
\end{aligned}$$

Para verificar que esta forma é única, observamos que $\mathbf{v} = \mathbf{u} + k\mathbf{w}$. Calculando o produto interno com $\mathbf{w}$, obtemos

$$(\mathbf{v}, \mathbf{w}) = (\mathbf{u}, \mathbf{w}) + k(\mathbf{w}, \mathbf{w}),$$

mas como $\mathbf{u}$ e $\mathbf{w}$ são ortogonais, temos

$$\begin{aligned}
(\mathbf{v}, \mathbf{w}) &= k(\mathbf{w}, \mathbf{w}) \\
\frac{(\mathbf{v}, \mathbf{w})}{(\mathbf{w}, \mathbf{w})} &= k,
\end{aligned}$$

determinando unicamente k. ■

Exemplo 7.80. No exemplo 7.78, obtemos a projeção ortogonal usando a fórmula dada no teorema:

$$\begin{aligned}
\mathbf{v}_3 =& \mathbf{v}_2 - \text{Proj}_{\mathbf{v}_1}(\mathbf{v}_2) \\
=& \mathbf{v}_2 - \frac{\langle \mathbf{v}_1, \mathbf{v}_2 \rangle}{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle} \mathbf{v}_1 \\
=& (7, 8)^T - \frac{11}{5}(4, 2)^T \\
=& \frac{1}{5}(-9, 18)^T.
\end{aligned}$$

◄

Exemplo 7.81. Em $\mathbb{R}^3$, sejam

$$\mathbf{w} = (1, 2, 0)^T, \qquad \mathbf{v} = (2, 1, 1)^T$$

Os vetores não são ortogonais (seu produto interno é 4).

Usando a projeção ortogonal de $\mathbf{v}$ em $\mathbf{w}$ obtemos

$$\begin{aligned}
\mathbf{u} &= \mathbf{v} - \text{Proj}_{\mathbf{w}}(\mathbf{v}) \\
&= \mathbf{v} - \frac{\langle \mathbf{w}, \mathbf{v} \rangle}{\langle \mathbf{w}, \mathbf{w} \rangle} \mathbf{w} \\
&= (2, 1, 1)^T - \frac{\langle (1, 2, 0)^T, (2, 1, 1)^T \rangle}{\langle (1, 2, 0)^T, (1, 2, 0)^T \rangle} (1, 2, 0)^T \\
&= (2, 1, 1)^T - \frac{4}{5}(1, 2, 0)^T \\
&= \left(\frac{6}{5}, -\frac{3}{5}, 1 \right)^T.
\end{aligned}$$

Então $\mathbf{v} = \mathbf{p} + k\mathbf{w}$, e como podemos verificar, $\mathbf{p}$ e $\mathbf{w}$ são ortogonais:

$$(\mathbf{u}, \mathbf{w}) = \left\langle \left(\frac{6}{5}, -\frac{3}{5}, 1\right)^T, (1,2,0)^T \right\rangle = 0. \qquad \blacktriangleleft$$

Exemplo 7.82. No espaço $C^0[-1,1]$ das funções contínuas entre -1 e 1, podemos definir o produto interno como

$$(f, g) = \int_{-1}^{1} f(x)g(x)dx.$$

Neste espaço, as funções $f(x) = x^2$ e $\ln(x+2)$ não são ortogonais, porque

$$\int_{-1}^{1} x^2 \ln(x+2)dx = 2\ln(3) - \frac{26}{9}.$$

Podemos obter uma função ortogonal a g. Basta calcular a projeção ortogonal de f em g:

$$\begin{aligned} \mathbf{h} = \mathbf{f} - \frac{\langle \mathbf{g}, \mathbf{f} \rangle}{\langle \mathbf{g}, \mathbf{g} \rangle}\mathbf{g} &= x^2 - \frac{\langle x^2, \ln(x+2) \rangle}{\langle \ln(x+2), \ln(x+2) \rangle} \ln(x+2) \\ &= x^2 - \frac{2\ln(3) - 26/9}{3\ln^2(3) - 6\log(3) + 4} \ln(x+2). \end{aligned} \qquad \blacktriangleleft$$

O exercício 224 pede a demonstração do teorema 7.83.

Teorema 7.83. *Seja W subespaço de um espaço vetorial V. Então $V = W \oplus W^\perp$.*

Definição 7.84 (Projeção ortogonal em subespaço)**.** Seja W subespaço de um espaço vetorial V. Uma projeção de um vetor $\mathbf{w} \in W$ em $W^\perp$ é uma *projeção ortogonal de* $\mathbf{v}$ *em* W. ♦

Teorema 7.85. *Seja W subespaço de um espaço vetorial V, e $\{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_k\}$ uma base ortogonal de W. O operador*

$$\mathrm{Proj}_W(\mathbf{v}) = \frac{\langle \mathbf{w}_1, \mathbf{v} \rangle}{\langle \mathbf{w}_1, \mathbf{w}_1 \rangle}\mathbf{w}_1 + \cdots + \frac{\langle \mathbf{w}_k, \mathbf{v} \rangle}{\langle \mathbf{w}_k, \mathbf{w}_k \rangle}\mathbf{w}_k$$

realiza a projeção ortogonal de um vetor $\mathbf{v} \in V$ pelo subespaço W: $\mathbf{v} - \mathrm{Proj}_W(\mathbf{v}) \in W^\perp$.

Exemplo 7.86. Seja $\mathbf{b}_1 = (0,1,0)^T, \mathbf{b}_2 = (2,0,0)^T$ uma base para um subespaço W de $\mathbb{R}^3$ com dimensão 2. Considere o vetor $\mathbf{v} = (3,3,4)^T$ em $\mathbb{R}^3$. Calculamos agora sua projeção em W.

Antes de começarmos, pré-calculamos:

$$\begin{aligned} \langle \mathbf{b}_1, \mathbf{b}_1 \rangle &= 1 \\ \langle \mathbf{b}_2, \mathbf{b}_2 \rangle &= 4. \end{aligned}$$

Calculamos agora a projeção de $\mathbf{v}$.

$$\begin{aligned} \mathrm{Proj}_W(\mathbf{v}) &= \frac{\langle \mathbf{b}_1, \mathbf{v} \rangle}{\langle \mathbf{b}_1, \mathbf{b}_1 \rangle}\mathbf{b}_1 + \frac{\langle \mathbf{b}_2, \mathbf{v} \rangle}{\langle \mathbf{b}_2, \mathbf{b}_2 \rangle}\mathbf{b}_2 \\ &= \left\langle (0,1,0)^T, (3,3,4)^T \right\rangle \mathbf{b}_1 + \frac{\left\langle (2,0,0)^T, (3,3,4)^T \right\rangle}{4}\mathbf{b}_2 \end{aligned}$$

$$
\begin{aligned}
&= 3\mathbf{b}_1 + \frac{3}{2}\mathbf{b}_2 \\
&= (0,3,0)^T + (3,0,0)^T \\
&= (3,3,0)^T.
\end{aligned}
$$

Definimos

$$\mathbf{u} = \mathbf{v} - \text{Proj}_{\mathbb{R}^2}(\mathbf{v}) = (3,3,4)^T - (3,3,0)^T = (0,0,4)^T.$$

Verificamos que $(0,0,4)^T$ é ortogonal a todos os vetores de W. Vetores em W são da forma

$$
\begin{aligned}
\mathbf{w} &= a\mathbf{b}_1 + b\mathbf{2} \\
&= (0,a,0)^T + (2b,0,0)^T \\
&= (2b,a,0)^T
\end{aligned}
$$

O produto interno de $(0,0,4)^T$ com $\mathbf{w} \in W$ será sempre igual a $0 \cdot (2b) + 0a + 0 \cdot 4 = 0$. ◀

7.4 Ortogonalização

A partir de uma base não ortogonal, podemos obter uma base ortogonal usando o *processo de ortogonalização de Gram-Schmidt*.

Teorema 7.87. *Todo espaço vetorial de dimensão finita tem uma base ortogonal.*

Demonstração. Todo espaço vetorial de dimensão finita tem uma base. Presumimos que seja dada uma base não ortogonal, $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ para um espaço vetorial. Para obter uma base ortogonal $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n$, começamos incluíndo $\mathbf{b}_1$ na nova base:

$$\mathbf{c}_1 = \mathbf{b}_1$$

Agora suponha que já temos k vetores ortogonais. O k-ésimo vetor $\mathbf{c}_k$ deve ser ortogonal a todos os anteriores, $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_{k-1}$. Escrevemos uma combinação linear destes vetores que já temos na base com $\mathbf{b}_k$:

$$\mathbf{c}_k = \mathbf{b}_k + a_1\mathbf{c}_1 + a_2\mathbf{c}_2 + \cdots + a_{k-1}\mathbf{c}_{k-1}. \tag{7.1}$$

Queremos que $\mathbf{c}_i$ e $\mathbf{c}_k$ sejam ortogonais, portanto

$$
\begin{aligned}
\langle \mathbf{c}_1, \mathbf{c}_k \rangle &= 0 \\
\langle \mathbf{c}_2, \mathbf{c}_k \rangle &= 0 \\
&\vdots \\
\langle \mathbf{c}_{k-1}, \mathbf{c}_k \rangle &= 0
\end{aligned}
\tag{7.2}
$$

Substituímos $\mathbf{c}_i$, como definido na equação 7.1, nas equações 7.2:

$$
\begin{aligned}
\langle \mathbf{c}_1, \mathbf{b}_k + a_1\mathbf{c}_1 + a_2\mathbf{c}_2 + \cdots + a_{k-1}\mathbf{c}_{k-1} \rangle &= 0 \\
\langle \mathbf{c}_2, \mathbf{b}_k + a_1\mathbf{c}_1 + a_2\mathbf{c}_2 + \cdots + a_{k-1}\mathbf{c}_{k-1} \rangle &= 0 \\
&\vdots
\end{aligned}
$$

$$\langle \mathbf{c}_{k-1}, \mathbf{b}_k + a_1\mathbf{c}_1 + a_2\mathbf{c}_2 + \cdots + a_{k-1}\mathbf{c}_{k-1}\rangle = 0$$

Tomamos uma destas equações. Temos

$$\begin{aligned}
\langle \mathbf{c}_i, \mathbf{b}_k + a_1\mathbf{c}_1 + a_2\mathbf{c}_2 + \cdots + a_{k-1}\mathbf{c}_{k-1}\rangle &= 0\\
\langle \mathbf{c}_i, \mathbf{b}_k\rangle + \langle \mathbf{c}_i, a_1\mathbf{c}_1\rangle + \langle \mathbf{c}_i, a_2\mathbf{c}_2\rangle + \cdots + \langle \mathbf{c}_i, a_{k-1}\mathbf{c}_{k-1}\rangle &= 0\\
\langle \mathbf{c}_i, \mathbf{b}_k\rangle + a_1\langle \mathbf{c}_i, \mathbf{c}_1\rangle + a_2\langle \mathbf{c}_i, \mathbf{c}_2\rangle + \cdots + a_{k-1}\langle \mathbf{c}_i, \mathbf{c}_{k-1}\rangle &= 0\\
\langle \mathbf{c}_i, \mathbf{b}_k\rangle + a_i\langle \mathbf{c}_i, \mathbf{c}_i\rangle &= 0,
\end{aligned}$$

porque os $k-1$ vetores anteriores são ortogonais entre si. Com isso obtemos

$$a_i = -\frac{\langle \mathbf{c}_i, \mathbf{b}_k\rangle}{\langle \mathbf{c}_i, \mathbf{c}_i\rangle}.$$

Podemos agora substituir os valores de a_i na equação 7.1. Determinamos portanto que o vetor $\mathbf{c}_k$ é

$$\begin{aligned}
\mathbf{c}_k &= a_1\mathbf{c}_1 + a_2\mathbf{c}_2 + \cdots + a_{k-1}\mathbf{c}_{k-1} + \mathbf{b}_k\\
&= \mathbf{b}_k - \frac{\langle \mathbf{c}_1, \mathbf{b}_k\rangle}{\langle \mathbf{c}_1, \mathbf{c}_1\rangle}\mathbf{c}_1 - \frac{\langle \mathbf{c}_2, \mathbf{b}_k\rangle}{\langle \mathbf{c}_2, \mathbf{c}_2\rangle}\mathbf{c}_2 - \cdots - \frac{\langle \mathbf{c}_{k-1}, \mathbf{b}_k\rangle}{\langle \mathbf{c}_{k-1}, \mathbf{b}_{k-1}\rangle}\mathbf{c}_{k-1}.
\end{aligned}$$

■

A demonstração do teorema 7.87 é construtiva, e nos dá um método para conseguir uma base ortogonal a partir de uma base qualquer.

Método 7.88 (Ortogonalização de Gram-Schmidt)**.** Sejam $\mathbf{b}_1, \ldots, \mathbf{b}_k$ uma base qualquer para um espaço vetorial. Podemos calcular, um a um, os vetores de uma base ortogonal para o mesmo espaço usando o processo de Gram-Schmidt:

$$\begin{aligned}
\mathbf{c}_1 &= \mathbf{b}_1\\
\mathbf{c}_2 &= \mathbf{b}_2 - \frac{\langle \mathbf{c}_1, \mathbf{b}_2\rangle}{\langle \mathbf{c}_1, \mathbf{c}_1\rangle}\mathbf{c}_1\\
\mathbf{c}_3 &= \mathbf{b}_3 - \frac{\langle \mathbf{c}_2, \mathbf{b}_3\rangle}{\langle \mathbf{c}_2, \mathbf{c}_2\rangle}\mathbf{c}_2 - \frac{\langle \mathbf{c}_1, \mathbf{b}_3\rangle}{\langle \mathbf{c}_1, \mathbf{c}_1\rangle}\mathbf{c}_1\\
&\vdots\\
\mathbf{c}_k &= \mathbf{b}_k - \sum_{i<k}\frac{\langle \mathbf{c}_i, \mathbf{b}_k\rangle}{\langle \mathbf{c}_i, \mathbf{c}_i\rangle}\mathbf{c}_i
\end{aligned}$$

Se quisermos uma base ortonormal, calculamos

$$\begin{aligned}
\mathbf{c}_1 &= \frac{\mathbf{c}_1}{\|\mathbf{c}_1\|}\\
\mathbf{c}_2 &= \frac{\mathbf{c}_2}{\|\mathbf{c}_2\|}\\
&\vdots\\
\mathbf{c}_k &= \frac{\mathbf{c}_k}{\|\mathbf{c}_k\|}
\end{aligned}$$

●

Exemplo 7.89. Usaremos o algoritmo de Gram-Schmidt na seguinte base não ortogonal de $\mathbb{R}^3$:

$$\begin{aligned}\mathbf{b}_1 &= (1,0,-2)^\mathsf{T}\\ \mathbf{b}_2 &= (2,-2,2)^\mathsf{T}\\ \mathbf{b}_3 &= (1,-1,0)^\mathsf{T}\end{aligned}$$

O primeiro vetor da base ortogonal será igual a $\mathbf{b}_1$:

$$\mathbf{c}_1 = \mathbf{b}_1 = (1,0,-2)^\mathsf{T}$$

O segundo vetor é

$$\begin{aligned}\mathbf{c}_2 &= \mathbf{b}_2 - \frac{\langle \mathbf{c}_1, \mathbf{b}_2\rangle}{\langle \mathbf{c}_1, \mathbf{c}_1\rangle}\mathbf{c}_1\\ &= (2,-2,2)^\mathsf{T} - \frac{\langle (1,0,-2)^\mathsf{T}, (2,-2,2)^\mathsf{T}\rangle}{\langle (1,0,-2)^\mathsf{T}, (1,0,-2)^\mathsf{T}\rangle}(1,0,-2)^\mathsf{T}\\ &= (2,-2,2)^\mathsf{T} - \frac{-2}{5}(1,0,-2)^\mathsf{T}\\ &= (2,-2,2)^\mathsf{T} + \left(\frac{2}{5},0,-\frac{4}{5}\right)^\mathsf{T}\\ &= \left(\frac{12}{5},-2,\frac{6}{5}\right)^\mathsf{T}.\end{aligned}$$

O terceiro vetor é

$$\begin{aligned}\mathbf{c}_3 &= \mathbf{b}_3 - \frac{\langle \mathbf{c}_2, \mathbf{b}_3\rangle}{\langle \mathbf{c}_2, \mathbf{c}_2\rangle}\mathbf{c}_2 - \frac{\langle \mathbf{c}_1, \mathbf{b}_2\rangle}{\langle \mathbf{c}_1, \mathbf{c}_1\rangle}\mathbf{c}_1\\ &= (1,-1,0)^\mathsf{T} - \frac{\langle (2,-2,2)^\mathsf{T}, (1,-1,0)^\mathsf{T}\rangle}{\langle (2,-2,2)^\mathsf{T}, (2,-2,2)^\mathsf{T}\rangle}(2,-2,2)^\mathsf{T} - \frac{\langle (1,0,-2)^\mathsf{T}, (1,-1,0)^\mathsf{T}\rangle}{\langle (1,0,-2)^\mathsf{T}, (1,0,-2)^\mathsf{T}\rangle}(1,0,-2)^\mathsf{T}\\ &= (1,-1,0)^\mathsf{T} - \frac{22/5}{56/5}\left(\frac{12}{5},-2,\frac{6}{5}\right)^\mathsf{T} + \frac{1}{5}(1,0,-2)^\mathsf{T}\\ &= (1,-1,0)^\mathsf{T} - \frac{11}{28}\left(\frac{12}{5},-2,\frac{6}{5}\right)^\mathsf{T} + \left(\frac{1}{5},0,-\frac{2}{5}\right)^\mathsf{T}\\ &= (1,-1,0)^\mathsf{T} - \left(\frac{33}{35},-\frac{11}{14},\frac{33}{70}\right)^\mathsf{T} + \left(\frac{1}{5},0,-\frac{2}{5}\right)^\mathsf{T}\\ &= \left(-\frac{1}{7},-\frac{3}{14},-\frac{1}{14}\right)^\mathsf{T}.\end{aligned}$$

Verificamos que os vetores são de fato ortogonais:

$$\begin{aligned}\langle \mathbf{c}_1, \mathbf{c}_2\rangle &= (1,0,-2)(12/5,-2,6/5)^\mathsf{T} = 12/5 + 0 - 12/5 = 0.\\ \langle \mathbf{c}_1, \mathbf{c}_3\rangle &= (1,0,-2)(-1/7,-3/14,-1/14)^\mathsf{T} = -1/7 + 0 + 2/14 = 0.\\ \langle \mathbf{c}_2, \mathbf{c}_3\rangle &= (12/5,-2,6/5)(-1/7,-3/14,-1/14)^\mathsf{T} = -12/35 + 3/7 - 3/35 = 0.\end{aligned}$$

Se quisermos uma base ortonormal,

$$\mathbf{d}_1 = \frac{\mathbf{c}_1}{\|\mathbf{c}_1\|} = \frac{1}{\sqrt{5}}(1,0,-2)^T = \left(\frac{1}{\sqrt{5}}, 0, -\frac{2}{\sqrt{5}}\right)^T$$
$$\mathbf{d}_2 = \frac{\mathbf{c}_2}{\|\mathbf{c}_2\|} = \frac{\sqrt{5}}{2\sqrt{14}}\left(\frac{12}{5}, -2, \frac{6}{5}\right)^T = \left(\frac{6}{\sqrt{5}\sqrt{14}}, -\frac{\sqrt{5}}{\sqrt{14}}, \frac{3}{\sqrt{5}\sqrt{14}}\right)^T$$
$$\mathbf{d}_3 = \frac{\mathbf{c}_3}{\|\mathbf{c}_3\|} = \sqrt{14}\left(-\frac{1}{7}, -\frac{3}{14}, -\frac{1}{14}\right)^T = \left(-\frac{\sqrt{14}}{7}, -\frac{3}{\sqrt{14}}, -\frac{1}{\sqrt{14}}\right)^T \quad \blacktriangleleft$$

Exemplo 7.90. No espaço $C^0[0,1]$, as combinações lineares de $f_1(x) = x$ e $f_2(x) = e^x$ são base para um subespaço, contendo as funções da forma $ax + be^x$. Esta base, no entanto, não é ortogonal se usarmos o produto interno que definimos anteriormente para funções:

$$\langle x, e^x \rangle = \int_0^1 x e^x \, dx = 1.$$

Usamos o processo de ortogonalização de Gram-Schmidt para obter uma base ortogonal. O primeiro vetor será $g_1(x) = f_1(x) = x$. O segundo vetor é

$$\begin{aligned} g_2(x) &= f_2(x) - \frac{\langle g_1(x) f_2(x) \rangle}{\langle g_1(x), g_1(x) \rangle} g_1(x) \\ &= e^x - \frac{\langle x, e^x \rangle}{\langle x, x \rangle} x \\ &= e^x - \frac{\int_0^1 x e^x \, dx}{\int_0^1 x^2 \, dx} x \\ &= e^x - \frac{1}{1/3} x = e^x - 3x. \end{aligned}$$

Agora verificamos que as funções $g_1(x)$ e $g_2(x)$ são ortogonais:

$$\langle g_1, g_2 \rangle = \langle x, e^x - 3x \rangle = \int_0^1 x(e^x - 3x) \, dx = 0. \quad \blacktriangleleft$$

7.5 Diagonalização de matrizes simétricas

Matrizes reais simétricas (e complexas Hermitianas) tem propriedades importantes relacionadas à sua diagonalização e ortogonalidade. Estas propriedades são relevantes, por exemplo, no estudo de formas quadráticas realizado no Capítulo 12.

Teorema 7.91. *Os autovalores de uma matriz real simétrica são todos reais.*

Exemplo 7.92. Os autovalores da matriz

$$\begin{pmatrix} 1 & 4 \\ 4 & -5 \end{pmatrix}$$

são 3 e -7, ambos reais. A matriz

$$\begin{pmatrix} -3 & 2 & 1 \\ 2 & -3 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

tem autovalores $-\sqrt{3}, \sqrt{3}, -5$. ◀

Definição 7.93 (matriz ortogonalmente diagonalizável)**.** Uma matriz A é *ortogonalmente diagonalizável* se $A = PDP^{-1}$, com D diagonal e P ortogonal. ♦

Teorema 7.94. *Uma matriz é ortogonalmente diagonalizável se e somente se é simétrica.*

Demonstração. ($\Rightarrow$ apenas) Seja A uma matriz ortogonalmente diagonalizável, com $A = PDP^{-1}$. Usando o fato de que $P^{-1} = P^T$, mostramos que A é simétrica

$$A = PDP^T = PD^TP^T = (P^T)D^TP^T = (PDP^T)^T = A^T. \qquad \blacksquare$$

Exemplo 7.95. A matriz

$$A = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}$$

é simétrica, e portanto diagonalizável. De fato, $A = PDP^{-1}$,

$$A = \begin{pmatrix} 1 & 1 \\ 1-\sqrt{2} & 1+\sqrt{2} \end{pmatrix} \begin{pmatrix} -\sqrt{2}-1 & 0 \\ 0 & \sqrt{2}-1 \end{pmatrix} \begin{pmatrix} \frac{\sqrt{2}+1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} \\ \frac{\sqrt{2}-1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} \end{pmatrix}. \qquad \blacktriangleleft$$

As colunas da matriz P são ortogonais:

$$\begin{pmatrix} 1 & 1-\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 \\ 1+\sqrt{2} \end{pmatrix} = 0.$$

Corolário 7.96. *Toda matriz simétrica é diagonalizável.*

Se uma matriz simétrica $A = PDP^{-1}$, nem sempre as colunas de P obtidas imediatamente do processo de diagonalização serão ortogonais. Duas colunas serão ortogonais quando pertencerem a autovalores distintos.

Teorema 7.97. *Seja A uma matriz simétrica. Quaisquer dois autovetores pertencentes a autovalores* distintos *de A são ortogonais entre si.*

Podemos, no entanto, usar o processo de ortogonalização de Gram-Schmidt para obter uma nova matriz ortogonal que também diagonaliza a mesma matriz simétrica.

Teorema 7.98. *Seja A uma matriz simétrica, com $A = PDP^{-1}$. Seja R o resultado do processo de Gram-Schmit aplicado nas colunas de A. Seja S a matriz obtida de R pela normalização dos vetores em cada coluna. Então*

$$\begin{aligned} A &= RDR^{-1} = RDR^T \\ &= SDS^{-1} = SDS^T. \end{aligned}$$

★ 7.6 Produto interno em espaços complexos

Nesta seção tratamos brevemente de espaços sobre corpos complexos. Será necessário relembrar, portanto, a definição e notação para conjugado.

Definição 7.99 (Conjugado de binômio e de número complexo)**.** Seja $a + z$ um binômio. Seu *conjugado* é $a - z$. Se a é real e $z = bi$ imaginário, então $a + z = a + bi$ é complexo, e o *conjugado* de $x = a + bi$ é $\overline{x} = a - bi$. ♦

No início do Capítulo demos a definição de produto interno para espaços vetoriais sobre o corpo dos reais. Em espaços complexos definimos produto interno de forma mais geral: o produto não precisa ser comutativo, mas deve respeitar a seguinte regra de simetria:

- **simetria:** $\langle \mathbf{u}, \mathbf{v} \rangle = \overline{\langle \mathbf{v}, \mathbf{u} \rangle}$.
- **positividade:** $\langle \mathbf{v}, \mathbf{v} \rangle \geq 0$, e $\langle \mathbf{0}, \mathbf{0} \rangle = 0$.
- **linearidade:** para todo escalar k e vetores $\mathbf{u}, \mathbf{v}, \mathbf{w}$,

$$\langle \mathbf{u} + \mathbf{w}, \mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{w}, \mathbf{v} \rangle$$
$$\langle k\mathbf{u}, \mathbf{v} \rangle = k \langle \mathbf{u}, \mathbf{v} \rangle$$

Observamos que para números $a + bi$ onde $b = 0$, esta definição equivale àquela que demos para espaços reais. O produto interno deve ser linear somente no primeiro argumento. Para espaços reais, isso implica na linearidade também no segundo argumento, porque nesses espaços o produto é comutativo. Em espaços complexos, o produto não é comutativo.

Exemplo 7.100. Em $\mathbb{C}^n$,

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1\overline{y_1} + x_2\overline{y_2} + \cdots + x_n\overline{y_n}$$

é produto interno. ◄

Exemplo 7.101. No espaço de funções contínuas de $\mathbb{C}$ em $\mathbb{C}$ definidas no intervalo $[0, 1]$,

$$\langle f, g \rangle = \int_a^b f(x)\overline{g(x)}dx$$

é produto interno. ◄

Teorema 7.102. *Sejam A uma matriz complexa $m \times n$, $\mathbf{x} \in \mathbb{C}^n$, $\mathbf{y} \in \mathbb{C}^m$, e seja $\langle \cdot, \cdot \rangle$ o produto interno complexo definido no exemplo 7.101. Então*

$$\langle A\mathbf{x}, \mathbf{y} \rangle = \left\langle \mathbf{x}, A^H\mathbf{y} \right\rangle .$$

7.7 Aplicações

7.7.1 Solução de sistemas lineares e mínimos quadrados [distância; projeção]

Se um sistema $A\mathbf{x} = \mathbf{b}$ é incompatível, podemos querer encontrar algum vetor $\mathbf{x}$ tão próximo quanto possível de uma solução para o sistema. Definimos que um vetor $\mathbf{z}$ é o mais próxima possível de uma

solução se minimiza o quadrado do erro. O erro de que falamos é a distância entre $\mathbf{b}$ e $A\mathbf{z}$, ou seja,

$$\begin{aligned} d(\mathbf{b}, A\mathbf{z})^2 &= ||\mathbf{b} - A\mathbf{z}||^2 \\ &= \sum [b_i - (A\mathbf{x})_i]^2. \end{aligned}$$

Definição 7.103 (Solução minimizando quadrados)**.** Uma solução minimizando quadrados para o sistema $A\mathbf{x} = \mathbf{b}$ é o vetor $\mathbf{z}$ que minimiza $||\mathbf{b} - A\mathbf{z}|| \ > \ ||\mathbf{b} - A\mathbf{y}||$. ♦

Suponha que $A\mathbf{x} = \mathbf{b}$ é incompatível, e que W é o espaço coluna de A. Certamente $\mathbf{b} \notin W$, de outra forma $\mathbf{b}$ seria combinação linear das colunas de A, e os coeficientes desta combinação linear nos dariam uma solução para o sistema.

Tendo definido a noção de distância neste espaço, no entanto, observamos que no espaço coluna de A podemos tomar o vetor mais próximo a $\mathbf{b}$: este será obtido a partir da projeção ortogonal de $\mathbf{b}$ em W. Assim, se resolvermos

$$A\mathbf{x} = \mathbf{b} - \text{Proj}_W(\mathbf{b})$$

obteremos a solução minimizando quadrados.

Nem sempre, no entanto, é fácil determinar $\text{Proj}_W(\mathbf{b})$. O Teorema 7.104 permite determinar de maneira simples uma solução minimizando quadrados.

Teorema 7.104. *Qualquer solução minimizando quadrados para $A\mathbf{x} = \mathbf{b}$ é uma solução para o sistema $A^T A\mathbf{x} = A^T\mathbf{b}$, e qualquer solução para $A^T A\mathbf{x} = A^T\mathbf{b}$ é solução minimizando quadrados para $A\mathbf{x} = \mathbf{b}$.*

Exemplo 7.105. O sistema

$$\begin{pmatrix} -1 & 1 \\ 3 & 2 \\ 2 & 3 \end{pmatrix} \mathbf{x} = \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}$$

é incompatível. Para encontrarmos uma solução minimizando quadrados, calculamos

$$A^T A = \begin{pmatrix} -1 & 2 \\ 3 & 1 \\ 2 & 3 \end{pmatrix},$$

e resolvemos $A^T A\mathbf{x} = A^T\mathbf{b}$:

$$\begin{pmatrix} 14 & 7 \\ 7 & 14 \end{pmatrix} \mathbf{x} = \begin{pmatrix} 9 \\ 10 \end{pmatrix}$$

e obtemos a solução

$$\mathbf{x} = \frac{1}{21} \begin{pmatrix} 8 \\ 11 \end{pmatrix},$$

que é solução minimizando quadrados para o sistema original. ◀

7.7.2 Covariância e correlação [produto interno; ângulo]

O conjunto de todas as variáveis aleatórias relacionadas a um mesmo experimento que tenham variância finita formam um espaço vetorial com as operações usuais de soma de variáveis aleatórias e multiplicação de uma variável por número real. (veja o exemplo 1.39 e o exercício 30). A esperança de uma variável aleatória é uma transformação linear que podemos usar para determinar o valor ao redor do qual uma

variável aleatória flutua – mas a esperança não nos diz quão distantes os valores podem ser entre si. Nos interessa, então, a distância entre a variável aleatória e sua esperança, $\mathbb{E}(|X - \mathbb{E}(X)|)$. Como a função módulo impõe certas dificuldades, usamos a raiz quadrada do quadrado de $X - \mathbb{E}(X)$, e definimos o *desvio padrão*.

Definição 7.106 (Desvio padrão)**.** Seja X uma variável aleatória. Então o *desvio padrão* de X é

$$\sigma_X = +\sqrt{[\mathbb{E}(X - \mathbb{E}(X))]^2}$$ ♦

Exemplo 7.107. ◀

Sejam X e Y duas variáveis aleatórias relacionadas ao mesmo experimento. Definimos o produto interno

$$\langle X, Y\rangle = \mathbb{E}(XY) = \sum_x \sum_y xy \Pr[X = x] \Pr[Y = y].$$

Exemplo 7.108. ◀

Estamos agora interessados em quão semelhante é a variação de duas variáveis aleatórias – se valores altos de uma correspondem com os valores altos da outra, e vice-versa. Usamos novamente a distância entre a variável e sua esperança, $X - \mathbb{E}(X)$ e $Y - \mathbb{E}(Y)$. Intuitivamente, se o produto interno dessas distâncias for grande, então X e Y são fortemente correlacionadas. Se for zero, as variáveis não são correlacionadas.

Definição 7.109 (Covariância e Variância)**.** A *covariância* entre X e Y é o produto interno da variável aleatória $X - \mathbb{E}(X)$ com a variável aleatória $Y - \mathbb{E}(Y)$:

$$\begin{aligned}\operatorname{cov}(X, Y) &= \langle X - \mathbb{E}(X), Y - \mathbb{E}(Y)\rangle \\ &= \mathbb{E}\big[(X - \mathbb{E}(X))(Y - \mathbb{E}(Y))\big]\end{aligned}$$

A *variância* de uma variável aletória X, que denotamos por σ_X^2, é a covariância de X com ela mesma.

$$\begin{aligned}\operatorname{cov}(X, X) &= \langle X - \mathbb{E}(X), X - \mathbb{E}(X)\rangle \\ &= \mathbb{E}\big[(X - \mathbb{E}(X))(X - \mathbb{E}(X))\big] \\ &= \sigma_X^2\end{aligned}$$ ♦

Covariância zero não implica, no entanto, em independência, como ilustrado no exemplo 7.110.

Exemplo 7.110. Sejam A, B e C variáveis aletórias definidas da seguinte forma:

$$\begin{aligned}&\Pr[A = 0] = \frac{1}{2}, \quad \Pr[A = 1] = \frac{1}{2} \\ &\Pr[B = -1] = \frac{1}{2}, \Pr[B = 1] = \frac{1}{2} \\ &C = AB\end{aligned}$$

É fácil verificar que $\operatorname{cov}(A, B) = 0$ (obseve que a esperança de A é $1/2$, e a de C é 0). No entanto, por definição, para que A e C sejam independentes seria necessário que

$$\Pr[C = c | A = a] = \Pr[C = c],$$

para todos a e c. Se tomarmos $a = 0$ e $c = 1$,

$$\Pr[C = 1|A = 0] = \Pr[AB = 1|A = 0] = 0$$
$$\Pr[C = 1] = \Pr[AB = 1] = \frac{1}{4},$$

e as variáveis A e C não são independentes, embora tenham covariância zero. ◀

A magnitude da covariância não é fácil de interpretar, portanto faz sentido que normalizemos para obter um valor entre -1 e 1, como observamos ao definir ângulos na seção 7.2.

Definição 7.111 (Coeficiente de correlação)**.** Se definirmos $\Delta_X = (x_1 - \mathbb{E}(X), \ldots, x_n - \mathbb{E}(X))$ e $\Delta_Y = (y_1 - \mathbb{E}(Y), \ldots, y_n - \mathbb{E}(Y))$, o *coeficiente de correlação* entre X e Y é o cosseno do ângulo[3] entre Δ_X e Δ_Y.

$$\begin{aligned}
\rho(X, Y) &= \frac{\langle X - \mathbb{E}(X), Y - \mathbb{E}(Y)\rangle}{||X - \mathbb{E}(X)||\,||Y - \mathbb{E}(Y)||} \\
&= \frac{\langle X - \mathbb{E}(X), Y - \mathbb{E}(Y)\rangle}{\sqrt{\langle X - \mathbb{E}(X), X - \mathbb{E}(X)\rangle}\,\sqrt{\langle Y - \mathbb{E}(Y), Y - \mathbb{E}(Y)\rangle}} \\
&= \frac{\mathbb{E}\left[(X - \mathbb{E}(X))(Y - \mathbb{E}(Y))\right]}{\sqrt{\mathbb{E}(X - \mathbb{E}(X))^2}\,\sqrt{\mathbb{E}(Y - \mathbb{E}(Y))^2}} \\
&= \frac{\mathbb{E}\left[(X - \mathbb{E}(X))(Y - \mathbb{E}(Y))\right]}{\sigma_X \sigma_Y} \\
&= \frac{\operatorname{cov}(X, Y)}{\sigma_X \sigma_Y}.
\end{aligned}$$

♦

ALém de interpretar o coeficiente de correlação como ângulo entre os vetores de dados, podemos observar outro significado para ele. *Regressão linear* é uma forma de modelar a relação entre duas variáveis a partir de dados observados, quando supomos que as duas variáveis são relacionadas, e que esta relação é linear. Uma linha de regressão linear é uma equação da forma

$$Y = a + bX.$$

Pode-se obter por exemplo a reta que melhor se ajusta aos dados usando o método dos *mínimos quadrados* (ou seja, minimizando a soma dos quadrados das distâncias de cada ponto até a reta, na direção vertical).

Se obtivermos uma linha de regressão que nos permita predizer X a partir de Y e outra que nos permita predizer Y a partir de X, o coeficiente de correlação é o cosseno do ângulo entre estas duas linhas de regressão ($a + bX$ e $\alpha + \beta Y$).

★ 7.7.3 Covariância [produto interno; matriz de Gram]

Se $\mathbf{X}$ é um vetor onde cada elemento é uma variável aleatória, chamamos a matriz de Gram de $\mathbf{X}$ de *matriz de covariância*:

$$\Sigma_{ij} = \operatorname{cov}(X_i, X_j) = \langle X_i, X_j\rangle = \mathbb{E}[(X_i - \mathbb{E}(X_i))(X_j - \mathbb{E}(X_j))].$$

[3] Há diversas maneiras de interpretar o coeficiente de correlação. Um artigo de Josph Lee Rogers e W. Alan Nicewander mostra treze delas [RN88].

Desta forma, temos

$$\Sigma = \begin{pmatrix} \mathbb{E}[(X_1 - \mathbb{E}(X_1))(X_1 - \mathbb{E}(X_1))] & (X_1 - \mathbb{E}(X_1))(X_2 - \mathbb{E}(X_2)) & \cdots & (X_1 - \mathbb{E}(X_1))(X_n - \mathbb{E}(X_n)) \\ \mathbb{E}[(X_2 - \mathbb{E}(X_2))(X_1 - \mathbb{E}(X_1))] & (X_2 - \mathbb{E}(X_2))(X_2 - \mathbb{E}(X_2)) & \cdots & (X_2 - \mathbb{E}(X_2))(X_n - \mathbb{E}(X_n)) \\ \vdots & \vdots & \ddots & \vdots \\ \mathbb{E}[(X_n - \mathbb{E}(X_n))(X_1 - \mathbb{E}(X_1))] & (X_n - \mathbb{E}(X_n))(X_2 - \mathbb{E}(X_2)) & \cdots & (X_n - \mathbb{E}(X_n))(X_n - \mathbb{E}(X_n)) \end{pmatrix}$$

A diagonal da matriz de covariância claramente nos informa as variâncias: $\Sigma_{ii} = \text{cov}(X_i, X_i) = \sigma^2(X_i)$.

★ 7.7.4 Otimização linear (*affine scaling*) [projeção, núcleo, escala]

(Esta seção é apenas um rascunho)

Este exemplo trata de otimização linear, já abordada na seção 4.8.2 (naquela seção pode-se encontrar a definição de prblema de otimização linear – definição 4.110 – e um exemplo).

Há um método para resolução de problemas de programação linear no qual a operação de projeção é essencial.

A idéia é seguir o gradiente do objetivo até chegar a uma solução ótima. Suponha que inicialmente temos uma solução inicial $\mathbf{x}^0$. Observe que por solução viável entendemos uma solução do sistema

$$A\mathbf{x} = \mathbf{b}.$$

Os pontos $\mathbf{x}$ são os pontos dentro da região viável.

O método de *affine scaling* começa com uma solução inicial x^0, muda a escala do problema, mudando também a escala de x^0 e obtendo y^0. Em seguida obtem uma solução melhor y^1. Desfaz a mudança de escala e obtem uma nova solução x^1 para o problema original.

Usaremos um exemplo prático no desenvolvimento. Queremos resolver o seguinte problema:

$$\begin{aligned} \max\ & 2x_1 + x_2 \\ \text{sujeito a } & x_1 - x_2 \leq 2 \\ & x_1 + 2x_2 \leq 8 \\ & x_2 \leq 3 \\ & \mathbf{x} \geq \mathbf{0}. \end{aligned}$$

Podemos expressá-lo na forma $A\mathbf{x} = \mathbf{b}$, já que

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \leq b$$

é o mesmo que

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n + s = b, \quad s \geq 0$$

Temos portanto

$$\begin{aligned} \max\ & 2x_1 + x_2 \\ \text{sujeito a } & x_1 - x_2 + x_3 = 2 \\ & x_1 + 2x_2 + x_4 = 8 \\ & x_2 + x_5 = 3 \\ & \mathbf{x} \geq \mathbf{0}, \end{aligned}$$

e temos

$$A = \begin{pmatrix} 1 & -1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} 2 \\ 8 \\ 3 \end{pmatrix}.$$

O problema com o qual iniciamos envolvia apenas duas variáveis, e por isso podíamos reprsentá-lo facilmente no plano. Mantendo em mente que x_3, x_4, x_5 são variáveis de folga podemos, mesmo na forma de igualdade, visualizar as restrições no plano.

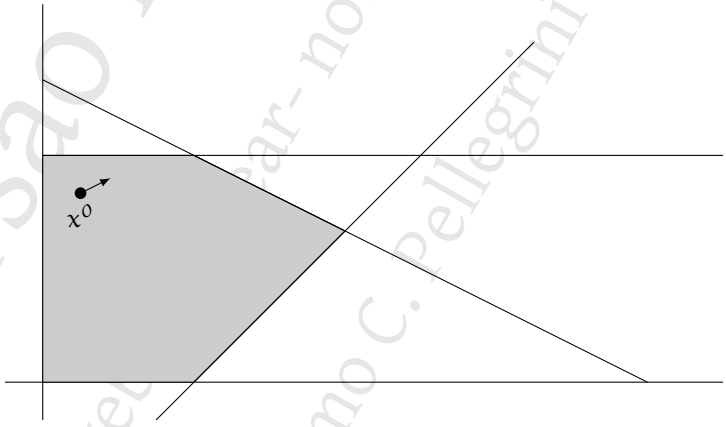
Suponha que tenhamos começado com a solução $x_1 = 1/2$, $x_2 = 5/2$. Para representar este ponto com variáveis de folga, escrevemos

$$\mathbf{x}^0 = \begin{pmatrix} 1/2 \\ 5/2 \\ 4 \\ 5/2 \\ 1/2 \end{pmatrix},$$

com $x_3 = 4$, $x_4 = 5/2$, e $x_5 = 1/2$. Estas são as folgas de cada desigualdade quando $x_1 = 1/2$ e $x_2 = 5/2$, porque

$$\begin{array}{rrr} x_1 - x_2 + x_3 = 2 & x_1 + 2x_2 + x_4 = 8 & x_2 + x_5 = 3 \\ (1/2) - (5/2) + x_3 = 2 & (1/2) + 2(5/2) + x_4 = 8 & (5/2) + x_5 = 3 \\ x_3 = 4 & x_4 = 5/2 & x_5 = 1/2 \end{array}$$

Podemos calcular o gradiente da função objetivo, ∇f, que é um vetor, e somá-lo a $\mathbf{x}^0$ para tentar chegar mais perto da solução ótima. No entanto, se $\mathbf{x}^0$ estiver muito perto da borda, seguir o gradiente do objetivo poderá não ser útil:



Mudamos a escala de $\mathbf{x}_0$ e das restrições, de forma a transformar o ponto $\mathbf{x}_0$ no ponto $(1, 1, \ldots, 1)^T$. Para isto usamos a matriz de escala

$$D = \operatorname{diag}(x_1, x_2, \ldots, x_n) = \begin{pmatrix} x_1 & 0 & \cdots & 0 \\ 0 & x_2 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & x_n \end{pmatrix}.$$

O ponto modificado é $\mathbf{y}^0 = D^{-1}\mathbf{x}^0$, logo

$$\mathbf{y}^0 = D^{-1}\begin{pmatrix} 1/2 \\ 5/2 \\ 4 \\ 5/2 \\ 1/2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Como aplicamos a transformação no ponto, podemos reescrever $A\mathbf{x} = \mathbf{b}$ como $A(D\mathbf{y}) = \mathbf{b}$, ou

$$(AD)\mathbf{y} = \mathbf{b}.$$

Renomeamos

$$Q = AD = \frac{1}{2}\begin{pmatrix} 1 & -5 & 8 & 0 & 0 \\ 1 & 10 & 0 & 5 & 0 \\ 0 & 5 & 0 & 0 & 1 \end{pmatrix}$$

Como $\mathbf{x} = D\mathbf{y}$, a função objetivo passa a ser

$$\begin{aligned} \mathbf{c}^T\mathbf{x} &= (2,1,0,0,0)\mathbf{x} \\ &= (2,1,0,0,0)(D\mathbf{y}) \\ &= \left[(2,1,0,0,0)D\right]\mathbf{y} \\ &= (1,5/2,0,0,0)\mathbf{y}. \end{aligned}$$

e temos um novo problema de otimização

$$\begin{aligned} &\max\ y_1 + \frac{5}{2}y_2 \\ \text{sujeito a}\ \ &Q\mathbf{y} = \mathbf{b} \\ &\mathbf{y} \geq \mathbf{0} \end{aligned}$$

Assim como $\mathbf{x}^0$ era viável, $\mathbf{y}^0$ também é para este novo problema.

As restrições do novo sistema são

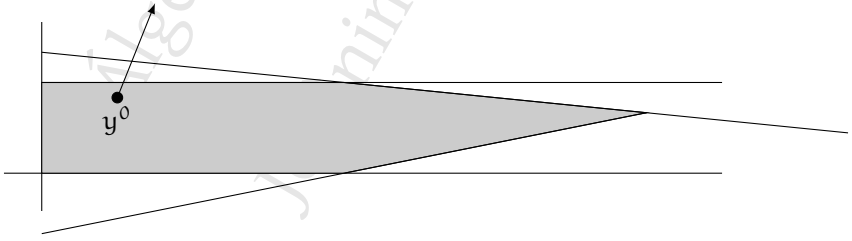
$$\begin{aligned} y_1 - 5y_2 + 8y_3 &= 4 \\ y_1 + 10y_2 + 5y_4 &= 16 \\ 5y_2 + y_5 &= 6 \end{aligned}$$

ou, substituindo

$$\begin{aligned} z_3 &= 8y_3 \\ z_4 &= 5y_4, \end{aligned}$$

$$\begin{aligned} y_1 - 5y_2 + z_3 &= 4 \\ y_1 + 10y_2 + z_4 &= 16 \\ y_2 + z_5 &= 6/5 \end{aligned}$$

Se tratarmos z_3, z_4, z_5 como variáveis de folga, estas restrições definem a região representada n afigura a seguir.



Como $\mathbf{x}_0 = D\mathbf{y}$, o gradiente de $c^T\mathbf{x}_0$ é

$$\begin{aligned}\nabla c^T\mathbf{x}_0 &= \nabla c^T D\mathbf{y} \\ &= c^T D \\ &= (2,1)\begin{pmatrix} 1/2 & 0 \\ 0 & 5/2 \end{pmatrix} \\ &= (1, 5/2).\end{aligned}$$

O operador que projeta no kernel de A é

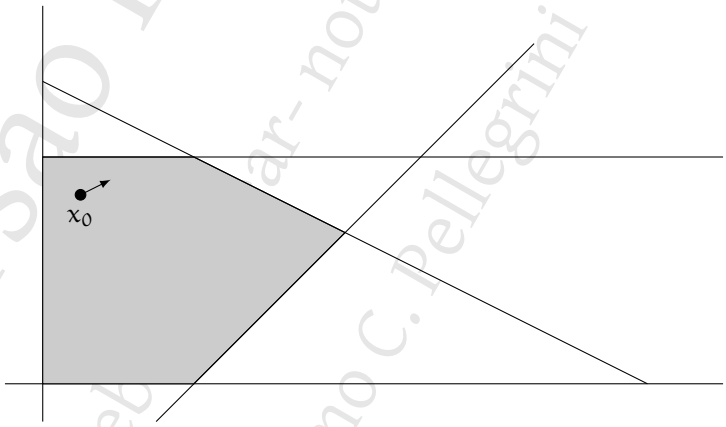
$$P = \mathcal{I} - DA^T\left(AD^2A^T\right)^{-1}AD.$$

Agora sim, um passo na direção do gradiente do objetivo certamente será benéfico. Há, no entanto, um problema: não sabemos que tamanho de passo podemos dar! Se o passo for muito longo, poderemos obter um ponto fora da região viável.

Uma solução para isto é não andar diretamente na direção do gradiente. Primeiro projetamos o gradiente no espaço nulo (núcleo) de A:

$$\mathbf{d} = \mathrm{Proj}_{\mathrm{nul}\,A}\left(\nabla f\right)$$

Agora temos uma direção $\mathbf{d}$ (um vetor pode ser encarado como uma "direção") para a qual podemos mover nossa solução. Esta projeção terá a mesma direção do gradiente, portanto melhorará a solução. Mas como foi projetada no espaço nulo de A, o novo vetor continuará sendo solução para $A\mathbf{x} = \mathbf{b}$, porque o vetor projetado no espaço nulo é solução de $A\mathbf{x} = \mathbf{0}$ (por definição de espaço nulo), e a soma de uma solução do sistema homogêneo com uma solução do sistema não-homogêneo continua sendo solução para o não-homogêneo.



Exercícios

Ex. 207 — Mostre que são ou que não são produtos internos:

a) Em $C^1[0,1]$, $\langle f, g\rangle = \int_0^1 f'(x)g'(x)dx$.

b) Em $C^1[0,1]$, $\langle f, g\rangle = \int_0^1 f'(x)g(x)dx$.

c) Em $C^1[0,1]$, $\langle f, g\rangle = f'(x)g'(x)$.

d) Em $C^1[0,1]$, $\langle f, g\rangle = (fg)'(x)$.

e) Em $C^1[0,1]$, $\langle f, g\rangle = f'(x)g'(x)\int_0^1 f(x)g(x)dx$.

f) Em $C^0[0,1]$, $\langle f, g\rangle = (f+g)^2$.

g) Em $C^0[0,1]$, $\langle f, g\rangle = \int_0^1 \operatorname{sen}(x)f(x)g(x)dx$.

h) Em $C^0[0,1]$, $\langle f, g\rangle = e^{f(x)+g(x)}$.

i) Em $C^0[0,1]$, $\langle f, g\rangle = e^{f(x)} + e^{g(x)}$.

j) Em $M_{n\times n}$, $\langle A, B\rangle = \det(A) + \det(B)$.

k) Em $M_{n\times n}$, $\langle A, B\rangle = \operatorname{Tr}(AB)$.

l) Em $M_{n\times n}$, $\langle A, B\rangle = \prod a_{ij}b_{ji}$ (note que os índices em A e B são trocados: $a_{i,j}$ e $b_{j,i}$).

m) Em $\mathbb{R}_n[x]$, $\langle p(x), q(x)\rangle = r(x)$, onde

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + b_0 \\ q(x) &= b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \\ r(x) &= a_n b_1 x^n + a_{n-1}b_2 x^{n-1} + \cdots + a_1 b_{n-1} x + a_0 b_n \end{aligned}$$

n) Em $\mathbb{R}_n[x]$, $\langle p(x), q(x)\rangle = r(x)$, onde

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + b_0 \\ q(x) &= b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \\ r(x) &= \prod_{i=0}^{n} a_i b_i x^n + \prod_{i=0}^{n-1} a_i b_i x^{n-1} + \cdots + a_1 a_0 b_1 b_0 x + a_0 b_0 \end{aligned}$$

o) Em $\mathbb{R}_n[x]$, $\langle p(x), q(x)\rangle = r(x)$, onde

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + b_0 \\ q(x) &= b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \\ r(x) &= |a_n b_n| x^n + |a_{n-1} b_{n-1}| x^{n-1} + \cdots + |a_1 b_1| x + |a_0 b_0| \end{aligned}$$

p) Em $\mathbb{R}^n$, $\langle \mathbf{x}, \mathbf{y}\rangle = \theta \mathbf{x}^T \mathbf{y}$, onde θ é o ângulo entre $\mathbf{x}$ e $\mathbf{y}$.

q) Em $\mathbb{R}^n$, $\langle \mathbf{x}, \mathbf{y}\rangle = \alpha \mathbf{x}^T \mathbf{y}$, onde α é uma constante.

r) Em $\mathbb{R}^n$, $\langle \mathbf{x}, \mathbf{y}\rangle = \det(\mathbf{x}\mathbf{y}^T) + \det(\mathbf{y}\mathbf{x}^T)$.

s) Em $\mathbb{C}^n$, $\langle \mathbf{x}, \mathbf{y}\rangle = \det(\overline{\mathbf{x}}\mathbf{y}^T)$.

t) Em $\mathbb{R}^n$, $\langle \mathbf{x}, \mathbf{y}\rangle = \operatorname{Tr}(\mathbf{x}\mathbf{y}^T)$.

Ex. 208 — As sequências reais convergentes formam um espaço vetorial. Neste espaço, defina o produto interno

$$f\big((a_n), (b_n)\big) = (AB)^2,$$

quando $(a_n) \to A$ e $b_n \to B$. Determine se f é produto interno.

Ex. 209 — Para que valores de z o conjunto de funções $\{\text{sen } \frac{z\pi x}{L}\}$, definidas em $[0, L]$, é ortogonal?

Ex. 210 — Prove que em qualquer espaço vetorial, os vetores $||\mathbf{u}||\mathbf{v} + ||\mathbf{v}||\mathbf{u}$ e $||\mathbf{u}||\mathbf{v} - ||\mathbf{v}||\mathbf{u}$ são ortogonais.

Ex. 211 — Demonstre a proposição 7.16.

Ex. 212 — Demonstre o teorema 7.40.

Ex. 213 — Explique como encontrar qualquer quantidade de vetores ortogonais em $C[-\pi, \pi]$ usando o produto interno usual $\int_{-\pi}^{\pi} f(x)g(x)dx$.

Ex. 214 — Seja A uma matriz diagonalizada (suas entradas diagonais são seus autovalores, o resto da matriz tem zeros). Que matrizes serão ortogonais a A se usarmos o produto de Frobenius?

Ex. 215 — Seja

$$F = \{1, \cos x, \text{sen } x, \cos^2 x\}$$

um conjunto de funções reais.

i) Prove que F é um conjunto LI.

ii) F gera um espaço vetorial. Encontre para este espaço uma base ortonormal com relação ao produto

$$\langle f, g\rangle = \frac{1}{2\pi}\int_0^{2\pi} f(x)g(x)dx.$$

Ex. 216 — Como a base do exemplo 7.62 foi obtida? (Que relação ela tem com a base canônica?)

Ex. 217 — Use o processo de ortogonalização de Gram-Schmidt para obter uma base para o espaço das matrizes 2×2, a partir da base

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

Ex. 218 — Em $C^0[1, e]$, as funções $f_1(x) = x^{-1}$, $f_2(x) = \cos(x)$ e $f_3(x) = \ln(x)$ geram um subespaço. Use o processo de ortogonalização de Gram-Schmidt para obter uma base *ortonormal* para este subespaço.

Ex. 219 — Na demonstração da proposição 7.85 dissemos que Proj $\circ$ Proj $=$ Proj. Demonstre.

Ex. 220 — Se uma matriz T representa uma projeção, é verdade que T^T também é um operador de projeção?

Ex. 221 — O espeço $\mathbb{R}_5[x]$ pode ser decomposto em dois outros espaços: $\mathbb{R}_3[x]$ e U, tal que U contém o zero e os polinômios de grau 4 e 5. A derivada segunda sempre levará qualquer membro de $\mathbb{R}_5[x]$ em $\mathbb{R}_3[x]$. No entanto, a derivada não é idempotente:

$$\frac{d^2}{dx^2}x^5 = 20x^3,$$

mas quando a aplicamos novamente, obtemos $d^2/dx^2(20x^3) = 120x$. Explique. Depois, exiba uma verdadeira projeção de $\mathbb{R}_5[x]$ em $\mathbb{R}_3[x]$ usando diferenciação.

★ **Ex. 222 —** Seja (a_n) a sequência das potências de dois, ou seja, $a_n = 2^n$:

$$\begin{aligned} a_1 &= 1/2 \\ a_2 &= 1/4 \\ a_3 &= 1/8 \\ &\vdots \end{aligned}$$

Encontre uma sequência ortogonal a esta.

Ex. 223 — Seja r uma reta em $\mathbb{R}^2$. Mostre que há infinitos operadores que fazem projeção em r.

Ex. 224 — Demonstre o teorema 7.83.

Ex. 225 — No espaço de funções contínuas definidas no intervalo $[-a, a]$, qual é o complemento ortogonal do subespaço das funções constantes?

Ex. 226 — Encontre duas funções LI em ℓ_2, obtendo assim um subespaço S. Depois use o processo de Gram-Schmidt para encontrar uma base ortogonal para S.

Ex. 227 — Definimos espaço vetorial no primeiro Capítulo com duas operações – uma entre vetores (soma) e uma entre vetor e escalar (multiplicação). Agora considere um espaço vetorial qualquer com produto interno. Defina "produto de dois vetores" como

$$\mathbf{v} \otimes \mathbf{w} = \langle \mathbf{v}, \mathbf{w} \rangle \, [\mathbf{v} + \mathbf{w}]$$

Um espaço vetorial com as operações de soma de vetores e o produto $\otimes$ é um corpo?

Ex. 228 — Considere o espaço $C^0[a, b]$, das funções reais contínuas no intervalo $[a, b]$. Seja h uma função neste espaço (e portanto contínua em $[a, b]$). Determine se são produto interno nesse espaço:

a) $\int_a^b f(x)g(x)h(x)dx$

b) $\int_a^b h(y) \left(\int_a^b f(x)g(x)dx \right) dy$

c) $\int_{a+\varepsilon}^{b-\varepsilon} h(y) \left(\int_a^b f(x)g(x)dx \right) dy$, com $\varepsilon < b - a$.

d) $f(b)g(b) - f(a)g(a)$.

e) $f(g(\frac{a+b}{2})) + g(f(\frac{a+b}{2}))$

f) $\lim_{x\to\infty} \frac{f(x)g(x)}{f(x)+g(x)}$

g) $\lim_{x\to\infty} \frac{f(x)g(x)}{|f(x)|+|g(x)|}$

h) $\lim_{x\to\infty} \frac{f(x)g(x)}{|f(x)|+|g(x)|+1}$

Ex. 229 — Determine a projeção ortogonal de $f(x) = x$ em $g(x) = \text{sen}(x)$, e mostre a função ortogonal a $\text{sen}(x)$ que se obtém desta forma.

Ex. 230 — Podemos definir espaços de funções contínuas $C[a, b]$ para qualquer intervalo $[a, b]$. Considere as funções

$$f(x) = x$$
$$g(x) = \frac{1}{x} - 1$$

Determine a e b tais que f e g sejam ortogonais em $C[a, b]$, usando o produto interno usual $\int_a^b f(x)g(x)dx$.

Ex. 231 — No exemplo 7.14 exibimos um produto interno em para espaços de ciclos em um grafo. Podemos criar outro produto interno, trocando a soma em $\mathbb{R}$ pela soma em $\mathbb{Z}_2$ (ou seja, trocando soma usual por ou-exclusivo). Qual passaria a ser o significado desse produto interno? E o significado de dois grafos serem ortogonais?

Ex. 232 — Releia a definição de matriz de Pascal no Exercício 140 (página 212) e dê uma forma fechada para o produto de duas de suas colunas i e j, em termos apenas dos índices i e j.

Ex. 233 — Mostre que ângulo e distância medem, de maneiras diferentes, o mesmo conceito em grafos: dados grafos A, B, C, D, prove que se o ângulo entre A e B é maior que o ângulo entre C e D, então $d(A, B) > d(C, D)$.

Ex. 234 — Prove que qualquer isometria central é a composição de no máximo tres reflexões.

Ex. 235 — Prove que qualquer isometria (central ou não) com um ponto fixo é uma rotação ou uma reflexão.

Ex. 236 — Sejam A e B dois grafos de ciclos disjuntos, não ortogonais. Quem é o grafo ortogonal a A que você consegue obter através de uma projeção ortogonal? Qual seria o resultado do processo de ortogonalização de Gram-Schmidt em grafos de ciclos?

★ **Ex. 237 —** Verifique que o Teorema 12.20 vale para matrizes complexas.

Ex. 238 — Seja A uma matriz quadrada *qualquer* com colunas $a_1, \ldots, a_n$. Mostre que

$$|\det A| \leq \prod \|a_i\|$$

★ **Ex. 239 —** Leia as seguintes definições.

Definição 7.112 (combinação positiva)**.** Uma *combinação positiva* de um conjunto de vetores é uma combinação linear destes vetores, tendo coeficientes não negativos. ⧫

Definição 7.113 (cone convexo)**.** O *cone convexo* gerado por um conjunto de vetores é o conjunto de todas as combinações positivas daquele conjunto. ⧫

Usando estas definições, prove o Lema de Farkas para $\mathbb{R}^2$, usando argumento geométrico[4].

Lema 7.114 (de Farkas)**.** *Sejam A uma matriz e $\mathbf{b}$ um vetor, sendo que o número de linhas de A é igual à quantidade de elementos de $\mathbf{b}$. Então exatamente um dos dois sistemas a seguir tem solução.*

[4] O Lema de Farkas é válido em $\mathbb{R}^n$, mas a demonstração é mais difícil do que a pedida aqui para $\mathbb{R}^2$

i) $A\mathbf{x} = \mathbf{b}$, *para algum* $\mathbf{x} \geq \mathbf{0}$.

ii) $\mathbf{y}^T A \geq \mathbf{0}$ *para algum* $\mathbf{y}$ *tal que* $\mathbf{b}^T\mathbf{y} < 0$.

Capítulo 8

Operadores Ortogonais e Normais

Este Capítulo está incompleto

8.1 Operadores Ortogonais

Estudamos agora os operadores lineares que preservam distâncias e normas de vetores, e que portanto representam *movimentos rígidos*.

Definição 8.1 (isometria)**.** Em um espaço V com produto interno, uma função $f : V \to V$ é uma *isometria* se preserva distâncias, ou seja,

$$d(\mathbf{v}, \mathbf{w}) = d(T\mathbf{v}, T\mathbf{w}).$$

Uma isometria T é *central* se preserva a origem, isto é, se $T(\mathbf{0}) = \mathbf{0}$, e é *não central* caso contrário.

Isometrias são também chamadas de *operadores ortogonais*. ♦

Trivialmente, como isometrias preservam distâncias, devem também preservar a distância entre um vetor e a origem (ou seja, sua norma).

Proposição 8.2. *Isometrias preservam norma de vetores, ou seja, se T é uma isometria em um espaço V, então para todo $\mathbf{v} \in V$,*

$$\langle \mathbf{v}, \mathbf{v} \rangle = \langle T\mathbf{v}, T\mathbf{v} \rangle .$$

Teorema 8.3. *Isometrias centrais são transformações lineares. Isometrias não centrais não são transformações lineares.*

Demonstração. Demonstramos somente a segunda parte do enunciado, que é trivialmente verificada: uma função que leve zero em algo diferente de zero não pode ser linear. ■

Exemplo 8.4. No espaço das funções contínuas em $[0, 1]$ com o produto interno usual, o operador que muda o sinal de uma função é uma isometria: sejam f e g funções em $\mathbb{R}$.

$$d(-f, -g) = \sqrt{\int_0^1 (-f + g)^2 dx} = d(g, f) = d(f, g).$$

Esta é também uma isometria central, porque não modifica a função constante zero. ◄

Exemplo 8.5. Dado um ângulo θ, o operador de rotação por θ em $\mathbb{R}^2$, cuja matriz é

$$\begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{pmatrix},$$

é uma isometria, e é central porque a rotação não modifica a origem. ◀

Exemplo 8.6. A matriz

$$R = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1/2 \\ 1/2 & 1 \end{pmatrix}$$

representa uma isometria quando aplicada em vetores de $\mathbb{R}^2$: preserva norma de vetores. No entanto, esta matriz *não* preserva norma de matrizes, porque temos que mudar o produto interno: seja

$$A = \begin{pmatrix} 1 & 0 \\ -2 & 5 \end{pmatrix}$$

A norma de Frobenius para A é

$$1^2 + (-2)^2 + 5^2 = 30.$$

Aplicando a isometria, temos

$$RA = \sqrt{2} \begin{pmatrix} 1 & -5/4 \\ -3/4 & 5/2 \end{pmatrix},$$

cuja norma é

$$\begin{aligned} &\sqrt{2}^2 + (-2\sqrt{2})^2 + (-3\sqrt{2})^2 + (5\sqrt{2})^2 \\ =&2 + 4 \cdot 2 + 9 \cdot 2 + 25 \cdot 2 \\ =&78. \end{aligned}$$

Embora a norma de Frobenius seja muito parecida com o produto interno usual para vetores, ela é diferente! ◀

Exemplo 8.7. A transofmração

$$R = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

é isometria quando aplicada em $\mathcal{M}_2 \times 2$: se

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

temos $||A|| = a^2 + b^2 + c^2 + d^2$. Mas

$$RA = \begin{pmatrix} c & d \\ -a & -b \end{pmatrix},$$

com $||RA|| = ||A||$. ◀

Exemplo 8.8. No espaço ℓ_2, de sequencias convergentes, a transformação $f(a_n) = -(a_n)$ é isometria. O produto interno é preservado por esta transformação:

$$\langle f(a_n), f(b_n)\rangle = \sum_1^\infty (-a_i)(-b_i) = \sum_1^\infty (a_i)(b_i) = \langle (a_n), (b_n)\rangle\,. \qquad \blacktriangleleft$$

Exemplo 8.9. $\blacktriangleleft$

Teorema 8.10. *Em um espaço vetorial com dimensão finita, a matriz de um operador representando uma isometria tem determinante* ± 1.

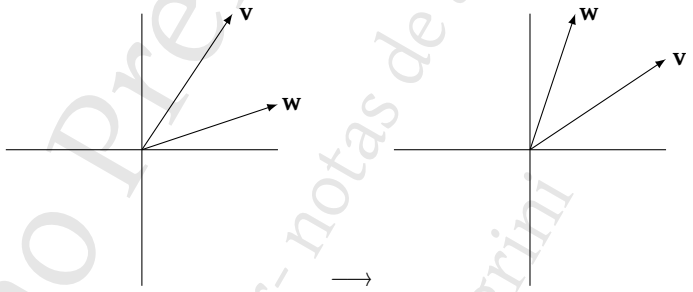
Demonstração. Se o determinante do operador for diferente de ± 1, ele modificaria a norma de vetores, e portanto mudaria a distância da origem até o vetor. ■

Definição 8.11 (rotação própria e imprópria)**.** As isometrias com determinante $+1$ são *rotações próprias*; as que tem determinante -1 são *rotações impróprias*. ♦

As rotações impróprias são claramente aquelas que mudam a orientação de um conjunto de vetores.

Exemplo 8.12. O operador que troca as coordenadas de ambos os eixos, levanto $(x, y)^T$ em $(y, x)^T$, tem a matriz

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

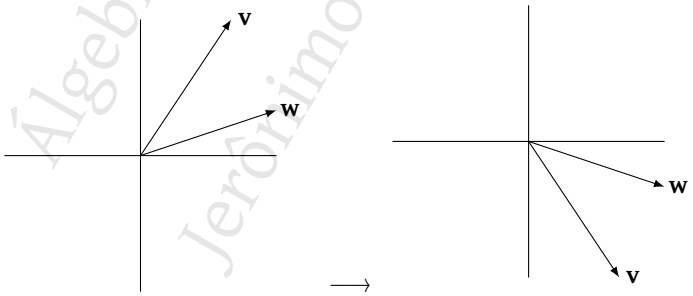


Este operador é uma isometria central, e uma rotação imprópria; a matriz tem determinante -1.

Claramente este operador muda a orientação de uma base, já que ele é exatamente a matriz de permutação de colunas. $\blacktriangleleft$

Exemplo 8.13. O operador que reflete no eixo y é

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$



Este operador é uma rotação imprópria, e seu determinante é -1. ◀

★ **Exemplo 8.14.** No exemplo 8.4 mencionamos que o operador que muda o sinal de uma função em $C[0,1]$ é uma isometria central. Este operador é uma rotação imprópria. ◀

Exemplo 8.15. O operador

$$A = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$$

é ortogonal: sejam

$$\mathbf{v} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}, \quad \mathbf{w} = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}.$$

Então

$$\langle \mathbf{v}, \mathbf{w} \rangle = v_1 w_1 + v_2 w_2.$$

Mas

$$\begin{aligned} \langle A\mathbf{v}, A\mathbf{w} \rangle &= \left\langle \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \right\rangle \\ &= \left\langle \frac{1}{\sqrt{2}}\begin{pmatrix} v_2 - v_1 \\ v_2 + v_1 \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} w_2 - w_1 \\ w_2 + w_1 \end{pmatrix} \right\rangle \\ &= \frac{(v_2 - v_1)(w_2 - w_1)}{2} + \frac{(v_2 + v_1)(w_2 + w_1)}{2} \\ &= v_1 w_1 + v_2 w_2. \end{aligned}$$ ◀

O exercício 240 pede a demonstração da proposição 8.16.

Proposição 8.16. *Se A é um operador ortogonal em $\mathbb{R}^2$, então A realiza (i) uma rotação, ou (ii) uma reflexão por alguma reta passando pela origem.*

Definição 8.17. Uma *matriz ortogonal* é toda matriz quadrada cujas colunas formam um conjunto ortonormal. ♦

Exemplo 8.18. A base canônica para $\mathbb{R}^n$ é uma matriz ortogonal, já que seus vetores são todos ortogonais entre si, e cada um deles tem norma igual a um. ◀

Exemplo 8.19. A matriz

$$\frac{1}{\sqrt{5}}\begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix}$$

é ortogonal, porque

$$\begin{aligned} \|(2/\sqrt{5}, 1/\sqrt{5})^T\| &= 1 \\ \|(1/\sqrt{5}, -2/\sqrt{5})^T\| &= 1 \\ \left\langle (2/\sqrt{5}, 1/\sqrt{5})^T, (1/\sqrt{5}, -2/\sqrt{5})^T \right\rangle &= 0. \end{aligned}$$ ◀

Teorema 8.20. *Uma matriz real A é ortogonal se e somente se A tem inversa e $A^T = A^{-1}$. Ou, equivalentemente, $A^T A = \mathcal{I}$.*

Demonstração. ($\Rightarrow$) As colunas de A são as linhas de A^T:

$$A = \left(\mathbf{a}^1, \mathbf{a}^2, \ldots, \mathbf{a}^n\right), \quad A^T = \begin{pmatrix} (\mathbf{a}^1)^T \\ (\mathbf{a}^2)^T \\ \vdots \\ (\mathbf{a}^n)^T \end{pmatrix}.$$

Calculamos

$$\begin{aligned} A^T A &= \begin{pmatrix} (\mathbf{a}^1)^T \\ (\mathbf{a}^2)^T \\ \vdots \\ (\mathbf{a}^n)^T \end{pmatrix} \left(\mathbf{a}^1, \mathbf{a}^2, \ldots, \mathbf{a}^n\right) \\ &= \begin{pmatrix} (\mathbf{a}^1)^T\mathbf{a}^1 & (\mathbf{a}^1)^T\mathbf{a}^2 & \cdots & (\mathbf{a}^1)^T\mathbf{a}^n \\ (\mathbf{a}^2)^T\mathbf{a}^1 & (\mathbf{a}^2)^T\mathbf{a}^2 & \cdots & (\mathbf{a}^2)^T\mathbf{a}^n \\ & & \vdots & \\ (\mathbf{a}^n)^T\mathbf{a}^1 & (\mathbf{a}^n)^T\mathbf{a}^2 & \cdots & (\mathbf{a}^n)^T\mathbf{a}^n \end{pmatrix} \qquad = \begin{pmatrix} \langle \mathbf{a}^1, \mathbf{a}^1 \rangle & \langle \mathbf{a}^1, \mathbf{a}^2 \rangle & \cdots & \langle \mathbf{a}^1, \mathbf{a}^n \rangle \\ \langle \mathbf{a}^2, \mathbf{a}^1 \rangle & \langle \mathbf{a}^2, \mathbf{a}^2 \rangle & \cdots & \langle \mathbf{a}^2, \mathbf{a}^n \rangle \\ & & \ddots & \\ \langle \mathbf{a}^n, \mathbf{a}^1 \rangle & \langle \mathbf{a}^n, \mathbf{a}^2 \rangle & \cdots & \langle \mathbf{a}^n, \mathbf{a}^n \rangle \end{pmatrix} \end{aligned}$$

Mas como colunas diferentes são ortogonais, então $\langle \mathbf{a}^i, \mathbf{a}^j \rangle = 0$ quando $i \neq j$. Por outro lado, como as colunas são ortonormais, sabemos que a norma de cada uma delas é um, portanto $\langle \mathbf{a}^i, \mathbf{a}^i \rangle = 1$, e fica então claro que

$$A^T A = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

($\Leftarrow$) Se $A^T = A^{-1}$, então $AA^T = \mathcal{I}$. Seguindo o mesmo raciocínio usado anteriormente nesta demonstração, verificamos que os produtos internos $\langle \mathbf{a}^i, \mathbf{a}^j \rangle$ devem necessariamente zero quando $i \neq j$, e um quando $i = j$. ■

Corolário 8.21. *Se A é ortogonal,* $\det A = \pm 1$.

Demonstração. Se $A^T = A^{-1}$, então

$$\begin{aligned} \det A^T &= \det A^{-1} \\ \det A &= \det A^{-1} \\ \det A &= (\det A)^{-1} \\ \det A &= \pm 1. \end{aligned}$$

■

Interpretamos este corolário: as matrizes ortogonais *preservam volume*: se A é ortogonal, então $\operatorname{vol} X = \operatorname{vol} AX$.

Exemplo 8.22. A matriz

$$\frac{1}{3}\begin{pmatrix} 2 & -1 & 2 \\ 2 & 2 & -1 \\ -1 & 2 & 2 \end{pmatrix}$$

é ortogonal, porque suas colunas formam um conjunto ortogonal, e seu determinante é $+1$. ◀

A recíproca do coroário 8.21 não é verdadeira, como mostra o exemplo 8.23.

Exemplo 8.23. A matriz

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

tem determinante $+1$, mas suas colunas não são ortogonais. ◀

Teorema 8.24. *Um operador é uma isometria se e somente se sua matriz é ortogonal.*

Demonstração. Matrizes ortogonais preservam volume; o volume de um vetor é sua norma. Assim, matrizes ortogonais preservam norma. Consequentemente, preservam produto interno, e representam isometrias. ■

Teorema 8.25. *Se A e B são ortogonais, então AB é ortogonal.*

Demonstração. A intuição nos diz que a composição de duas transformações que preservam distâncias também preservará distâncias. Apresentamos também uma demosntração algébrica a seguir.

Temos $A^T A = \mathcal{I}$ e $B^T B = \mathcal{I}$, logo

$$\begin{aligned} (AB)^T AB &= (B^T A^T)AB \\ &= B^T (A^T A)B \\ &= B^T B \\ &= \mathcal{I}. \end{aligned}$$ ■

O teorema 8.26 dá uma caracterização alternativa de transformações ortogonais. Sua demonstração é pedida no exercício 245.

Teorema 8.26. *Uma transformação é ortogonal se e somente se leva bases ortonormais em bases ortonormais.*

Teorema 8.27. *Os autovalores reais possíveis de uma matriz ortogonal são ± 1.*

Demonstração. Intuitivamente, se um operador ortogonal A preserva norma de vetores e temos $A\mathbf{v} = \lambda\mathbf{v}$, necessariamente $|\lambda|$ deve ser um – de outra forma estaríamos mudando a norma do vetor. A demonstração algébrica segue.

Seja A uma matriz ortogonal com autovetor $\mathbf{v}$ e autovalor $\lambda \in$. Então

$$\begin{aligned} 0 \neq \|\mathbf{v}\|^2 & \qquad \text{(autovetor não é zero)} \\ &= \|A\mathbf{v}\|^2 \\ &= \langle A\mathbf{v}, A\mathbf{v}\rangle \\ &= \langle \lambda\mathbf{v}, \lambda\mathbf{v}\rangle \\ &= \lambda^2 \|\mathbf{v}\|. \end{aligned}$$

Como $\|\mathbf{v}\| = \lambda^2\|\mathbf{v}\|$, necessariamente $\lambda^2 = 1$, e como $\lambda \in \mathbb{R}$, temos $\lambda = \pm 1$. ■

O Teorema 8.27, no entanto nada diz sobre autovalores complexos.

Exemplo 8.28. A matriz

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

é ortogonal (suas colunas formam um conjunto ortogonal), e tem autovalores

$$1, \quad \frac{i\sqrt{7}+3}{4}, \quad \frac{i\sqrt{7}-3}{4}.$$

O único autovalor real da matriz é 1. ◀

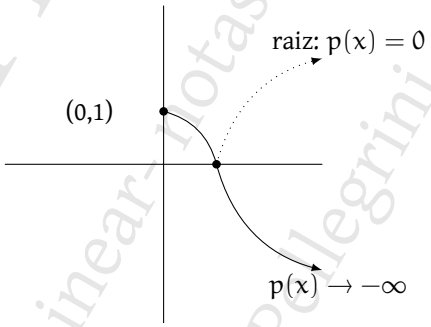
Sabemos que um dentre $+1$ e -1 é autovalor real de A. O teorema a seguir nos permite identificar, quando A tem ordem ímpar, um deles como autovalor da matriz.

Teorema 8.29. *Se A é quadrada, ortogonal e de ordem ímpar, então* $\det A$ *é autovalor de A.*

Demonstração. Suponha que $\det A = +1$. O poliômio característico de A é

$$\begin{aligned} p(x) &= -x^n + \cdots + \det A \\ &= -x^n + \cdots + 1 \end{aligned}$$

Assim, $p(0) = 1$, positivo. Quando $x \to +\infty$, temos também $p(x) \to -\infty$.



Pelo teorema do valor intermediário, $p(x)$ deve valer zero para algum x no intervalo $(0, \infty)$. Como sabemos que os autovalores reais de A só podem ser ± 1, temos que 1 é autovalor de A.

Se o $\det A = -1$, repetimos o argumento usando $(-\infty, 0)$ ao invés de $(0, +\infty)$. ■

Exemplo 8.30. A matriz do Exemplo 8.28 tem dimensão ímpar, e seu determinante, $+1$, também é um de seus autovalores. ◀

Teorema 8.31 (de Euler)**.** *Se uma matriz M ortogonal de ordem tres tem determinante $+1$, então M tem um autovetor fixo, correspondente a um eixo de rotação. O ângulo de rotação é*

$$\cos\theta = \frac{\operatorname{Tr} M}{2}.$$

Exemplo 8.32. A matriz de rotação pelo ângulo $\theta = 3\pi/4$ é

$$R = \begin{pmatrix} \cos(3\pi/4) & -\operatorname{sen}(3\pi/4) & 0 \\ \operatorname{sen}(3\pi/4) & \cos(3\pi/4) & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -\sqrt{2}/2 & -\sqrt{2}/2 & 0 \\ \sqrt{2}/2 & -\sqrt{2}/2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

R é ortogonal, e seu determinante é $+1$. O traço desta matriz é

$$\operatorname{Tr} R = 2\cos(3\pi/4) + 1 = 1 - \sqrt{2}.$$

O ângulo θ é, então

$$\begin{aligned} \cos\theta &= \frac{\operatorname{Tr} M - 1}{2} \\ &= \frac{2\cos(3\pi/4) + 1 - 1}{2} \\ &= \cos(3\pi/4), \end{aligned}$$

Os autovalores e autovetores de R são

$$\lambda_1 = -\sqrt{2} + i\sqrt{2}, \quad \begin{pmatrix} i \\ 1 \\ 0 \end{pmatrix}$$

$$\lambda_2 = -\sqrt{2} - i\sqrt{2}, \quad \begin{pmatrix} i \\ -1 \\ 0 \end{pmatrix}$$

$$\lambda_3 = 1, \quad \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

O único par autovalor/autovetor real é o terceiro, e o autovetor nos dáexatamente o eixo de rotação (z). ◀

No exemplo 8.32, a matriz de rotação já deixava evidente o eixo em que a rotação acontece (z). O exemplo 8.33 usa a composição de duas rotações em eixos diferentes.

Exemplo 8.33. A matriz R_A a seguir faz rotação de $3\pi/4$ pelo eixo z; a matriz R_B faz uma rotação de $\pi/4$ no eixo y.

$$R_A = \begin{pmatrix} \cos(3\pi/4) & -\operatorname{sen}(3\pi/4) & 0 \\ \operatorname{sen}(3\pi/4) & \cos(3\pi/4) & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_B = \begin{pmatrix} \cos(\pi/2) & 0 & -\operatorname{sen}(\pi/2) \\ 0 & 1 & 0 \\ \operatorname{sen}(\pi/2) & 0 & \cos(\pi/2) \end{pmatrix}$$

Numericamente,

$$R_A = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad R_B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

A composição das duas é

$$R_A R_B = \begin{pmatrix} -1/2 & -1/\sqrt{2} & 1/2 \\ 1/2 & -1/\sqrt{2} & -1/2 \\ 1/\sqrt{2} & 0 & 1/\sqrt{2} \end{pmatrix}$$

Se olharmos somente para a matriz $R_A R_B$, não temos como determinar facilmente o eixo de rotação. No entanto, podemos verificar que os autovalores de $R_A R_B$ são

$$1, \frac{i\sqrt{7}-3}{4}, \frac{i\sqrt{7}+3}{4}.$$

O autovetor correspondente ao autovalor 1 é

$$\mathbf{v} = \begin{pmatrix} 1 \\ 1-\sqrt{2} \\ 1+\sqrt{2} \end{pmatrix}$$

Como os autovetores gerados por este vetor são os únicos que a transformação não rotaciona (porque $R_A R_B \mathbf{v} = \mathbf{v}$), eles formam o eixo de rotação da transformação. Já o ângulo é θ, com

$$\begin{aligned} \cos\theta &= \frac{\operatorname{Tr} M - 1}{2} \\ &= \frac{-1/2 - 1}{2} \\ &= -3/4. \end{aligned}$$

O ângulo θ é aproximadamente $0.77\pi = 2.42$ radianos, ou 138.6^o. ◀

8.1.1 Decomposição QR

Nesta seção verificamos como uma matriz pode ser decomposta em produto de uma matriz ortogonal por uma matriz triangular.

Teorema 8.34. *Seja A uma matriz quadrada. Então existem uma matriz Q ortogonal e uma matriz R triangular superior e não singular tais que*

$$A = QR.$$

A demonstração deste teorema é construtiva, e nos dá um algoritmo para computar a decomposição QR.

Demonstração. Se aplicarmos o processo de Gram-Schmidt, descrito na seção 7.4, nas colunas $\mathbf{a}_1, \mathbf{a}_2, \ldots$ de A par obter colunas $\mathbf{o}_1, \mathbf{o}_2, \ldots$, ortogonais, teremos

$$\begin{aligned} \mathbf{o}_1 &= \mathbf{a}_1 \\ \mathbf{o}_2 &= \mathbf{a}_2 - \frac{\langle \mathbf{o}_1, \mathbf{a}_2 \rangle}{\langle \mathbf{o}_1, \mathbf{o}_1 \rangle} \mathbf{o}_1 \\ \mathbf{o}_3 &= \mathbf{a}_3 - \frac{\langle \mathbf{o}_2, \mathbf{a}_3 \rangle}{\langle \mathbf{o}_2, \mathbf{o}_2 \rangle} \mathbf{o}_2 - \frac{\langle \mathbf{o}_1, \mathbf{a}_3 \rangle}{\langle \mathbf{o}_1, \mathbf{o}_1 \rangle} \mathbf{o}_1 \\ &\vdots \\ \mathbf{o}_k &= \mathbf{a}_k - \sum_{i<k} \frac{\langle \mathbf{o}_i, \mathbf{a}_k \rangle}{\langle \mathbf{o}_i, \mathbf{o}_i \rangle} \mathbf{o}_i, \end{aligned}$$

e temos o conjunto ortogonal $\mathbf{o}_1, \ldots \mathbf{o}_k$. Normalizamos os vetores, para que todos tenham norma um, definindo $\mathbf{q}_i = \mathbf{o}_i/\|\mathbf{o}_i\|$, e já temos amatriz Q:

$$\begin{pmatrix} \mathbf{q}_1 & \mathbf{q}_2 & \cdots & \mathbf{q}_n \end{pmatrix} = \begin{pmatrix} \frac{1}{\|\mathbf{o}_1\|}\mathbf{q}_1 & \frac{1}{\|\mathbf{o}_2\|}\mathbf{q}_2 & \cdots \frac{1}{\|\mathbf{o}_n\|}\mathbf{q}_n \end{pmatrix}.$$

Agora observamos que

$$\begin{aligned}
\mathbf{a}_1 &= \mathbf{o}_1 \\
\mathbf{a}_2 &= \mathbf{o}_2 + \frac{\langle \mathbf{o}_1, \mathbf{a}_2 \rangle}{\langle \mathbf{o}_1, \mathbf{o}_1 \rangle}\mathbf{o}_1 \\
\mathbf{a}_3 &= \mathbf{o}_3 + \frac{\langle \mathbf{o}_2, \mathbf{a}_3 \rangle}{\langle \mathbf{o}_2, \mathbf{o}_2 \rangle}\mathbf{o}_2 + \frac{\langle \mathbf{o}_1, \mathbf{a}_3 \rangle}{\langle \mathbf{o}_1, \mathbf{o}_1 \rangle}\mathbf{o}_1 \\
&\vdots \\
\mathbf{a}_k &= \mathbf{o}_k + \sum_{i<k} \frac{\langle \mathbf{o}_i, \mathbf{a}_k \rangle}{\langle \mathbf{o}_i, \mathbf{o}_i \rangle}\mathbf{o}_i
\end{aligned}$$

Definimos a matriz R com

$$r_{ij} = \begin{cases} 0 & \text{se } i > j \\ \|\mathbf{o}_i\| & \text{se } i = j \\ \|\mathbf{o}_i\| \frac{\langle \mathbf{o}_i, \mathbf{a}_j \rangle}{\langle \mathbf{o}_i, \mathbf{o}_i \rangle} & \text{se } i < j \end{cases}$$

Temos portanto

$$A = \underbrace{\begin{pmatrix} \mathbf{q}_1 & \mathbf{q}_2 & \cdots & \mathbf{q}_n \end{pmatrix}}_{Q} \underbrace{\begin{pmatrix} \|\mathbf{o}_1\| & \|\mathbf{o}_1\| \frac{\langle \mathbf{o}_1, \mathbf{o}_2 \rangle}{\langle \mathbf{o}_1, \mathbf{o}_1 \rangle} & \|\mathbf{o}_1\| \frac{\langle \mathbf{o}_1, \mathbf{o}_3 \rangle}{\langle \mathbf{o}_1, \mathbf{o}_1 \rangle} & \cdots & \|\mathbf{o}_1\| \frac{\langle \mathbf{o}_1, \mathbf{o}_n \rangle}{\langle \mathbf{o}_1, \mathbf{o}_1 \rangle} \\ 0 & \|\mathbf{o}_2\| & \|\mathbf{o}_2\| \frac{\langle \mathbf{o}_2, \mathbf{o}_3 \rangle}{\langle \mathbf{o}_2, \mathbf{o}_2 \rangle} & \cdots & \|\mathbf{o}_2\| \frac{\langle \mathbf{o}_2, \mathbf{o}_n \rangle}{\langle \mathbf{o}_2, \mathbf{o}_2 \rangle} \\ 0 & 0 & \|\mathbf{o}_3\| & & \|\mathbf{o}_3\| \frac{\langle \mathbf{o}_3, \mathbf{o}_n \rangle}{\langle \mathbf{o}_3, \mathbf{o}_3 \rangle} \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & & \|\mathbf{o}_n\| \end{pmatrix}}_{R},$$

e a k-ésima coluna de A é

$$\begin{aligned}
\mathbf{a}_k &= \mathbf{q}_k\|\mathbf{o}_k\| + \sum_{i<k} \frac{\langle \mathbf{o}_i, \mathbf{a}_k \rangle}{\langle \mathbf{o}_i, \mathbf{o}_i \rangle}\mathbf{q}_i\|o_i\| \\
&= \mathbf{o}_k + \sum_{i<k} \frac{\langle \mathbf{o}_i, \mathbf{a}_k \rangle}{\langle \mathbf{o}_i, \mathbf{o}_i \rangle}\mathbf{o}_i, \qquad (\mathbf{o}_i = \mathbf{q}_i/\|\mathbf{o}_i\|)
\end{aligned}$$

completando a demonstração. ■

Exemplo 8.35. Seja

$$A = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix},$$

a ortogonalização das colunas de A nos dará os vetores

$$\mathbf{o}_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad \mathbf{o}_2 = \begin{pmatrix} 2/5 \\ -1/5 \end{pmatrix}$$

Normalizamos os vetores. As normas são $\|\mathbf{o}_1\| = \sqrt{5}$ e $\|\mathbf{o}_2\| = 1/\sqrt{5}$, logo

$$\mathbf{q}_1 \begin{pmatrix} 1/\sqrt{5} \\ 2/\sqrt{5} \end{pmatrix}, \quad \mathbf{q}_2 \begin{pmatrix} 2\sqrt{5}/5 \\ -\sqrt{5}/5 \end{pmatrix}$$

A matriz Q está pronta:

$$Q = \begin{pmatrix} 1/\sqrt{5} & 2\sqrt{5}/5 \\ 2/\sqrt{5} & -\sqrt{5}/5 \end{pmatrix}.$$

A matriz R é

$$R = \begin{pmatrix} \|\mathbf{o}_1\| & \|\mathbf{o}_1\| \frac{\langle \mathbf{o}_1, \mathbf{o}_2 \rangle}{\langle \mathbf{o}_1, \mathbf{o}_1 \rangle} \\ 0 & \|\mathbf{o}_2\| \end{pmatrix} = \begin{pmatrix} \sqrt{5} & -2/\sqrt{5} \\ 0 & 1/\sqrt{5} \end{pmatrix}.$$

Temos Q evidentemente ortogonal, R triangular superior e invertível, e

$$A = QR.$$ ◀

8.2 Operadores normais

Definição 8.36. Um operador real é normal se comuta com sua transposta ♦

8.3 Decomposição em Valores Singulares

Teorema 8.37. *Seja M uma matriz real ou complexa. Então existem duas matrizes U e V unitárias (ortogonais, se M é real); e uma matriz Σ diagonal, tais que*

$$M = U\Sigma V^H.$$

Exemplo 8.38. Seja

$$M = \begin{pmatrix} 1 & 2\sqrt{2}+1 \\ 1 & 2\sqrt{2}-1 \end{pmatrix}.$$

A decomposição de M em valores singulares é

$$M = \underbrace{\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -4 \\ 1 & 4 \end{pmatrix}}_{U} \underbrace{\begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix}}_{\Sigma} \underbrace{\begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 1 \end{pmatrix}}_{V^T}.$$

As matrizes U e V são ortogonais, e Σ é singular. Os valores singulares de M são 2 e -1. ◀

8.4 Aplicações

8.4.1 Análise de Componentes Principais

Exercícios

Ex. 240 — Demonstre a proposição 8.16.

Ex. 241 — Há uma classe de matrizes tais que $A^T A = D$, com D diagonal. Que matrizes são estas?

Ex. 242 — O conjunto de matrizes descrito no exercício 241 é fechado para multiplicação de matrizes? E nesse conjunto, a multiplicação é comutativa?

Ex. 243 — Quais são as isometrias que podemos ter em $\mathcal{M}_n \times n$, usando o produto de Frobenius?

★ **Ex. 244 —** Quais são as isometrias que podemos ter em $\mathcal{M}_n \times n$, usando o produto $\langle A, B\rangle =$ maior autovalor de $A^T B$?

Ex. 245 — Prove o Teorema 8.26.

Ex. 246 — O produto de matrizes ortogonais é comutativo?

★ **Ex. 247 —** Quais destes conjuntos são grupos com a operação de multiplicação de matrizes?

a) Matrizes ortogonais

b) Matrizes ortogonais com determinante $+1$

c) Matrizes ortogonais com determinante -1

Ex. 248 — Calcule a decomposição QR de

$$A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

Capítulo 9

Pseudoinversa

Sabemos que nem toda matriz quadrada tem inversa. Neste Capítulo estudamos uma generalização da noção de inversão de matrizes: toda matriz tem uma *pseudoinversa*, mesmo que seja singular ou que não seja quadrada.

Assim como fizemos com o determinante, definiremos a pseudoinversa por suas propriedades, e depois demonstraremos que é única. A prova de existência da pseudoinversa, no entanto, envolve conceitos adicionais que ficam fora do escopo deste texto.

Definição 9.1 (Pseudoinversa de matriz real)**.** A *pseudoinversa* de Moore-Penrose[1] de uma matriz real A é a matriz A^+ tal que

i) $AA^+A = A$

ii) $A^+AA^+ = A^+$

iii) $(AA^+)^T = AA^+$

iv) $(A^+A)^T = A^+A$ ♦

Da definição fica claro que se uma matriz é não-singular, sua inversa é igual à pseudoinversa.

Observe que mesmo matrizes que não são quadradas tem pseudoinversa, como ilustrado na última matriz do exemplo 9.2. Matrizes singulares também (mesmo a matriz zero tem ela mesmo como pseudoinversa).

Exemplo 9.2. As pseudoinversas das matrizes

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 2 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 4 & 1 \end{pmatrix}$$

são

$$A^+ = \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad B^+ = \begin{pmatrix} \frac{1}{25} & \frac{2}{25} \\ \frac{2}{25} & \frac{4}{25} \end{pmatrix}, \quad C^+ = \begin{pmatrix} \frac{1}{2} & \frac{1}{10} & \frac{1}{5} \\ 0 & \frac{1}{5} & \frac{2}{5} \\ \frac{1}{2} & \frac{1}{10} & \frac{1}{5} \end{pmatrix}, \quad D^+ = \begin{pmatrix} \frac{1}{5} & 0 \\ \frac{2}{5} & 0 \\ -2 & 1 \end{pmatrix}. \quad ◀$$

[1] Há outras noções de pseudoinversa, de que não tratamos aqui.

O teorema 9.3 nos garante que toda matriz tem uma pseudoinversa.

Teorema 9.3. *Toda matriz real A tem pseudoinversa.*

Demonstração. A matriz A, $m \times n$, pode ser decomposta em valores singulares:

$$A = U_m \Sigma_{m\times n} V_n^T,$$

onde

- U_m é ortogonal, de ordem m
- $\Sigma_{m\times n}$ é $m \times n$, diagonal na sua parte superior,
- V_n é ortognal, de ordem n.

Então a pseudoinversa de A é a matriz $n \times m$

$$A^+ = V\Sigma^+ U^T.$$

Verificamos as propriedades de pseudoinversa a seguir.

i)

$$\begin{aligned} AA^+A &= (U\Sigma V^T)(V\Sigma^+U^T)(U\Sigma V^T) \\ &= U(\Sigma V^T V\Sigma^+ U^T U\Sigma)V^T \\ &= U\Sigma \mathcal{I}_n \Sigma^+ \mathcal{I}_m \Sigma V^T && (U, V \text{ ortogonais: } U^T = U^{-1}, V^T = V^{-1}.) \\ &= U(\Sigma\Sigma^+\Sigma)V^T \\ &= U\Sigma V^T && (\text{pseudoinversa de } \Sigma, \text{ prop. (i)}) \\ &= A. \end{aligned}$$

ii) Similar a (i)

iii)

$$\begin{aligned} (AA^+)^T &= \left[A(V\Sigma^+U^T)\right]^T \\ &= \left[(U\Sigma V^T)(V\Sigma^+U^T)\right]^T \\ &= (V\Sigma^+U^T)^T(U\Sigma V^T)^T \\ &= U\Sigma^T V^T V(\Sigma^+)^T U^T \\ &= U\Sigma^T \mathcal{I}_n (\Sigma^+)^T U^T && (V \text{ é ortogonal: } V^T = V^{-1}.) \\ &= AA^+. \end{aligned}$$

iv) Similar a (iii) ■

A decomposição em valores singulares não é única, mas mostramos a seguir que há exatamente uma pseudoinversa para cada matriz.

Teorema 9.4. *Toda matriz real* A *tem no máximo uma pseudoinversa.*

Demonstração. Seja A uma matriz real, e sejam B e C pseudoinversas de A. Usamos abaixo álgebra básica de matrizes e suas transpostas, além das propriedades listadas na definição de pseudoinversa para mostrar que $AB = AC$.

$$\begin{aligned}
AB =& (AB)^T && \text{(propriedade (iii))}\\
=& B^T A^T\\
=& B^T (ACA)^T && \text{(propriedade (i))}\\
=& B^T A^T C^T A^T\\
=& (AB)^T (AC)^T\\
=& ABAC && \text{(propriedade (iii))}\\
=& AC && \text{(propriedade (i))}
\end{aligned}$$

Mostramos que $AB = AC$. Pode-se, de forma semelhante, mostrar que $BA = CA$. ■

Lema 9.5. *A pseudoinversa de um vetor coluna* $\mathbf{v}$ *é o vetor* linha $\mathbf{v}^+$*, com*

$$\mathbf{v}^+ = \begin{cases} \frac{1}{||\mathbf{v}||^2}\mathbf{v} & \text{se } \mathbf{v} \neq \mathbf{0} \\ \mathbf{0} & \text{se } \mathbf{v} = \mathbf{0}. \end{cases}$$

Da mesma forma se define a pseudoinversa de um vetor linha (será um vetor coluna, obedecendo a mesma regra, exceto que para colunas $||\mathbf{v}||^2 = \mathbf{v}^T\mathbf{v}$*, e para linhas,* $||\mathbf{w}||^2 = \mathbf{w}\mathbf{w}^T$*).*

A pseudoinversa de uma matriz quadrada diagonal D *é outra matriz diagonal* E*, com*

$$e_{ii} = \begin{cases} 1/d_{ii} & \text{se } d_{ii} \neq 0 \\ 0 & \text{se } d_{ii} = 0. \end{cases}$$

Exemplo 9.6. Sejam

$$A = \begin{pmatrix} 2 & 0 & 1/2 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 \\ -3 \\ 5 \\ 0 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2/5 \end{pmatrix}.$$

Como

$$\frac{1}{AA^T} = \frac{4}{21}$$
$$\frac{1}{B^T B} = 35,$$

Então as pseudoinversas são

$$A^+ = \frac{4}{21}A^T = \frac{1}{21}\begin{pmatrix} 8 \\ 0 \\ 2 \\ 4 \end{pmatrix}, \quad B^+ = \frac{1}{35}\begin{pmatrix} 1 & -3 & 5 & 0 \end{pmatrix}, \quad D^+ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5/2 \end{pmatrix}. \qquad ◀$$

A demonstração to teorema 9.7 é pedida no exercício 251.

Teorema 9.7. *Seja A uma matriz real. Então*

i) $(A^+)^+ = A$.

ii) *Se A tem inversa, então* $A^+ = A^{-1}$.

iii) $(A^T)^+ = (A^+)^T$.

iv) $(kA)^+ = k^{-1}A^+$, *para* $k \neq 0$.

Teorema 9.8. *Para toda matriz* A, $\ker(A^+) = \ker(A^T)$, *e* $\mathrm{Im}(A^+) = \mathrm{Im}(A^T)$.

9.1 Calculando pseudoinversas

Há diversos métodos para obter a pseudoinversa de uma matriz. Damos inicialmente dois métodos simples (o de decomposição em posto e o método por blocos); e dois outros de robustez numérica razoável, normalmente usados em aplicações práticas.

9.1.1 Decomposição em posto completo

Seja A uma matriz $m \times n$ com posto r. O Lema 4.43 nos garante que A pode ser decomposta em

$$A = BC,$$

com B $m \times r$ e C $r \times n$, sendo r o posto tanto de B como de C.

Exemplo 9.9. Seja

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 6 \\ 3 & 2 \\ 0 & 1 \end{pmatrix}$$

A matriz tem posto 2, então

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 6 \\ 3 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \qquad \blacktriangleleft$$

Teorema 9.10. *Seja A matriz real* A $m \times n$ *com posto* r, *e* $A = BC$ *sua decomposição em posto completo com* B $m \times r$, C $r \times n$, *ambas de posto completo igual a* r. *Então*

$$A^+ = C^T(CC^T)^{-1}(B^TB)^{-1}B^T.$$

Exemplo 9.11. A matriz

$$A = \begin{pmatrix} 2/5 & 4/5 \\ 0 & 0 \end{pmatrix}$$

evidentemente não tem inversa, porque tem uma linha com zeros. Seu posto é um, e sua decomposição em posto completo é

$$A = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 2/5 & 4/5 \end{pmatrix}$$

Logo,

$$\begin{aligned} A^+ &= C^T(CC^T)^{-1}(B^TB)^{-1}B^T \\ &= \begin{pmatrix} 2/5 \\ 4/5 \end{pmatrix} \left[\begin{pmatrix} 2/5 & 4/5 \end{pmatrix} \begin{pmatrix} 2/5 \\ 4/5 \end{pmatrix} \right]^{-1} \left[\begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right]^{-1} \begin{pmatrix} 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 2/5 \\ 4/5 \end{pmatrix} \begin{pmatrix} \frac{4}{5} \end{pmatrix}^{-1} (1)^{-1} \begin{pmatrix} 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1/2 & 0 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

Verificamos facilmente as quatro propriedades que definem pseudoinversa:

$$AA^+A = \begin{pmatrix} 2/5 & 4/5 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1/2 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2/5 & 4/5 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2/5 & 4/5 \\ 0 & 0 \end{pmatrix},$$

$$A^+AA^+ = \begin{pmatrix} 1/2 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2/5 & 4/5 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1/2 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1/2 & 0 \\ 1 & 0 \end{pmatrix},$$

$$(AA^+) = \frac{1}{5} \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}, \qquad \text{(simétrica)}$$

$$(A^+A) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \qquad \text{(simétrica)}$$

◀

Exemplo 9.12. Seja

$$A = \overbrace{\begin{pmatrix} 1 & 2 \\ 3 & 6 \\ 3 & 2 \\ 0 & 1 \end{pmatrix}}^{B} \overbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}^{C}.$$

Então, como $C = \mathcal{I}$ e $B = A$,

$$\begin{aligned} A^+ &= C^T(CC^T)^{-1}(B^TB)^{-1}B^T \\ &= \mathcal{I}^T(\mathcal{I}\mathcal{I})^{-1}(A^TA)^{-1}A^T \\ &= (A^TA)^{-1}A^T \\ &= \left[\frac{1}{179} \begin{pmatrix} 45 & -26 \\ -26 & 19 \end{pmatrix} \right]^{-1} \begin{pmatrix} 1 & 3 & 3 & 0 \\ 2 & 6 & 2 & 1 \end{pmatrix} \\ &= \frac{1}{179} \begin{pmatrix} -7 & -21 & 83 & -26 \\ 12 & 36 & -40 & 19 \end{pmatrix}. \end{aligned}$$

Verificamos que $AA^+A = A$:

$$\begin{pmatrix}1&2\\3&6\\3&2\\0&1\end{pmatrix}\frac{1}{179}\begin{pmatrix}-7&-21&83&-26\\12&36&-40&19\end{pmatrix}\begin{pmatrix}1&2\\3&6\\3&2\\0&1\end{pmatrix}=\frac{1}{179}\begin{pmatrix}17&51&3&12\\51&153&9&36\\3&9&169&-40\\12&36&-40&19\end{pmatrix}\begin{pmatrix}1&2\\3&6\\3&2\\0&1\end{pmatrix}$$
$$=\begin{pmatrix}1&2\\3&6\\3&2\\0&1\end{pmatrix}. \qquad \blacktriangleleft$$

Exemplo 9.13. Abordamos agora um caso em que a matriz A é $m \times n$, e o posto é estritamente menor, tanto do que m como do que n. Seja

$$A = \begin{pmatrix}1&0&5\\0&1&0\\1&-1&5\end{pmatrix}$$

O posto é dois, porque $L3 = L1 - L2$. Disso concluímos que

$$A = \overbrace{\begin{pmatrix}1&0\\0&1\\1&-1\end{pmatrix}}^{B}\overbrace{\begin{pmatrix}1&0&5\\0&1&0\end{pmatrix}}^{C}.$$

Assim,

$$\begin{aligned}A^+ &= C^T(CC^T)^{-1}(B^TB)^{-1}B^T\\ &= \begin{pmatrix}1&0\\0&1\\5&0\end{pmatrix}\left[\begin{pmatrix}1&0&5\\0&1&0\end{pmatrix}\begin{pmatrix}1&0\\0&1\\5&0\end{pmatrix}\right]^{-1}\left[\begin{pmatrix}1&0&1\\0&1&-1\end{pmatrix}\begin{pmatrix}1&0\\0&1\\1&-1\end{pmatrix}\right]^{-1}\begin{pmatrix}1&0&1\\0&1&-1\end{pmatrix}\\ &= \frac{1}{3}\begin{pmatrix}1/13&1/26&1/26\\1&2&-1\\5/13&5/26&5/26\end{pmatrix}. \qquad \blacktriangleleft\end{aligned}$$

9.1.2 Por blocos

Se A pode ser decomposta em

$$A = \begin{pmatrix}A_{11}&A_{12}\\A_{21}&A_{22}\end{pmatrix},$$

onde A_{11} é quadrada e tem o mesmo posto de A, então

$$A^+ = \begin{pmatrix}A_{11}&A_{12}\end{pmatrix}^T B^T \begin{pmatrix}A_{11}\\A_{21}\end{pmatrix}^T,$$

com

$$B = \left[\begin{pmatrix}A_{11}&A_{12}\end{pmatrix}A^T\begin{pmatrix}A_{11}\\A_{21}\end{pmatrix}\right]^{-1}.$$

Exemplo 9.14. A matriz

$$A = \begin{pmatrix} 2 & 0 \\ -2 & 0 \end{pmatrix}$$

é singular, com posto um. Podemos identificar os blocos

$$A = \left(\begin{array}{c|c} 2 & 0 \\ \hline -2 & 0 \end{array}\right),$$

com $A_{ij} = (a_{ij})$, ou seja,

$$\begin{aligned} A_{11} &= (2) \\ A_{12} &= (0) \\ A_{21} &= (-2) \\ A_{22} &= (0) \end{aligned}$$

. Temos

$$\begin{aligned} B &= \begin{pmatrix} 2 & 0 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ -2 \end{pmatrix} \\ &= (16)^{-1}. \end{aligned}$$

e

$$\begin{aligned} A^+ &= \begin{pmatrix} 2 \\ 0 \end{pmatrix} (16)^{-1} \begin{pmatrix} 2 & -2 \end{pmatrix} \\ &= \begin{pmatrix} 1/4 & -1/4 \\ 0 & 0 \end{pmatrix}, \end{aligned}$$

que é a pseudoinversa de A. ◀

Exemplo 9.15. Seja

$$A = \begin{pmatrix} 1 & 2 & 4 \\ -1 & 3 & -4 \\ -1/2 & -1 & -2 \end{pmatrix}$$

Então

$$A_{11} = \begin{pmatrix} 1 & 2 \\ -1 & 3 \end{pmatrix}, \quad A_{12} = \begin{pmatrix} 4 \\ -4 \end{pmatrix}, \quad A_{21} = \begin{pmatrix} -1/2 & -1 \end{pmatrix}, \quad A_{22} = (-2).$$

Como o posto A = posto $A_{11} = 2$, calculamos

$$\begin{aligned} B &= \left[\begin{pmatrix} A_{11} & A_{12} \end{pmatrix} A^T \begin{pmatrix} A_{11} \\ A_{21} \end{pmatrix} \right]^{-1} \\ &= \left[\begin{pmatrix} 1 & 2 & 4 \\ -1 & 3 & -4 \end{pmatrix} \begin{pmatrix} 1 & -1 & -1/2 \\ 2 & 3 & -1 \\ 4 & -4 & -2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ -1 & 3 \\ -1/2 & -1 \end{pmatrix} \right]^{-1} \\ &= \left[\begin{pmatrix} 21 & -11 & -21/2 \\ -11 & 26 & 11/2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ -1 & 3 \\ -1/2 & -1 \end{pmatrix} \right]^{-1} \end{aligned}$$

$$= \frac{1}{2}\begin{pmatrix} 149/2 & 39 \\ -159/2 & 101 \end{pmatrix}^{-1}$$
$$= \frac{1}{10625}\begin{pmatrix} 202 & -78 \\ 159 & 149 \end{pmatrix}$$

e

$$A^+ = \begin{pmatrix} A_{11} & A_{12} \end{pmatrix}^T B^T \begin{pmatrix} A_{11} \\ A_{21} \end{pmatrix}^T$$
$$= \begin{pmatrix} 1 & 2 & 4 \\ -1 & 3 & -4 \end{pmatrix}^T \frac{1}{10625}\begin{pmatrix} 202 & 78 \\ 159 & 149 \end{pmatrix}^T \begin{pmatrix} 1 & 2 \\ -1 & 3 \\ -1/2 & -1 \end{pmatrix}^T$$
$$= \frac{1}{5}\begin{pmatrix} 12/85 & -2/17 & -6/85 \\ 4/5 & 1 & -2/5 \\ 48/85 & -8/17 & -24/85 \end{pmatrix}. \quad \blacktriangleleft$$

★ 9.1.3 Método de Greville

O método recursivo de Greville calcula a pseudoinversa de uma matriz particionando-a e computando as pseudoinversas de matrizes menores. Ë interessante por ser rápido e não depender de informações adicionais sobre a matriz, como autovalores.

Teorema 9.16. *Se A é $m \times n$, e $\mathbf{a}$ sua última coluna, ou seja,*

$$A = \begin{pmatrix} B & \mathbf{a} \end{pmatrix},$$

então

$$A^+ = \begin{pmatrix} B^+(\mathcal{I} - \mathbf{a}\mathbf{x}) \\ \mathbf{x} \end{pmatrix},$$

onde

$$\mathbf{x}^T = \begin{cases} (\|(\mathcal{I} - BB^+)\mathbf{a}\|)^{-2}(\mathcal{I} - BB^+)\mathbf{a} & \text{se } \|(\mathcal{I} - BB^+)\mathbf{a}\| \neq 0 \\ (1 + \|B^+\mathbf{a}\|^2)^{-1}(B^+)^T B^+\mathbf{a} & \text{caso contrário.} \end{cases}$$

Exemplo 9.17. Seja

$$A = \begin{pmatrix} 1 & 2 & -1 \\ -2 & -4 & -2 \end{pmatrix}$$

Calculamos a pseudoinversa de A usando o método de Greville. Temos

$$A = (B \,\vdots\, \mathbf{a}), \quad B = \begin{pmatrix} 1 & 2 \\ -2 & -4 \end{pmatrix}, \quad \mathbf{a} = \begin{pmatrix} -1 \\ -2 \end{pmatrix}.$$

Assim,

$$A^+ = \begin{pmatrix} B^+(\mathcal{I} - \mathbf{a}\mathbf{x}) \\ \mathbf{x} \end{pmatrix}$$

Obtemos a pseudoinversa de B. Usaríamos o método de Greville para isto, mas para não tornar o exemplo demasiado longo e conceitualmente difícil, apresentamos de imediato a matriz

$$\mathrm{B}^{+} = \frac{1}{25}\begin{pmatrix} 1 & -2 \\ 2 & -4 \end{pmatrix}.$$

Agora, calculamos a norma de $(\mathcal{I} - \mathrm{B}\mathrm{B}^{+})\mathbf{a}$:

$$\begin{aligned} \|(\mathcal{I} - \mathrm{B}\mathrm{B}^{+})\mathbf{a}\| &= \left\| \left(\mathcal{I} - \frac{1}{5}\begin{pmatrix} 1 & -2 \\ -2 & 4 \end{pmatrix} \right) \begin{pmatrix} -1 \\ -2 \end{pmatrix} \right\| \\ &= \left\| \frac{1}{5}(-8, -4) \right\| \\ &= \frac{4}{\sqrt{5}}. \end{aligned}$$

Assim,

$$\begin{aligned} \mathbf{x}^{\mathsf{T}} &= \|(\mathcal{I} - \mathrm{B}\mathrm{B}^{+})\mathbf{a}\|^{-2}(\mathcal{I} - \mathrm{B}\mathrm{B}^{+})\mathbf{a} \\ &= \frac{5}{16}\,\frac{1}{5}\begin{pmatrix} -8 \\ -4 \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} -1 \\ -2 \end{pmatrix}. \end{aligned}$$

E temos

$$\mathrm{B}^{+}(\mathcal{I} - \mathbf{a}\mathbf{x}) = \frac{1}{25}\begin{pmatrix} 1 & -2 \\ 2 & -4 \end{pmatrix}\frac{1}{25}\begin{pmatrix} 1/2 & 1/4 \\ 1 & 1/2 \end{pmatrix} = \begin{pmatrix} 1/10 & -1/20 \\ 1/5 & -1/10 \end{pmatrix},$$

e finalmente

$$\mathrm{A}^{+} = \begin{pmatrix} \mathrm{B}^{+}(\mathcal{I} - \mathbf{a}\mathbf{x}) \\ \mathbf{x} \end{pmatrix} = \begin{pmatrix} 1/10 & -1/20 \\ 1/5 & -1/10 \\ -1/2 & -1/4 \end{pmatrix}.$$

Verificamos uma das condições:

$$\begin{aligned} \mathrm{A}\mathrm{A}^{+}\mathrm{A} &= \begin{pmatrix} 1 & 2 & -1 \\ -2 & -4 & -2 \end{pmatrix}\begin{pmatrix} 1/10 & -1/20 \\ 1/5 & -1/10 \\ -1/2 & -1/4 \end{pmatrix}\begin{pmatrix} 1 & 2 & -1 \\ -2 & -4 & -2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & -1 \\ -2 & -4 & -2 \end{pmatrix} \\ &= \mathrm{A}. \end{aligned}$$

◀

★ 9.1.4 Método iterativo de Ben-Israel e Cohen usando maior autovalor

Há um método iterativo para aproximar a matriz pseudoinversa de uma matriz dada.

Teorema 9.18. *Seja λ o maior autovalor de AA^T (que é quadrada). Para qualquer b tal que $0 < b\lambda < 2$, e qualquer $p \geq 2$, defina a sequência de matrizes $B_0, B_1, \ldots$ definida recursivamente a seguir:*

$$\begin{aligned} B_0 &= bA^T \\ T_k &= \mathcal{I} - B_k A \\ B_{k+1} &= B_k + \sum_{i=1}^{p-1} T_k^i B_k \end{aligned}$$

Quando $p \to \infty$, $B_k \to A^+$.

Exemplo 9.19. Calcularemos a pseudoinversa de

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \\ 0 & 1 \end{pmatrix}$$

Temos

$$AA^T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix},$$

com autovalores 0, 1 e 2. Como o maior autovalor é $\lambda = 2$, escolhemos $b = 1/2$, de forma que $b\lambda = 1$.

Na primeira iteraçãom temos

$$\begin{aligned} B_0 &= \frac{1}{2} A^T, \\ T_0 &= \mathcal{I} - B_0 A. \end{aligned}$$

Ou seja,

$$B_0 = \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & -1/2 & 1/2 \end{pmatrix}, \quad T_0 = \begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix}.$$

Na segunda iteração temos

$$\begin{aligned} B_1 &= B_0 \\ T_1 &= \mathcal{I} - B_1 A. \end{aligned}$$

$$B_1 = B_0, \quad T_1 = \begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix}$$

Na terceira iteração,

$$\begin{aligned} B_2 &= B_1 + (T_0^0 B_0 + T_1 B_1) = B_1 + B_0 + T_1 B_1 \\ T_2 &= \mathcal{I} - B_2 A \end{aligned}$$

$$B_2 = \begin{pmatrix} 3/4 & 0 & 0 \\ 0 & -1/2 & 1/2 \end{pmatrix}, \quad T_2 = \begin{pmatrix} 1/4 & 0 \\ 0 & 0 \end{pmatrix}.$$

As próximas iterações nos darão

$$B_3 = \begin{pmatrix} 0.984375 & 0 & 0 \\ 0 & -1/2 & 1/2 \end{pmatrix}, \quad B_4 = \begin{pmatrix} 0.9999999 & 0 & \\ 0 & 1/2 & -1/2 \end{pmatrix},$$

e B_i claramente converge para

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1/2 & 1/2 \end{pmatrix},$$

que é a pseudoinversa de A. ◀

★ 9.1.5 Usando autovalores

Se conhecemos todos os autovalores de uma matriz, o Teorema 9.20 nos dá uma forma fechada para a pseudoinversa.

Teorema 9.20. *Sejam λ_i os autovalores de AA^T (que é quadrada). Então a pseudoinversa de A pode ser calculada pela fórmula*

$$A^+ = \sum_{\lambda_i \neq 0} \frac{1}{\lambda_i} \left(\prod_{j \neq i} (\lambda_i - \lambda_j)^{-1} \right) A^T \left(\prod_{j \neq i} (AA^T - \lambda_j \mathcal{I}) \right).$$

Exemplo 9.21. Seja

$$A = \begin{pmatrix} 1/2 & -1/2 \\ 1 & -1 \end{pmatrix}.$$

Temos

$$AA^T = \begin{pmatrix} 1/2 & 1 \\ 1 & 2 \end{pmatrix}$$

com autovalores 0 e $5/2$. Logo,

$$\begin{aligned} A^+ &= \frac{2}{5} \left(\frac{5}{2} - 0 \right)^{-1} A^T (AA^T - 0\mathcal{I}) \\ &= \frac{2^2}{5^2} A^T AA^T \\ &= \frac{2}{5} \begin{pmatrix} 1 & 2 \\ -1 & -2 \end{pmatrix}. \end{aligned}$$ ◀

Exemplo 9.22. Calcularemos a pseudoinversa de

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \\ 0 & 1 \end{pmatrix}$$

Calculamos

$$AA^T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix}$$

cujos autovalores são 0, 1 e 2. A pseudoinversa de A é

$$A^+ = \frac{1}{1} \left((1-0)^{-1} (1-2)^{-1} \right) A^T \left((AA^T - 0\mathcal{I})(AA^T - 2\mathcal{I}) \right)$$

$$
\begin{aligned}
&+\frac{1}{2}\left((2-0)^{-1}(2-1)^{-1}\right)A^{\mathsf{T}}\left((AA^{\mathsf{T}}-0\mathcal{I})(AA^{\mathsf{T}}-1\mathcal{I})\right)\\
&=(1)(-1)A^{\mathsf{T}}(AA^{\mathsf{T}}-2\mathcal{I})\\
&+(1/2)(1)A^{\mathsf{T}}(AA^{\mathsf{T}}-\mathcal{I})\\
&=-A^{\mathsf{T}}(AA^{\mathsf{T}}-2\mathcal{I})+\frac{1}{2}A^{\mathsf{T}}(AA^{\mathsf{T}}-\mathcal{I})\\
&=\begin{pmatrix}1 & 0 & 0\\ 0 & -\frac{1}{2} & \frac{1}{2}\end{pmatrix}.
\end{aligned}
$$

◀

A fórmula apresentada nesta seção é obtida do teorema da regularização de Tikhonov, que determina que $A^{+}=\lim_{x\to 0}A^{\mathsf{T}}(AA^{\mathsf{T}}+x\mathcal{I})^{-1}$, que não detalhamos neste texto.

9.2 Matrizes complexas

Pseudoinversas são definidas para matrizes complexas da maneira usual: a definição para matrizes reais é adaptada, tricando "transposta" por "conjugada transposta".

Definição 9.23 (Pseudoinversa de matriz complexa)**.** Seja A uma matriz complexa. A pseudoinversa de A é A^{+} tal que

i) $AA^{+}A=A$

ii) $A^{+}AA^{+}=A^{+}$

iii) $(AA^{+})^{\mathsf{H}}=AA^{+}$

iv) $(A^{+}A)^{\mathsf{H}}=A^{+}A$ ♦

Exemplo 9.24. A matriz

$$A=\begin{pmatrix}i & 0\\ 1 & 0\end{pmatrix}$$

tem pseudoinversa

$$A^{+}=\begin{pmatrix}-\frac{i}{2} & \frac{1}{2}\\ 0 & 0\end{pmatrix}$$

◀

Todos os teoremas e métodos deste capítulo valem quando se troca A^{T} por A^{H}.

9.3 Aplicações

9.3.1 Sistemas lineares

Tratamos agora de sistemas lineares descritos na forma

$$A\mathbf{x}=\mathbf{b}.$$

Quando A é singular ou não é quadrada, podemos ter um sistema indeterminado ou um sistema incompatível. Nestas situações, podemos tentar escolher a "melhor" dentre as possíveis alternativas.

- Se o sistema é indeterminado, temos infinitas soluções. Queremos aquela com a menor norma possível.
- Se o sistema é incompatível, não há solução. Queremos então encontrar o vetor para o qual a distância $d(A\mathbf{x}, \mathbf{b})$ é a menor possível.

Quando A é quadrada e $\det A \neq 0$, uma das maneiras de determinar a solução para um sistema linear é computar $\mathbf{x} = A^{-1}\mathbf{b}$. O teorema a seguir nos garante, no entanto, que mesmo quando A é singular ou nao é quadrada, se usarmos a pseudoinversa ao invés da inversa obteremos uma solução com a menor distância possível de $\mathbf{b}$.

Teorema 9.25. *Seja A uma matriz real $m \times n$ e $\mathbf{b} \in \mathbb{R}^m$. Então*

$$||A\mathbf{x} - \mathbf{b}||^2 = ||A\mathbf{x} - AA^+\mathbf{b}||^2 + ||(\mathcal{I}_m - AA^+)\mathbf{b}||^2.$$

Demonstração. Usando a definição de pseudoinversa ($AA^+A = A$), temos

$$\begin{aligned} A\mathbf{x} - \mathbf{b} =& (A\mathbf{x} - AA^+\mathbf{b}) - (\mathcal{I}_m - AA^+)\mathbf{b} \\ =& AA^+(A\mathbf{x} - \mathbf{b}) = (\mathcal{I}_m - AA^+)\mathbf{b}. \end{aligned}$$

Para demonstrar o teorema, observamos que a igualdade enunciada assemelha-se ao Teorema de Pitágoras para vetores ortogonais. Assim, ela deve valer se e somente se $A\mathbf{x} - AA^+\mathbf{b}$ e $(\mathcal{I}_m - AA^+)\mathbf{b}$ forem ortogonais. Calculamos o produto interno

$$\begin{aligned} \left\langle AA^+(A\mathbf{x} - \mathbf{b}, (\mathcal{I}_m - AA^+)\mathbf{b} \right\rangle &= \left\langle A\mathbf{x} - \mathbf{b}, (AA^+)^T(\mathcal{I}_m - AA^+)\mathbf{b} \right\rangle \\ &= \left\langle A\mathbf{x} - \mathbf{b}, (AA^+)(\mathcal{I}_m - AA^+)\mathbf{b} \right\rangle \\ &= \langle A\mathbf{x} - \mathbf{b}, \mathbf{0} \rangle = 0, \end{aligned}$$

e concluimos a demonstração. ■

Olhando novamente para a igualdade no teorema 9.25, observamos que no lado direito, apenas o primeiro termo, $||A\mathbf{x} - AA^+\mathbf{b}||^2$, depende da escolha de $\mathbf{x}$. Queremos portanto minimizá-lo a fim de minimizar o lado esquerdo, $||A\mathbf{x} - \mathbf{b}||^2$. Para minimizar $||A\mathbf{x} - AA^+\mathbf{b}||^2$ podemos evidentemente escolher $\mathbf{x}$ tal que $A\mathbf{x} = AA^+\mathbf{b}$, ou seja,

$$\mathbf{x} = A^+\mathbf{b}.$$

Desta discussão concluímos que:

- Se A é quadrada e não-singular, então $A^+\mathbf{b} = A^{-1}\mathbf{b}$, e ambas nos darão a mesma solução única;
- Se o sistema é incompatível, $A^+\mathbf{b}$ nos dá a solução que mais se aproxima do que poderia ser uma solução ótima;
- Se o sistema é indeterminado, $A^+\mathbf{b}$ nos dará, dentre as infinitas soluções, uma que minimiza a norma.

Exemplo 9.26. Seja $A\mathbf{x} = \mathbf{b}$ um sistema linear com

$$A = \begin{pmatrix} 1 & -1 & 0 \\ 0 & -2 & -1 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$$

O sistema é indeterminado. A pseudoinversa de A é

$$A^+ = \frac{1}{3}\begin{pmatrix} \frac{5}{2} & -1 \\ -\frac{1}{2} & -1 \\ 1 & -1 \end{pmatrix}$$

E a solução com a menor norma possível é, portanto,

$$\mathbf{x} = A^+\mathbf{b} = \frac{1}{3}\left(\frac{23}{2}, -\frac{7}{2}, 4\right)^\mathsf{T}.$$

A norma de $\mathbf{x}$ é $\sqrt{107}/\sqrt{6} \approx 17.83$. ◀

Exemplo 9.27. Seja $A\mathbf{x} = \mathbf{b}$ um sistema linear com

$$A = \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} -1 \\ 3 \end{pmatrix}$$

O sistema é claramente incompatível. A pseudoinversa de A é

$$A^+ = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 \end{pmatrix}$$

E a solução $\hat{\mathbf{x}}$ tal que $A\hat{\mathbf{x}}$ mais se aproxima de $\mathbf{b}$ é

$$\hat{\mathbf{x}} = A^+\mathbf{b} = \begin{pmatrix} -2 \\ 0 \end{pmatrix}.$$

Para completar o exemplo, $A\hat{\mathbf{x}} = (-2, 2)^\mathsf{T}$, com norma $2\sqrt{2} \approx 2.83$. A norma de $\mathbf{b}$ é $\sqrt{10} \approx 3.16$. ◀

Exercícios

Ex. 249 — Calclue as pseudoinversas das matrizes a seguir.

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 2 & 5 & 6 \end{pmatrix}$$

Ex. 250 — (Fácil) Prove que se A é $m \times n$, então A^+ é $n \times m$.

Ex. 251 — Prove o teorema 9.7.

Ex. 252 — Se (AA^T) é não-singular, determine uma fórmula simples para a pseudoinversa de A.

Ex. 253 — Seja

$$A = \begin{pmatrix} 1 & 2 & 1 \\ -1/2 & -1 & -1/2 \end{pmatrix}.$$

i) Calcule a pseudoinversa de A usando o método da decomposição em posto completo.

ii) Calcule a decomposição de A em valores singulares, e use esta decomposição para calcular A^+.

★ iii) Calcule A^+ usando o método dos autovalores, e verifique que o resultado é o mesmo obtido no item (i).

★ iv) Calcule algumas iterações do método iterativo de Ben-Israel e Cohen; verifique que a sequência converge para a matriz obtida no item (i).

Ex. 254 — Considere todos os sistemas incompatíveis $A\mathbf{x} = \mathbf{b}$ onde os coeficientes de A estão no intervalo $[-1, +1]$. Existe um valor máximo para a distância mínima entre as aproximações $A^+\hat{\mathbf{x}}$ e $\mathbf{b}$?

Ex. 255 — Considere o sistema $A\mathbf{x} = \mathbf{b}$, com

$$A = \begin{pmatrix} 1 & 3 & 1 \\ 0 & -1 & 0 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} -2 \\ 6 \end{pmatrix}$$

Encontre a solução $\mathbf{x}$ que minimize a distância $d(A\mathbf{x}, \mathbf{b})$.

Ex. 256 — Prove que para qualquer matriz complexa A,

- $(kA)^H = \overline{k}A^H$
- Se A é quadrada, $\det A^* = \overline{\det A}$

Capítulo 10

Forma de Jordan

No Capítulo 6 mencionamos que uma matriz de ordem n é diagonalizável se e somente se tem n autovalores LI (teorema 6.55), mas nada dissemos a respeito das matrizes que não são diagonalizáveis. Neste Capítulo verificamos que todo operador é similar a uma matriz em uma forma "quase" diagonal, chamada de *forma de Jordan*[1]. A forma de Jordan de um operador é diagonal em blocos,

$$\begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_k \end{pmatrix},$$

e cada bloco J_i tem uma mesma entrada (possivelmente nnula) em toda a diagonal, e uns acima dela, sendo todas as outras entradas iguais a zero:

$$J_i = \begin{pmatrix} \lambda_i & 1 & & \\ & \lambda_i & & \\ & & \ddots & 1 \\ & & & \lambda_i \end{pmatrix}.$$

Embora não detalhemos este fato no texto, somente garantimos a existência da forma normal de Jordan para espaços vetoriais sobre corpos que sejam *algebricamente fechados* (ou seja, todo polinômio não constante neste corpo tem alguma raiz neste mesmo corpo – o que não acontece com reais, por exemplo: o polinômio $x^2 + 1$ tem raízes complexas, mas não reais). Ao desenvolvermos a forma de Jordan, portanto, falaremos em operadores em $\mathbb{C}^n$, já que $\mathbb{C}$ é algebricamente fechado.

Definimos agora formalmente a forma de Jordan.

Definição 10.1 (bloco de Jordan)**.** Um *bloco de Jordan* é uma matriz quadrada onde todos os elementos da diagonal são iguais a um mesmo elemento λ; elementos acima da diagonal são todos iguais a um; e todos

[1] Também chamada de *forma normal* de Jordan, ou *forma canônica* de Jordan.

os outros elementos da matriz são zero.

$$\begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & & 0 \\ 0 & 0 & \lambda & & \vdots \\ \vdots & & & \ddots & 1 \\ 0 & 0 & \dots & & \lambda \end{pmatrix} \quad \blacklozenge$$

Pode-se alternativamente definir blocos de Jordan tendo uns abaixo da diagonal, e não acima.

Exemplo 10.2. Todas as matrizes a seguir são blocos de Jordan.

$$\begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix} \quad \begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{pmatrix} \quad \begin{pmatrix} i & 1 & 0 & 0 \\ 0 & i & 1 & 0 \\ 0 & 0 & i & 1 \\ 0 & 0 & 0 & i \end{pmatrix} \quad \begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix} \quad \blacktriangleleft$$

Definição 10.3 (forma de Jordan)**.** A matriz de um operador linear T está na *forma de Jordan* se é diagonal por blocos, e os blocos da diagonal são blocos de Jordan, cada um tendo um autovalor de T em sua diagonal – ou seja,

$$\operatorname{diag}(B_1, \dots, B_k) = \begin{pmatrix} B_1 & 0 & \dots & 0 \\ 0 & B_2 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \dots & B_k \end{pmatrix},$$

onde cada B_i é um bloco de Jordan. $\blacklozenge$

Exemplo 10.4. O operador representado pela matriz abaixo não é diagonalizável, porque tem somente o autovalor -1, com um único autovetor LI.

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

A forma de Jordan deste operador é

$$\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \quad \blacktriangleleft$$

Exemplo 10.5. Todas as matrizes a seguir estão na forma de Jordan.

$$A = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix} \quad B = \left(\begin{array}{cc:cc} 3 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ \hdashline 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 4 \end{array}\right) \quad C = \left(\begin{array}{cc:cc} \pi & 1 & 0 & 0 \\ 0 & \pi & 0 & 0 \\ \hdashline 0 & 0 & e & 1 \\ 0 & 0 & 0 & e \end{array}\right)$$

$$D = \left(\begin{array}{ccc:ccc:cc} 3 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 5 \end{array}\right) \quad E = \left(\begin{array}{ccc:ccc:cc} 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 8 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 8 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 8 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 8 \end{array}\right)$$

Note que a matriz D tem *tres* blocos de Jordan: um de ordem 3 com $\lambda_1 = 3$ na diagonal; outro de ordem 2, também com $\lambda_2 = 3$ na diagonal; e um de ordem 2 com $\lambda_3 = 5$ na diagonal. $\blacktriangleleft$

O Exercício 258 pede a demonstração do Lema 10.6.

Lema 10.6. *Se* N *é uma matriz nilpotente tal que* $N^k = 0$*, então*

$$\begin{aligned} e^N &= \mathcal{I} + N + \frac{N^2}{2} + \frac{N^3}{6} + \cdots + \frac{n^{k-1}}{(k-1)!} \\ &= \sum_{i=0}^{k-1} \frac{N^i}{i!}. \end{aligned}$$

Lema 10.7. *Seja* D *uma matriz diagonal e* N *uma matriz nilpotente tais que* $DN = ND$*. Então*

$$e^{D+N} = e^{D+N} = e^D e^N.$$

Teorema 10.8. *Seja* J *uma matriz na forma de Jordan, composta por blocos de Jordan* $J_1, J_2, \ldots, J_k$*. Então*

$$e^{kJ} = e^D e^N,$$

onde D *é a matriz diagonal com os autovalores de* J*, e* N *é* $J - D$*, contendo apenas os uns na diagonal.*

Demonstração. A forma de Jordan é sempre a soma de uma matriz diaonal com uma nilpotente, e o Lema 10.7 dá a forma da exponencial. ■

★ 10.1 Existência e cálculo da forma de Jordan

Nesta seção mostramos a existência da forma de Jordan. Como a demonstração é construtiva, dela podemos extrair também um algoritmo para a construção da forma de Jordan de qualquer matriz quadrada.

10.1.1 Subespaços invariantes

Definição 10.9 (subespaço invariante para um operador)**.** Seja W um subespaço de um espaço vetorial V. Dizemos W é *invariante sob* W se para todo vetor $\mathbf{w} \in W$, o operador resulta em outro vetor também em W – ou seja, $T\mathbf{w} \in W$. ♦

Exemplo 10.10. Em $\mathbb{R}^2$, considere o subespaço W contendo os vetores $(x, 2x)^T$. Este subespaço é composto pelos pontos da reta $y = 2x$. O operador $T(x, y) = (4x, 8y)$. O subespaço W é invariabte sob T, porque leva os pontos daquela reta a outros pontos também nela.

O subespaço W já não é invariante para o operador $S(x, y) = (1, y)$, porque $S(2, 4)^T = (1, 4)^T$, e $(1, 4)^T \notin W$. ◀

Um fato evidente é que o subespaço trivial é invariante para qualquer operador linear.

Exemplo 10.11. Em $\mathbb{R}^3$, considere o subespaço W contendo os vetores $(x, 2x, z)^T$. Este subespaço é composto pelos pontos de um plano. Este subespaço é invariante para o operador $T(x, y, z) = (x/2, y/2, 10z)$, mas não para o operador $S(x, y, z) = (z, y, x)^T$. ◀

Exemplo 10.12. Sabemos que o espaço das funções contínuas e diferenciáveis (definido no exemplo 1.54) é subespaço de $\mathcal{F}(\mathbb{R})$. Este subespaço é invariante sob o operador $T(f) = 2f$, porque se f é contínua, $2f(x)$ também é. ◀

Teorema 10.13. *Seja V um espaço vetorial igual à soma direta de dois subespaços U, W: $V = U \oplus W$. Se B_U e B_W são bases para U e W, então $B = B_U \cup B_W$ é base para V.*

Teorema 10.14. *Seja V um espaço vetorial igual à soma direta de dois subespaços U, W: $V = U \oplus W$. Se B_U e B_W são bases para U e W. Em forma matricial, as bases B_U e B_W concatenadas formam a matriz*

$$B = \begin{pmatrix} B_U & B_W \end{pmatrix}.$$

Seja T um operador em V, expresso na base B na forma matricial:

$$T = \begin{pmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{pmatrix}.$$

Se $T_{12} = 0$ então W é invariante para T.
Se $T_{21} = 0$ então U é invariante pra T.

Este teorema pode ser generalizado para a soma direta de vários subespaços (não apenas dois).

10.1.2 Autovetores generalizados

Se T é diagonalizável, então V é a soma direta dos autoespaços de T.

$$\begin{aligned} N_1(\lambda) &= \ker(T - \lambda\mathcal{I}) \\ N_2(\lambda) &= \ker(T - \lambda\mathcal{I})^2 \\ &\cdots \\ N_m(\lambda) &= \ker(T - \lambda\mathcal{I})^m \end{aligned}$$

Então

$$N_1(\lambda) \subset N_2(\lambda) \subset \cdots \subset N_m(\lambda).$$

Seja T um operador com n autovalores e n autovetores diferentes, $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Os autoespaços são

$$\ker(T - \lambda_i\mathcal{I}), \quad i = 1, \ldots, n.$$

Cada autoespaço é invariante para T, porque se

$$(T - \lambda_i\mathcal{I})\mathbf{v} = \mathbf{0}$$

então, para $T\mathbf{v}$, temos

$$(T - \lambda_i\mathcal{I})T\mathbf{v} = T(T - \lambda_i\mathcal{I})\mathbf{v} = \mathbf{0}.$$

Definição 10.15 (autovetor generalizado)**.** Seja T um operador linear. Um vetor $\mathbf{v}$ é um *autovetor generalizado* se existem um escalar λ e um inteiro positivo p tais que

$$\begin{aligned} (T - \lambda\mathcal{I})^p\mathbf{v} &= \mathbf{0}, \quad \text{e} \\ (T - \lambda\mathcal{I})^{p-1}\mathbf{v} &\neq \mathbf{0}. \end{aligned}$$

Dizemos que $\mathbf{v}$ tem *ordem* p. ♦

Observe que se $p = 1$, o autovetor generalizado é o mesmo que um autovetor, como definido no capítulo 6.

Exemplo 10.16. Seja

$$T = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

um operador linear. Os autovalores de T são 1 e 2. Para o autovalor 1, o vetor

$$\mathbf{v} = \begin{pmatrix} 3 \\ 2 \\ -1 \end{pmatrix}$$

é um autovetor generalizado de ordem 2, porque

$$(T - 1\mathcal{I})^2\mathbf{v} = \begin{pmatrix} 0 & 2 & 4 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \\ -1 \end{pmatrix} = \mathbf{0},$$

mas

$$(T - 1\mathcal{I})\mathbf{v} = \begin{pmatrix} 0 & 2 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}$$ ◀

Definição 10.17 (cadeia de Jordan)**.** Seja $\mathbf{v}$ um autovetor generalizado de ordem p para o autovalor λ do operador T. Então a sequência de vetores

$$\begin{aligned} &\mathbf{v}, \\ &(T - \lambda\mathcal{I})\mathbf{v}, \\ &(T - \lambda\mathcal{I})^2\mathbf{v}, \\ &\quad\vdots \\ &(T - \lambda\mathcal{I})^{p-1}\mathbf{v} \end{aligned}$$

é uma *cadeia de Jordan*, ou *cadeia de autovetores generalizados*, pertencente ao autovalor λ. ♦

Exemplo 10.18. Para o operador T, autovalor 1 e o vetor $\mathbf{v}$ do exemplo 10.16, uma cadeia de Jordan é

$$\mathbf{v},\ (T - \mathcal{I})\mathbf{v} = \begin{pmatrix} 3 \\ 2 \\ -1 \end{pmatrix},\ \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}$$ ◀

Teorema 10.19. *Uma cadeia de Jordan pertencente a um autovalor de um operador é LI.*

Demonstração. Seja T um operador e

$$\mathbf{u},\ T\mathbf{u}, \ldots, T^k\mathbf{u}$$

uma cadeia de Jordan (ou seja, $T^k\mathbf{u} \neq \mathbf{0}$, mas $T^{k+1}\mathbf{u} = \mathbf{0}$). Então, suponha que

$$a_0\mathbf{u} + a_1T\mathbf{u} + \ldots + a_kT^k\mathbf{u} = \mathbf{0}.$$

Queremos mostrar que isto implica em todos os a_i serem zero.

Já que $T^{k+1}\mathbf{u} = \mathbf{0}$, e o mesm vale para T^q, com $q > k$, aplicamos T^k sobra a combinação linear. Obtemos

$$\begin{aligned} T^k a_0\mathbf{u} + a_1 T^{k+1}\mathbf{u} + \ldots + a_k T^{k+k}\mathbf{u} &= \mathbf{0} \\ T^k a_0\mathbf{u} + \mathbf{0} + \ldots + \mathbf{0} &= \mathbf{0} \\ a_0 T^k\mathbf{u} &= \mathbf{0}, \end{aligned}$$

o que implica que $a_0 = 0$. Podemos então reescrever a combinação linear sem o primeiro termo, já que ele será zero:

$$a_1 T\mathbf{u} + \ldots + a_k T^k\mathbf{u} = \mathbf{0}.$$

No entanto, podemos usar raciocínio análogo ao anterior para mostrar que $a_1 = 0$, e assim por diante, até $a_k = 0$. Com isso temos todos os $a_i = 0$, e a cadeia de Jordan é LI. ■

O exercício 259 pede a demonstração do teorema 10.21, que generaliza o teorema 10.19 para a união de várias cadeias de Jordan.

Teorema 10.20. *A união de cadeias de Jordan pertencentes a diferentes autovalores de um operador é LI.*

Teorema 10.21. *Seja T um operador em um espaço V, com autovalores $\lambda_1, \ldots, \lambda_k$. Então*

$$V = \ker(T - \lambda_1 \mathcal{I})^{m_1} \oplus \cdots \oplus \ker(T - \lambda_k \mathcal{I})^{m_k}.$$

10.1.3 Existência da forma de Jordan (para operadores nilpotentes)

Definição 10.22. Um operador linear T é *nilpotente* se existe $a > 0$ tal que $T^a = 0$. O número a é o *índice de nilpotencia* de T. ♦

Exemplo 10.23. Os operadores

$$A = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & -3 \\ 3 & -3 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

são nilpotentes, porque

$$A^2 = 0, B^2 = 0, C^3 = 0.$$

Os índices de nilpotência de A, B e C são 2, 2 e 3.

Já o operador

$$D = \operatorname{diag}(2,3,4) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}$$

não é nilpotente, porque para todo $k > 0$, $D^k = \operatorname{diag}(2^k, 3^k, 4^k)$. ◄

Teorema 10.24. *Se T é um operador nilpotente em um espaço V de dimensão n, então o único autovalor de T é zero, com multiplicidade algébrica n.*

Lema 10.25. *Seja $T : V \to V$ um operador linear nilpotente. Existe uma base de V formada por cadeias de Jordan – ou seja, uma base da forma*

$$\left(\mathbf{v}_1, T\mathbf{v}_1, \ldots, T^{a_1-1}\mathbf{v}_1,\ \mathbf{v}_2, T\mathbf{v}_2, \ldots, T^{a_2-1}\mathbf{v}_2,\ \ \ldots,\ \ \mathbf{v}_q, T\mathbf{v}_q, \ldots, T^{a_q-1}\mathbf{v}_q\right),$$

com $T^{a_i}\mathbf{v}_i = 0$.

Demonstração. A demonstração é por indução na dimensão de V.

Como base temos espaços de dimensão um: trivialmente, qualquer operador de dimensão um já está na forma de Jordan, porque já é diagonal.

A hipótese de indução é a de que para todo operador T em um espaço V de dimensão k existe uma base onde T está na forma de Jordan.

Presumimos que o posto do operador não é zero, e que também não é completo. Como a imagem de T tem posto menor que $\dim V$, tomamos agora o mesmo operador T, mas restrito à sua imagem, $T(V)$. Pela hipótese de indução, podemos encontrar vetores $\mathbf{v}_1, \ldots, \mathbf{v}_q$ tais que

$$\begin{aligned}
&\mathbf{v}_1, T\mathbf{v}_1, \ldots, T^{a_1-1}\mathbf{v}_1,\\
&\mathbf{v}_2, T\mathbf{v}_2, \ldots, T^{a_2-1}\mathbf{v}_2,\\
&\quad\vdots\\
&\mathbf{v}_q, T\mathbf{v}_q, \ldots, T^{a_q-1}\mathbf{v}_q,
\end{aligned}$$

formem uma base para a imagem $T(V)$, e $T^{a_i}\mathbf{v}_i = \mathbf{0}$.

Agora, para todo $1 \leq i \leq q$, podemos escolher um vetor $\mathbf{u}_i$ tal que $T(\mathbf{u}_i) = \mathbf{v}_i$. Obtemos então

$$\begin{aligned}
&\mathbf{u}_1, \mathbf{v}_1, T\mathbf{v}_1, \ldots, T^{a_1-1}\mathbf{v}_1,\\
&\mathbf{u}_2, \mathbf{v}_2, T\mathbf{v}_2, \ldots, T^{a_2-1}\mathbf{v}_2,\\
&\quad\vdots\\
&\mathbf{u}_q, \mathbf{v}_q, T\mathbf{v}_q, \ldots, T^{a_q-1}\mathbf{v}_q,
\end{aligned}$$

que é o mesmo que

$$\begin{aligned}
&\mathbf{u}_1, T\mathbf{u}_1, T^2\mathbf{u}_1, \ldots, T^{a_1}\mathbf{u}_1,\\
&\mathbf{u}_2, T\mathbf{u}_2, T^2\mathbf{u}_2, \ldots, T^{a_2}\mathbf{u}_2,\\
&\quad\vdots\\
&\mathbf{u}_q, T\mathbf{u}_q, T^2\mathbf{u}_q, \ldots, T^{a_q}\mathbf{u}_q,
\end{aligned}$$

com $T^{a_i+1}\mathbf{u}_i = \mathbf{0}$ para todo $\mathbf{u}_i$. Continuamos tendo então q cadeias de Jordan, que portanto são LI (pelo teorema 10.21).

Continuamos agora observando que certamente, todos os vetores $T^{a_i}\mathbf{u}_i$ pertencem a $\ker T$. Temos então q vetores do kernel de T, e podemos extender este conjunto com mais m vetores $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_m$ para completar uma base para $\ker T$.

Os vetores

$$\begin{aligned}
&\mathbf{u}_1, T\mathbf{u}_1, T^2\mathbf{u}_1, \ldots, T^{a_1}\mathbf{u}_1,\\
&\mathbf{u}_2, T\mathbf{u}_2, T^2\mathbf{u}_2, \ldots, T^{a_2}\mathbf{u}_2,\\
&\quad\vdots\\
&\mathbf{u}_q, T\mathbf{u}_q, T^2\mathbf{u}_q, \ldots, T^{a_q}\mathbf{u}_q,\\
&\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_m
\end{aligned}$$

são uma base do espaço V. Contamos as dimensões:

- A nulidade de T é $q + m$.
- O posto de T é $a_1 + \ldots + a_q$.

Pelo teorema do núcleo e da imagem, temos

$$\begin{aligned}\dim V =& (a_1 + \cdots + a_q) + q + m \\ =& (a_1 + 1) + \cdots + (a_q + 1) + m,\end{aligned}$$

que é o número de vetores que temos. ■

Teorema 10.26. *Seja $T : V \to V$ um operador linear nilpotente. Existe uma base de V em que a matriz do operador T é representada na forma de Jordan.*

Demonstração. Suponha que exista P tal que $P^{-1}TP = J$, onde J está na forma de Jordan. Então particione P de acordo com os blocos de Jordan:

$$P = \begin{pmatrix} P_1 & P_2 \ldots P_k \end{pmatrix}.$$

Cada P_i é composto de n_i colunas:

$$P_i = \begin{pmatrix} \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{n_i} \end{pmatrix}.$$

Como $P^{-1}TP = J$, temos

$$AP_i = P_i J_i = P_i(\lambda_i \mathcal{I} + N_i).$$

Olhando para o bloco P_i, temos

$$\begin{pmatrix} A\mathbf{v}_1, A\mathbf{v}_2, \ldots, A\mathbf{v}_{n_i} \end{pmatrix} = \lambda_i \begin{pmatrix} \mathbf{v}_1, \ldots, \mathbf{v}_{n_i} \end{pmatrix} + \begin{pmatrix} \mathbf{v}_2, \mathbf{v}_3, \ldots, \mathbf{v}_{n_i}, \mathbf{0} \end{pmatrix},$$

$$\begin{pmatrix} (A - \lambda_i \mathcal{I})\mathbf{v}_1, (A - \lambda_i \mathcal{I})\mathbf{v}_2, \ldots, (A - \lambda_i \mathcal{I})\mathbf{v}_{n_i} \end{pmatrix} = \begin{pmatrix} \mathbf{v}_2, \mathbf{v}_3, \ldots, \mathbf{v}_{n_i}, \mathbf{0} \end{pmatrix}$$

ou seja,

$$\begin{aligned}\mathbf{v}_2 =& (A - \lambda_i \mathcal{I})\mathbf{v}_1, \\ \mathbf{v}_3 =& (A - \lambda_i \mathcal{I})\mathbf{v}_2, \\ &\vdots\end{aligned}$$

Assim, há uma base para V onde T fica na forma de Jordan *se e somente* se há uma base formada por uma cadeia de Jordan para cada autovalor. Com o Lema 10.25, concluímos a demonstração. ■

Como os autovalores de um operador nilpotente são todos zero, sua forma de Jordan sempre terá a diagonal zero, zeros ou uns imediatamente acima da diagonal:

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & \ddots & & \vdots \\ & & & 0 & 1 \\ 0 & \cdots & & & 0 \end{pmatrix}$$

10.1.4 Existência da forma de Jordan (caso geral)

Mostraremos agora que a existência da forma de Jordan para operadores nilpotentes implica na sua existência também para o caso geral.

Primeiro, mostramos que o espaço vetorial V pode ser decomposto na soma direta dos *kernels* das cadeias de Jordan de um operador T sobre V.

Lema 10.27. *Seja T um operador sobre um espaço V de dimensão finita, e λ um autovalor de T. Então é possível decompor V em*

$$V = \ker W \oplus \ker U,$$

tais que T é nilpotente em W, e a restrição de T a U é inversível.

Demonstração. Considere os operadores $T, T^2, T^3 \ldots$. Como V tem dimensão finita, pelo teorema do núcleo e da imagem, deve haver algum k para o qual $\ker(T^k) = \ker(T^{k+1})$. Escolhemos o menor k tal que esta igualdade valha.

Agora, também é claro que

$$\ker(T) \subseteq \ker(T^2) \subseteq \cdots \subseteq \ker T(T^k) = \ker(T^{k+1}) = \cdots$$

Tomamos $W = \ker(T^k)$ e $U = \operatorname{Im}(T^k)$, e argumentamos a seguir que estes subespaços satisfazem o enunciado do lema.

- $V = W \oplus U$: A soma das dimensões está correta, pelo teorema do núcleo e da imagem. Agora, seja $\mathbf{v} \in W \cap U$. Isso é o mesmo que (i) $\mathbf{v} \in W$, e então $T(\mathbf{v}) = \mathbf{0}$; (ii) $\mathbf{v} = T^k(\mathbf{x})$ para algum $x \in V$. Então $T^{2k}(\mathbf{x}) = \mathbf{0}$, e $\mathbf{x} \in \ker(T^{2k}) = \ker(T^k)$. Portanto, $\mathbf{v} = T^k(\mathbf{x}) = \mathbf{0}$. Isso mostra que $W \oplus U$ é soma direta.
- T *é nilpotente em W*: trivialmente, porque $W = \ker(T^k)$.
- *a restrição de T a U é inversível*: seja $\mathbf{v} \in \ker(T) \cap U$. Então $T(\mathbf{v}) = \mathbf{0}$. Como $U = \operatorname{Im}(T^k)$, então $\mathbf{v} = T^k(\mathbf{x})$, para algum $\mathbf{x} \in V$. Poratnto $T^{k+1}(\mathbf{x}) = T^k(\mathbf{v}) = \mathbf{0}$. Isso é o mesmo que dizer que $\ker(T^k) = \ker(T^{k+1})$. O kernel de T restrito a U portanto tem somente o zero, e T é inversível. ■

Teorema 10.28. *Seja T um operador sobre V, e $\lambda_1, \ldots, \lambda_k$ os autovalores de T. Então existem $a_1, \ldots, a_k$ tais que V pode ser decomposto em*

$$V = \ker(T - \lambda_1 \mathcal{I})^{a_1} \oplus \ker(T - \lambda_2 \mathcal{I})^{a_2} \oplus \cdots \oplus \ker(\lambda_k \mathcal{I})^{a_k},$$

sendo cada $\ker(T - \lambda_i \mathcal{I})^{a_i}$ invariante para T.

Demonstração. Segue por indução no número de autovalores, usando o lema 10.27. ■

Teorema 10.29. *Seja $T : V \to V$ um operador linear. Existe uma base de V em que a matriz do operador T é representada na forma de Jordan.*

Demonstração. ■

Exemplo 10.30. Abaixo temos um operador em $\mathbb{R}^4$:

$$\begin{pmatrix} 2 & 0 & 0 & 1 \\ 3 & 3 & 0 & 3 \\ 0 & 0 & 4 & 7 \\ 1 & 0 & 0 & 2 \end{pmatrix}$$

Os autovalores deste são 3, 1 e 4, e sua forma de Jordan é

$$\begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}. \qquad \blacktriangleleft$$

10.2 Estabilidade numérica

A matriz A mostrada a seguir já está na forma de Jordan.

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Se adicionarmos ε a uma das entradas da matriz, sua forma de Jordan muda consideravelmente (veja que agora a forma de Jordan é diagonal).

$$B = \begin{pmatrix} 1 & 1 & 0 \\ \varepsilon & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \longrightarrow \quad = \begin{pmatrix} 1-\sqrt{\varepsilon} & 0 & 0 \\ 0 & 1+\sqrt{\varepsilon} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

10.3 Aplicações

10.3.1 Álgebra Linear [forma de Jordan]

Uma intrigante aplicação da forma de Jordan é na demonstração de um teorema de enunciado absolutamente simples, mas cuja demonstração sem a forma de Jordan torna-se surpreendentemente complexa.

Teorema 10.31. *Toda matriz é similar a sua transposta.*

Demonstração. Sabemos que $A = PJP^{-1}$, portanto basta mostrar que J é similar a J^T, que mostramos a seguir.

$$\begin{pmatrix} \lambda & 1 & \\ & \ddots & 1 \\ & & \lambda \end{pmatrix} = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix} \begin{pmatrix} \lambda & & \\ 1 & \ddots & \\ & 1 & \lambda \end{pmatrix} \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix} \qquad \blacksquare$$

Enunciamos também outro teorema que podemos provar facilmente usando a forma de Jordan.

Teorema 10.32. *Para qualquer matriz A, $\lim_{n\to\infty} A^n = 0$ se e somente se os módulos dos autovalores de A são menores que 1.*

Demonstração. A é similar a J na forma de Jordan, que tem os autovalores na diagonal e elementos unitários acima da diagonal. Para cada bloco de jordan B,

$$B^2 = \begin{pmatrix} \lambda^2 & 2\lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda^2 & 2\lambda & 1 & & \\ \vdots & & \ddots & & & \\ 0 & & & & & \\ 0 & & & & \lambda^2 & 2\lambda \\ 0 & \cdots & & & & \lambda^2 \end{pmatrix},$$

e

$$B^n = \begin{pmatrix} \lambda^n & n\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & \binom{n}{3}\lambda^{n-3} & \cdots \\ 0 & \lambda^n & n\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & \cdots \\ \vdots & & \ddots & & \\ & & & \lambda^n & n\lambda^{n-1} \\ 0 & \cdots & & & \lambda^n \end{pmatrix}.$$

Cada linha tem, começando no elemneto da diagonal, os coeficientes da expansão binomial de $(1+\lambda)^n$:

$$\binom{n}{0}\lambda^n, \ \binom{n}{1}\lambda^{n-1}, \ \cdots, \ \binom{n}{n}\lambda^0$$

Todas as entradas são da forma $a\lambda^{n-k}$, com $k \leq n$. Se $|\lambda| < 1$, todos os valores tendem a zero. Claramente, se a matriz tende a zero em uma base, tenderá a zero em qualquer base, já que a representação do zero não depende de base. ■

10.3.2 Equações Diferenciais [forma de Jordan]

Se um sistema dinâmico é descrito por uma matriz não diagonalizável, podemos usar sua forma de Jordan. Por exemplo,

$$\begin{aligned} \frac{d}{dx}x_1(t) &= 2x_1(t) + x_2(t) \\ \frac{d}{dx}x_2(t) &= 2x_2(t) + x_3(t) \\ \frac{d}{dx}x_3(t) &= 2x_3(t). \end{aligned}$$

A solução para este sistema é

$$\mathbf{x}(t) = e^{tJ}\mathbf{x}(0),$$

por isso só precisamos calcular e^{tJ}. Como temos um único bloco de Jordan, já sabemos que teremos

$$e^{tJ} = e^D e^N,$$

com

$$D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad N = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Temos $N^3 = 0$, portanto

$$\begin{aligned} e^tN &= \sum_{i=0}^{2} \frac{N^i}{i!} \\ &= \frac{N^0}{0!} + \frac{N}{1} + \frac{N^2}{2} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & t & 0 \\ 0 & 0 & t \\ 0 & 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 & t^2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \end{aligned}$$

$$= \begin{pmatrix} 1 & t & t^2/2 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}$$

Calculamos também

$$e^D = \begin{pmatrix} e^{2t} & 0 & 0 \\ 0 & e^{2t} & 0 \\ 0 & 0 & e^{2t} \end{pmatrix}$$

Finalmente, temos

$$\begin{aligned} e^{tJ} &= e^D e^N \\ &= \begin{pmatrix} e^{2t} & 0 & 0 \\ 0 & e^{2t} & 0 \\ 0 & 0 & e^{2t} \end{pmatrix} \begin{pmatrix} 1 & t & t^2/2 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} e^{2t} & te^{2t} & \frac{1}{2}t^2e^{2t} \\ 0 & e^{2t} & te^{2t} \\ 0 & 0 & e^{2t} \end{pmatrix}. \end{aligned}$$

A descrição de $\mathbf{x}$ em função de t é, portanto,

$$\begin{aligned} \mathbf{x}(t) &= e^{tJ}\mathbf{x}(0) \\ &= \begin{pmatrix} e^{2t} & te^{2t} & \frac{1}{2}t^2e^{2t} \\ 0 & e^{2t} & te^{2t} \\ 0 & 0 & e^{2t} \end{pmatrix} \mathbf{x}(0) \\ &= e^{2*t} \begin{pmatrix} x_1(0) + tx_2(0) + \frac{t^2x_3(0)}{2} \\ x_2(0) + tx_3(0) \\ x_3(0) \end{pmatrix}. \end{aligned}$$

Finalmente temos

$$\begin{aligned} x_1(t) &= e^{2t}\left(x_1(0) + tx_2(0) + \frac{t^2x_3(0)}{2}\right) \\ x_2(t) &= e^{2t}\big(x_2(0) + tx_3(0)\big) \\ x_3(t) &= e^{2t}\big(x_3(0)\big). \end{aligned}$$

Neste exemplo o sistema dinâmico já era descrito por uma matriz na forma de Jordan. É evidente que um sistema dinâmico poderia ser descrito por uma matriz A não diagonalizável, e que houvesse a necessidade de calcular P, P^{-1} e J tais que $A = PJP^{-1}$. Este processo é semelhante ao que usamos quando tratamos de sistemas dinâmicos na Seção 6.6.5, e o Exercício 262 traz um sistema como este.

Este método, descrevendo a solução como $e^{tD}e^{tN}$, é importante para a *análise* do sistema dinâmico e de sua solução, mas não é o mais eficiente para se computá-la.

Exercícios

Ex. 257 — Calcule a forma de Jordan:

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 2 & 2 \\ 1 & 0 & 1 \end{pmatrix} \quad C = \begin{pmatrix} 0 & 0 & 0 \\ 2 & 1 & 2 \\ 3 & 0 & 1 \end{pmatrix} \quad D = \begin{pmatrix} 2 & 0 & 0 & \dots & 0 & 0 \\ 2 & 2 & 0 & & & \\ 0 & 2 & 2 & & & \\ \vdots & & 2 & \ddots & & \\ 0 & & & \ddots & 2 & \\ 0 & & & & 2 & 2 \end{pmatrix}$$

(D tem entradas igual a 2 somente na diagonal e nas posições imediatamente abaixo da diagonal)

Ex. 258 — Prove o Lema 10.6.

Ex. 259 — Prove o teorema 10.21.

Ex. 260 — Seja T um operador nilpotente. Prove que $(\mathcal{I} + T)$ não é singular.

Ex. 261 — Dê um exemplo de matriz real de ordem 4 que não é similar a nenhuma matriz real na forma de Jordan.

Ex. 262 — Descreva $\mathbf{x}(t)$ em função de $\mathbf{x}(0)$ (use a forma canônica de Jordan):

$$\begin{aligned} x_1'(t) &= 2x_1(t) + x_2(t) \\ x_2'(t) &= 2x_2(t) + x_3(t) \\ x_3'(t) &= 3x_3(t) + x_4(t) \\ x_4'(t) &= 3x_4(t) \end{aligned}$$

$$\begin{aligned} x_1'(t) &= 2x_1(t) + x_2(t) \\ x_2'(t) &= 2x_2(t) \\ x_3'(t) &= 3x_3(t) + x_4(t) \\ x_4'(t) &= 3x_4(t) \end{aligned}$$

$$\begin{aligned} x_1'(t) &= 4x_1(t) + x_2(t) + x_3(t) \\ x_2'(t) &= 4x_2(t) + x_3(t) \\ x_3'(t) &= 5x_3(t) + x_4(t) \\ x_4'(t) &= 2x_1(t) + 5x_4(t) \end{aligned}$$

Capítulo 11

Reticulados

Um reticulado é um subconjunto discreto de um espaço vetorial – em $\mathbb{R}^n$, por exemplo, um reticulado é um conjunto de pontos dispostos de maneira regular.

Definição 11.1 (Reticulado)**.** Um *reticulado* é o conjunto de todas as combinações lineares de um conjunto B de vetores LI, onde os coeficientes das combinações são inteiros. O conjunto B é chamado de *base* do reticulado.

Denotamos o reticulado com base B por $\mathcal{L}(B)$. ♦

Em outras palavras, um reticulado é um subconjunto de um espaço vetorial, onde os vetores sào combinações lineares inteiras da base.

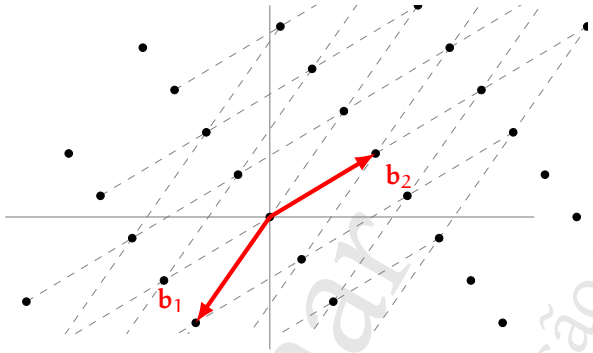
O conjunto de pontos com coordenadas inteiras em $\mathbb{R}^n$ é um exemplo extremamente simples de reticulado.

Exemplo 11.2. Os inteiros são um reticulado. Uma base para este reticulado é $+1$, e outra é -1. ◀

Exemplo 11.3. O conjunto $\{x : x = a\sqrt{2}\}$ com $a \in \mathbb{Z}$ é um reticulado em $\mathbb{R}$: sua base é $\sqrt{2}$, e o reticulado consiste de todas as combinações lineares (ou seja, os múltiplos) de $\sqrt{2}$. Este reticulado é mostrado na figura a seguir, com a base $\mathbf{b}_1 = \sqrt{2}$ destacada.

◀

Exemplo 11.4. A figura a seguir mostra um reticulado em $\mathbb{R}^2$.



◀

Exemplo 11.5. O conjunto de todas as matrizes de ordem n com entradas pares é um reticulado. Seja B a base canônica para o espaço vetorial $\mathcal{M}_n$. Multiplicamos todas as matrizes da base por 2, obtendo 2B, e $\mathcal{L}(2B)$ é o reticulado de matrizes pares. ◀

Exemplo 11.6. O conjunto de funções da forma

$$a\,\mathrm{sen}(x) + b\cos(x)$$

no intervalo $[-\pi, \pi]$, com $a, b \in \mathbb{Z}$ é um reticulado. ◀

Definição 11.7. Uma matriz quadrada A é unimodular se $|\det A| = 1$. ♦

Observe que se A é unimodular, $\det A^{-1} = \det A$.

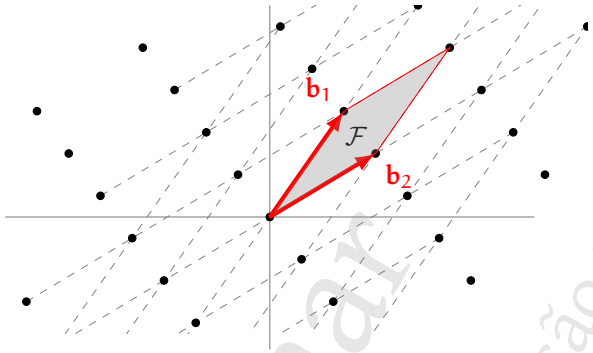
Teorema 11.8. *Sejam A e B duas bases para um reticulado. Então existe uma matriz unimodular U tal que $A = BU$.*

Demonstração. Denotamos $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ e $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Como A é base, então é possível escrever todos os $\mathbf{b}_i$ como combinação linear *inteira* das colunas de A – ou seja, existe uma matriz M com entradas inteiras tal que $AM = B$. Mas B também é base, e mesmo vale – existe uma matriz N tal que $BN = A$. Temos, portanto, que $AMN = A$, ou $MN = \mathcal{I}$. Assim, $\det(M)\det(N) = 1$. Mas $\det(M)$ e $\det(N)$ são inteiros (porque as duas matrizes são inteiras), por isso $\det(M) = \det(N) = \pm 1$. ■

Definição 11.9 (domínio fundamental)**.** Seja $L = \mathcal{L}(B)$ um reticulado. Então o *domínio fundamental* de L dado pela base B, que denotamos $\mathcal{F}(B)$, é o conjunto de combinações lineares de vetores da base B com coeficientes (não apenas inteiros) $0 \leq a_i < 1$.

$$\mathcal{F}(B) = \left\{\mathbf{x} : \mathbf{x} = \sum a_i \mathbf{b}_i,\ a_i \in [0, 1), \mathbf{b}_i \in B\right\}. \quad ♦$$

Exemplo 11.10. Em $\mathbb{R}^n$ o domínio fundamental é o paralelepípedo definido pelos vetores da base e seu volume é, por definição, o determinante da base. A figura a seguir mostra um reticulado em $\mathbb{R}^2$, com sua base, formada pelos vetores $\mathbf{b}_1$ e $\mathbf{b}_2$.



◀

Exemplo 11.11. Com a base $a\,\mathrm{sen}(x) + b\,\mathrm{sen}(x)$, e $x \in [-\pi, +\pi]$, temos um reticulado. Seu domínio fundamental é o conjunto

$$\{a\,\mathrm{sen}(x) + b\cos(x) : a, b \in [0, 1)\}$$

◀

Como diferentes bases para um mesmo reticulado podem ser obtidas pela multiplicação por uma matriz unimodular, concluímos que o determinante de todas as bases de um reticulado é o mesmo. Isso nos permite definir o determinante do reticulado.

Definição 11.12 (determinante de um reticulado)**.** O *determinante de um reticulado* em $\mathbb{R}^n$ é o módulo do determinante de qualquer uma de suas bases. ♦

Fica claro também que o volume do domínio fundamental de um reticulado não depende da base.

11.1 Ortogonalidade de bases

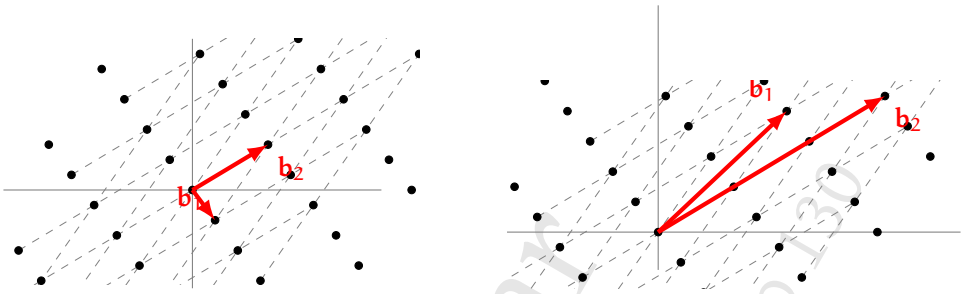
Definimos desvio de ortogonalidade apenas para bases de vetores de $\mathbb{R}^n$. É possível generalizar esta definição para espaços quaisquer, inclusive espaços de funções (desde que tenham bases), mas isto fica fora do escopo deste texto.

Definição 11.13 (desvio de ortogonalidade)**.** Seja $B = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ uma base para um reticulado, subconjunto de $\mathbb{R}^n$. O *desvio de ortogonalidade* da base B é

$$\delta(B) = \frac{\prod_i \|\mathbf{b}_i\|}{|\det B|}.$$

♦

Claramente, o desvio de ortogonalidade é 1 se a base é ortonormal, e maior que 1 caso contrário. A figura mostra, à esquerda, uma base com desvio de ortogonalidade baixo; à direita, outra base para o mesmo reticulado, com desvio maior.



Exemplo 11.14. Seja

$$B = \begin{pmatrix} 2 & 4 \\ 1 & 0 \end{pmatrix}$$

uma base. Seu desvio de ortogonalidade é

$$\frac{\|(2,1)^T\| \cdot \|(4,0)^T\|}{|\det B|} = \frac{4\sqrt{5}}{4} = \sqrt{5}.$$

Podemos obter outra pase para o mesmo reticulado aplicando uma transformação unimodular – por exemplo,

$$U = \begin{pmatrix} 8 & 3 \\ -5 & -2 \end{pmatrix}$$

A nova base é

$$AU = \begin{pmatrix} -4 & -2 \\ 8 & 3 \end{pmatrix}$$

A base AU tem desvio de ortogonalidade

$$\frac{\|(-4,8)^T\| \cdot \|(-2,3)^T\|}{|\det(AU)|} = \frac{4\sqrt{5}\sqrt{13}}{4} = \sqrt{5}\sqrt{13}.$$ ◀

11.2 Problemas em reticulados

Nesta seção definimos alguns problemas em reticulados e algoritmos para resolvê-los.

Definição 11.15 (problema do menor vetor (SVP))**.** Seja $\mathcal{L}$ um reticulado em um espaço com produto interno. Um *menor vetor* de $\mathcal{L}$ é um vetor não nulo em $\mathcal{L}$ com a menor norma dentre todos. ♦

Definição 11.16 (problema do vetor mais próximo (CVP))**.** Seja $\mathcal{L}$ um reticulado em um espaço V com produto interno. Dado $\mathbf{v} \in V$, o *vetor em $\mathcal{L}$ mais próximo de* $\mathbf{v}$ é o vetor $\mathbf{w} \in \mathcal{L}$ com a menor distância $d(\mathbf{v}, \mathbf{w})$. ♦

Definição 11.17 (problema da menor base (SBP))**.** Seja $\mathcal{L}$ um reticulado em um espaço com produto interno. Uma *menor base* para $\mathcal{L}$ é uma base que minimiza alguma norma que se defina para bases. ♦

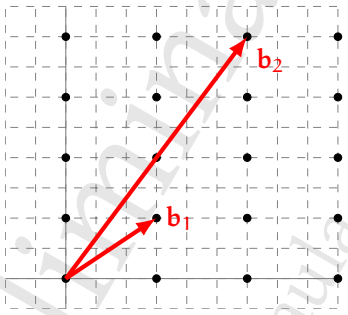
Quando o desvio de ortogonalidade e a dimensão do reticulado são grandes, estes problemas são difíceis.

11.2.1 Redução de bases com posto dois: algoritmo de Gauss-Lagrange

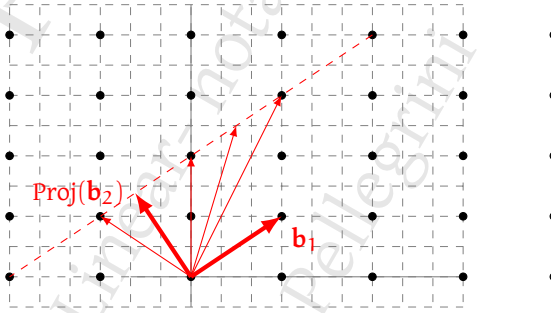
Para reticulados de dimensão dois há um algoritmo que permite encontrar eficientemente uma base de tamanho mínimo.

Em $\mathbb{R}^2$, dois vetores não nulos são LI (e consequentemente formam uma base) se e somente se não são multiplos um do outro. Assim, quaisquer dois vetores formando ângulo diferente de zero são LI.

Tomamos como exemplo $\mathbf{b}_1 = (3,2)^\mathsf{T}$ e $\mathbf{b}_2 = (6,8)^\mathsf{T}$, mostrados na figura a seguir.



Fixe $\mathbf{b}_1$. Podemos subtrair de $\mathbf{b}_2$ projeções de $\mathbf{b}_2$ em $\mathbf{b}_1$, obtendo outros vetores, e menor vetor que podemos obter desta forma será ortogonal a $\mathbf{b}_1$ (que conseguimos ao subtrair de $\mathbf{b}_2$ sua projeção ortogonal em $\mathbf{b}_1$).

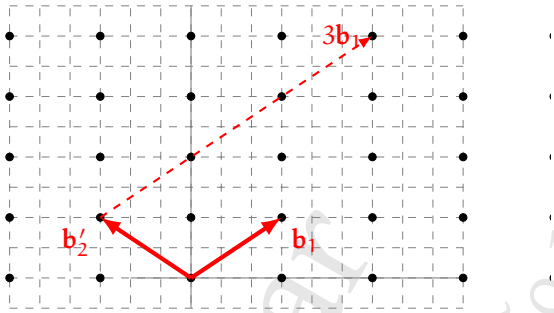


Infelizmente, a projeção ortogonal pode não ser um múltiplo inteiro de $\mathbf{b}_1$ (e o vetor ortogonal $\mathbf{b}_3$ portanto pode não pertencer ao reticulado). A intuição nos diz, no entanto, que podemos tomar o múltiplo mais próximo, arredondando o coeficiente.

Subtraindo de $\mathbf{b}_2$ sua projeção ortogonal em $\mathbf{b}_1$ temos $\frac{1}{13}(-24,36)^\mathsf{T}$, que não pertence ao reticulado. O múltiplo de $\mathbf{b}_1$ que subtraímos de $\mathbf{b}_2$ é

$$\frac{\langle \mathbf{b}_1, \mathbf{b}_2 \rangle}{\langle \mathbf{b}_1, \mathbf{b}_1 \rangle} = \frac{34}{13} \approx 2.615,$$

que não é inteiro. Arredondamos, e usando $k = 3$ calculamos $\mathbf{b}_2' = \mathbf{b}_2 - 3\mathbf{b}_1 = (-3,2)^\mathsf{T}$.



Conseguimos uma nova base, e reduzimos o maior vetor da base original. Podemos realizar outros passos para tentar obter bases ainda menores. Só teremos que, na próxima vez, trocar os vetores, para que subtraiamos do maior vetor um múltiplo do menor vetor.

Claramente, não é possível continuar reduzindo o tamanho dos vetores indefinidamente, e em algum momento deveremos parar.

Definimos que a base já está reduzida (e que portanto podemos parar o processo de redução) se um passo de subtração não resultar em uma base menor. Pararemos quando $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2'\| \leq \|\mathbf{b}_2\|$.

Definição 11.18 (base reduzida de reticulado, no sentido de Gauss-Lagrange)**.** Seja L um reticulado em $\mathbb{R}^2$. Uma base $B = (\mathbf{b}_1, \mathbf{b}_2)$ para L é *reduzida no sentido de Gauss-Lagrange* se

$$\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \|\mathbf{b}_2 + k\mathbf{b}_1\|,$$

para todo $k \in \mathbb{Z}$. ♦

Com o passo de redução de base e o critério de parada, já podemos descrever o algoritmo de Gauss-Lagrange.

Método 11.19 (algoritmo de Gauss-Lagrange)**.** Tem-se uma base $(\mathbf{b}_1, \mathbf{b}_2)^T$ para um reticulado em $\mathbb{R}^2$.

- Se $\|\mathbf{b}_2\| < \|\mathbf{b}_1\|$ troque $\|\mathbf{b}_1\|$ com $\|\mathbf{b}_2\|$
- Seja
$$k = \left\lfloor \frac{\langle \mathbf{b}_1, \mathbf{b}_2 \rangle}{\|\mathbf{b}_1\|^2} \right\rceil$$
- Se $k = 0$ pare; a base já está reduzida.
- Subtraia $k\mathbf{b}_1$ de $\mathbf{b}_2$.
- Recomece.

Ao término do algoritmo, $\mathbf{b}_1$ e $\mathbf{b}_2$ estão entre os menores vetores do reticulado. ●

Se $k = 0$ então a multiplicidade estava em $[-0.5, +0.5]$ antes de arredondar. Isso significa que teríamos que subtrair uma parte muito pequena da projeção ortogonal, e que portanto $\mathbf{b}_1$ já está próximo de ortogonal a $\mathbf{b}_2$. Não nos adianta subtrair múltiplo inteiro de $\mathbf{v}_1$. E como $\mathbf{v}_1$ é menor que $\mathbf{v}_2$, não adianta também trocar os vetores.

Exemplo 11.20. Seja $(3,15)^T$, $(9,25)^T$ uma base. Usamos o método de Gauss-Lagrange para reduzí-la.

$$\begin{aligned}\|\mathbf{b}_1\| &= \|(3,15)^T\| \approx 15.3\\ \|\mathbf{b}_2\| &= \|(9,25)^T\| \approx 26.6\end{aligned}$$

Escolhemos

$$k = \left\lfloor \frac{\langle (3,15)^T, (9,25)^T \rangle}{\|(3,15)^T\|^2} \right\rceil = \left\lfloor \frac{402}{234} \right\rceil = 2$$

Calculamos portanto

$$(9,25)^T - 2(3,15)^T = (3,-5)^T$$

e temos uma base menor:

$$\begin{aligned}\|\mathbf{b}_1\| &= \|(3,15)^T\| \approx 15.3\\ \|\mathbf{b}_2\| &= \|(3,-5)^T\| \approx 5.8\end{aligned}$$

Trocamos os vetores,

$$\begin{aligned}\|\mathbf{b}_1\| &= \|(3,-5)^T\| \approx 5.8\\ \|\mathbf{b}_2\| &= \|(3,15)^T\| \approx 15.3\end{aligned}$$

e começamos novamente

$$k = \left\lfloor \frac{\langle (3,-5)^T, (3,15)^T \rangle}{\|(3,-5)^T\|^2} \right\rceil = \left\lfloor -\frac{66}{34} \right\rceil = -2$$

Subtraímos

$$(3,15)^T + 2(3,-5)^T = (9,5)^T.$$

Agora temos

$$\begin{aligned}\|\mathbf{b}_1\| &= \|(3,-5)^T\| \approx 5.8\\ \|\mathbf{b}_2\| &= \|(9,5)^T\| \approx 10.2\end{aligned}$$

Como $\|\mathbf{b}_1\| < \|\mathbf{b}_2\|$, desta vez não precisamos trocar os vetores. Novamente calculamos k:

$$k = \left\lfloor \frac{\langle (3,-5)^T, (9,5)^T \rangle}{\|(3,-5)^T\|^2} \right\rceil = \left\lfloor \frac{2}{34} \right\rceil = 0.$$

Temos agora uma base formada pelos dois menores vetores do reticulado. ◀

O algoritmo de Gauss-Lagrange não pode ser generalizado para espaços de dimensão maior sem tornar-se muito ineficiente.

11.2.2 Vetor mais próximo com posto e ortogonalidade altos: algoritmo de Babai

Apresentamos nesta seção o algoritmo de Babai. A partir de uma base B e um ponto qualquer $\mathbf{x} \in \mathbb{R}^n$, o algoritmo de Babai encontra um ponto $\mathbf{y}$ pertencente a $\mathcal{L}(B)$. Se B tiver desvio baixo de ortogonalidade, o ponto $\mathbf{y}$ será próximo do vetor mais próximo de $\mathbf{x}$.

Se $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ é uma base para um reticulado de posto n, então B tem posto n, e portanto é também base para $\mathbb{R}^n$. Assim, podemos descrever qualquer ponto de $\mathbb{R}^n$ como combinação linear da base B:

$$\mathbf{x} = (x_1\mathbf{b}_1, \ldots, x_n\mathbf{b}_n)^T.$$

Usaremos isto na descrição do algoritmo de Babai.

Método 11.21 (algoritmo de Babai)**.** Seja $\mathcal{L}$ um reticulado com base $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Seja $(x_1\mathbf{b}_1, \ldots, x_n\mathbf{b}_n)^T$, com $x_i \in \mathbb{R}$ um ponto qualquer em $\mathbb{R}^n$ (note que este ponto não necessariamente pertence ao reticulado, já que os x_i podem não ser inteiros). O algoritmo de Babai simplesmente arredonda os coeficientes,

$$a_i = \lfloor x_i \rceil,$$

e retorna o ponto do reticulado

$$(a_1\mathbf{b}_1, \ldots, a_n\mathbf{b}_n).$$

Tendo um ponto qualquer $\mathbf{p}$ em $\mathbb{R}^n$, portanto, obtemos os coeficientes

$$\mathbf{x} = B^{-1}\mathbf{p},$$

e o ponto mais próximo será

$$B\lfloor \mathbf{x} \rceil. \qquad \bullet$$

Exemplo 11.22. Damos um exemplo em $\mathbb{R}^2$, para que possamos ilustrar também com um gráfico. Seja

$$B = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}$$

uma base, e $\mathbf{x} = (5, 2)^T$ um ponto fora de $\mathcal{L}(B)$. Então

$$B^{-1}\mathbf{x} = \begin{pmatrix} \frac{1}{3} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 5 \\ 2 \end{pmatrix} = \begin{pmatrix} \frac{5}{3} \\ 1 \end{pmatrix}$$

Arredondamos, obtendo $(2, 1)^T$. O ponto mais próximo é

$$B(2, 1)^T = (6, 2)^T. \qquad \blacktriangleleft$$

11.2.3 Posto alto, ortogonalidade baixa (reticulados difíceis)

Para bases pouco ortogonais e com posto algo há outros algoritmos, mas nenhum deles dá a solução exata e executa em pouco tempo. Um algoritmo muito conhecido para este problema é conhecido por "LLL" (que são as iniciais dos autores do algoritmo – Lenstra, Lenstra e Lovasz), que é uma variação do método de ortogonalização de Gram-Schmidt. O leitor interessado por encontrar mais informações nos livros de Steven Galbraith [Gal12] e de Hoffstein, Pipher e Silverman [HPS08].

11.3 Aplicações

11.3.1 Criptografia [reticulados; desvio de ortogonalidade]

O criptossistema GGH foi proposto em 1997 por Goldreich, Goldwasser e Halewi [GGH97]. Este criptossistema foi "quebrado" – o que significa que não pode ser usado na prática porque não é seguro. Apesar disso, é um excelente exemplo de como problemas em reticulados são usados em Criptografia.

Neste criptossistema, cada participante tem um reticulado $\mathcal{L}$. Sua chave privada é uma base "boa" (com desvio de ortogonalidade muito baixo), e a chave privada é uma base "ruim" (com desvio alto). Cada ponto do reticulado é uma mensagem que pode ser enviada.

De posse da base pública, qualquer um pode encriptar uma mensagem: seja $m \in \mathcal{L}$ a mensagem. Para encriptar, basta deslocar ligeiramente a mensagem, resultando num ponto em $\mathbb{R}^n$, fora do reticulado, mas perto de m. para obter a mensagem original, deve-se resolver o problema do vetor mais próximo. Como a base que todos conhecem (a chave pública) tem desvio de ortogonalidade muito grande, o esperado era que ninguém conseguisse resolver o problema e decifrar a mensagem. Já a base privada tem desvio de ortogonalidade baixo, por isso com ela é fácil obter m a partir da mensagem encriptada. A seguir, detalhamos parcialmente o funcionamento do criptossistema.

Primeiro, uma base B ortogonal (ou quase ortogonal) é criada. A base "ruim" R (com desvio de ortogonalidade grande) é criada a partir de B. Uma das maneiras de obter R é criar uma sequencia U_1, U_2, ..., U_k de matrizes unimodulares geradas aleatoriamente: basta gerar matrizes triangulares superiores (ou inferiores) com a diagonal igual a 1 e números inteiros aleatórios nas outras entradas. Assim,

$$R = BU_1U_2 \cdots U_k.$$

Como as matrizes U_i são unimodulares, R é base para o mesmo reticulado gerado por B. Mas como as U_i tem entradas aleatórias acima (ou abaixo) da diagonal, R terá um desvio de ortogonalidade grande.

Para encriptar uma mensagem $\mathbf{m} \in \mathcal{L}$, criamos um *vetor de erro* $\mathbf{e} = (e_1, e_2, \dots, e_n)$, e somamos à mensagem. A mensagem encriptada será

$$\mathbf{c} = \mathbf{m}R + \mathbf{e},$$

ou seja, o erro é somado aos coeficientes do ponto m na base R. O erro deve ser pequeno, de forma que $\mathbf{c}$ continue mais próximo de $\mathbf{m}$ do que de qualquer outro ponto do reticulado.

Para decifrar, usa-se o algoritmo de Babai que determina o ponto mais próximo de $\mathbf{c}$ no reticulado, usando a base B. Com isso obtemos mR. Para obter os coeficientes, basta multipicar por R^{-1}.

Exemplo 11.23. Damos agora um exemplo minimalita do funcionamento do GGH.

Primeiro escolhemos uma base privada (com desvio pequeno).

$$B = \begin{pmatrix} 120 & 992 & 544 \\ 20 & -2273 & 4141 \\ 30 & -3 & -2 \end{pmatrix}$$

Escolhemos uma matriz unimodular U:

$$\begin{pmatrix} 1 & -10500 & 350 \\ 1520 & -15959999 & 537000 \\ 25000 & -262530001 & -141254999 \end{pmatrix}$$

A base R é

$$\begin{pmatrix} 15107960 & -158649899552 & -76309973456 \\ 100070060 & -1050859866414 & -586157544859 \\ -54530 & 572624999 & 280909498 \end{pmatrix}$$

Os desvios de ortogonalidade de B e R são

$$\begin{aligned} \delta(B) &\approx 8 \\ \delta(R) &\approx 3.9 \times 10^{23}. \end{aligned}$$

Escolhemos uma mensagem,

$$\mathbf{m} = (2, 4, 6)^T.$$

Um vetor de erro

$$\mathbf{e} = (10, -5, 8)^T.$$

O texto cifrado é

$$\mathbf{c} = R\mathbf{m} + \mathbf{e} = \begin{pmatrix} -1092429223014 \\ -7720184594695 \\ 3975847932 \end{pmatrix}$$

Para decifrar, obtemos as coordenadas de $\mathbf{c}$ na base B e arredondamos

$$\mathbf{x} = \lfloor B^{-1}\mathbf{c} \rceil = \begin{pmatrix} 39897 \\ 60614956 \\ 1897599998 \end{pmatrix}.$$

Reescrevemos na base B

$$B\mathbf{x} = \begin{pmatrix} -1092429223024 \\ -7720184594690 \\ 3975847924 \end{pmatrix}$$

e obtemos as coordenadas na base R

$$R^{-1}(B\mathbf{x}) = (2, 4, 6)^T.$$

A base B é fundamental para decriptar. Se usássemos somente a base R teríamos as coordenadas

$$\mathbf{x}' = \lfloor R^{-1}\mathbf{c} \rceil = \begin{pmatrix} 633239422721646 \\ 60308114400 \\ -12061617 \end{pmatrix}.$$

Este ponto na base B é

$$R\mathbf{x}' = \begin{pmatrix} -1155699408288 \\ -8136001665837 \\ 4203990954 \end{pmatrix}. \qquad \blacktriangleleft$$

O criptossistema GGH infelizmente não é seguro: o criptanalista Phong Nguyen mostrou que existe uma maneira de decifrar as mensagens sem usar a chave privada.

Os livros de Hoffstein, Pipher e Silverman [HPS08], de Galbraith [Gal12] e o de Goldwasser e Micciancio [MG12] permitem compreender em maior profundidade reticulados e sua aplicação em Criptografia.

11.3.2 Cristalografia [reticulados]

(Esta seção está incompleta)

Cristais são sólidos cujos átomos se organizam espacialmente como os pontos de um reticulado.

O livro de Nevill Szwacki e Teresa Szwacka [SS10] e o de Schwarzenbach [Sch96] tratam de reticulados em cristais.

Exercícios

Ex. 263 — Quantas bases pode ter um reticulado em $\mathbb{R}$? E em $\mathbb{R}^2$ e $\mathbb{R}^n$, de maneira geral?

Ex. 264 — Para todo n, o espaço vetorial $\mathbb{R}^n$ não é reticulado, porque claramente admitimos combinações lineares não inteiras da base. Há espaços vetoriais que também são reticulados?

★ **Ex. 265 —** Seja $(V, +, \cdot)$ um espaço vetorial. Prove que um subgrupo aditivo $(S, +)$ é discreto (não é contínuo) se e somente se os elementos de S são os elementos de um reticulado.

★ **Ex. 266 —** (Daniele Micciancio) Encontre um conjunto de vetores B tal que $\mathcal{L}(B)$ não seja um reticulado.

★ **Ex. 267 —** Os n primeiros termos de uma série de Fourier são um reticulado. Mostre como calcular o volume de seu domínio fundamental. Tente dar uma interpretação a ele.

Ex. 268 — Encontre uma base Gauss-Lagrange-reduzida para o reticulado com base $(3, 28)^T$, $(4, 11)^T$.

Ex. 269 — No exemplo 11.14, demos duas bases para um reticulado em $\mathbb{R}^2$, uma delas com desvio de ortogonalidade $\sqrt{5}$. Prove que esta base é a menor no sentido de Gauss-Lagrange, ou mostre uma que seja menor que esta.

Capítulo 12

Formas Quadráticas e Bilineares

No Capítulo 5 definimos formas multilineares, e construímos o determinante como forma multilinear. Agora voltamos a atenção a um caso especial: as formas bilineares, funções de dois argumentos, e lineares em cada um deles.

12.1 Formas Bilineares

Uma possível definição para formas bilineares seria a seguinte.

Definição 12.1 (Forma bilinear)**.** Uma forma bilinear é uma forma multilinear com dois argumentos. ♦

Damos também uma definição mais explícita, que é mais comum em textos introdutórios de Álgebra Linear.

Definição 12.2 (Forma bilinear)**.** Uma função $f : U \times V \to \mathbb{R}$ é *bilinear* se

- Dado $\mathbf{u} \in U$, $f(\mathbf{u}, \cdot)$ é linear em seu segundo argumento.
- Dado $\mathbf{v} \in V$, $f(\cdot, \mathbf{v})$ é linear em seu primeiro argumento. ♦

Teorema 12.3. *Toda forma bilinear $f(\mathbf{x}, \mathbf{y})$ sobre $\mathbb{R}$, $\mathbb{Q}$ ou $\mathbb{C}$, sem termos lineares, pode ser representada por uma matriz B, de forma que*

$$f(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T B \mathbf{y}$$

Demonstração. (Esta demonstração é um tanto informal)
Uma forma bilinear deve necessariamente ser como

$$a_{11}x_1y_1 + a_{12}x_1y_2 + \cdots,$$

sem que haja termos quadráticos (x_i^2) nem constantes.
Expandimos $\mathbf{x}^T B\mathbf{y}$, obtendo

$$(x_1, \ldots, x_n)B \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

$$
\begin{aligned}
&= (x_1 b_{11} + x_2 b_{21} + \cdots + x_n b_{n1} + \cdots + x_n b_{1n} + x_2 b_{2n} + \cdots + x_n b_{nn}) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \\
&= \left(\left[\sum_i b_{i1} x_i \right] + \cdots + \left[\sum_i b_{in} x_i \right] \right) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \\
&= y_1 \left(\sum_i b_{i1} x_i \right) + \cdots + y_n \left(\sum_i b_{in} x_i \right) \\
&= \sum_j \sum_i b_{ij} x_i y_j,
\end{aligned}
$$

e portanto temos todas as combinações de x_i com y_j com diferentes coeficientes. O coeficiente de $x_i y_j$ será o elemento b_{ij}. ■

Exemplo 12.4. A forma bilinear

$$f(\mathbf{x}, \mathbf{y}) = 2x_1 y_1 - 3x_1 y_2 + x_2 y_1 - 5x_2 y_2$$

é representada pela matriz

$$\begin{pmatrix} 2 & -3 \\ 1 & -5 \end{pmatrix},$$

porque

$$(x_1, x_2) \begin{pmatrix} 2 & -3 \\ 1 & -5 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 2x_1 y_1 - 3x_1 y_2 + x_2 y_1 - 5x_2 y_2. \quad ◀$$

Definição 12.5 (forma bilinear simétrica)**.** Uma forma bilinear $f(x, y)$ é *simétrica* se $f(x, y) = f(y, x)$. ♦

O Exercício 271 pede a demonstração da proposição 12.6.

Proposição 12.6. *Toda forma bilinear simétrica é representável por uma matriz simétrica.*

Corolário 12.7. *Toda matriz que representa forma bilinear simétrica é diagonalizável.*

12.1.1 Com termos lineares

Sejam $\mathbf{x}$ e $\mathbf{y}$ vetores com n componentes. Defina

$$B = \left(\begin{array}{ccc:c} q_{11} & q_{12} & \cdots & q_{1n} & p_1 \\ q_{21} & q_{22} & & & p_2 \\ \vdots & & \ddots & & \vdots \\ q_{n1} & & & q_{nn} & p_n \\ \hdashline s_1 & s_2 & \cdots & s_n & c \end{array} \right), \quad \mathbf{x}' = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \\ 1 \end{pmatrix}, \quad \mathbf{y}' = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \\ 1 \end{pmatrix}.$$

Note que marcamos uma submatriz quadrada de ordem tres. Essa submatriz representa a forma bilinear, quando ignoramos os termos lineares (e estes, por sua vez, são representados na linha e coluna adicional). Então

$$(\mathbf{x}')^T B \mathbf{y}' = \sum_{i,j} q_{ij} x_i y_j + \sum_i r_i x_i + \sum_i s_i y_i + c$$

Exemplo 12.8. A forma bilinear

$$2x_1y_1 - 3x_1y_3 + x_2y_3 - 9x_3y_2 - x_1 + 4x_2 - 5x_3 + y_2 + 2$$

é representada pela matriz

$$A = \left(\begin{array}{ccc:c} 2 & 0 & -3 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & -9 & 0 & 0 \\ \hdashline -1 & 4 & -5 & 2 \end{array}\right)$$

de forma que, se

$$\mathbf{x}' = \begin{pmatrix} x_1 & x_2 & x_3 & 1 \end{pmatrix}, \quad \mathbf{y}' = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ 1 \end{pmatrix},$$

então

$$\begin{aligned}(\mathbf{x}')^{\mathsf{T}} A \mathbf{y} &= \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ 1 \end{pmatrix} \left(\begin{array}{ccc:c} 2 & 0 & -3 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & -9 & 0 & 0 \\ \hdashline -1 & 4 & -5 & 2 \end{array}\right) \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ 1 \end{pmatrix} \\ &= 2x_1y_1 - 3x_1y_3 + x_2y_3 - 9x_3y_2 - x_1 + 4x_2 - 5x_3 + y_2 + 2. \end{aligned}$$ ◀

12.2 Formas Quadráticas

Definição 12.9 (forma quadrática)**.** Uma *forma quadrática* em x é uma forma bilinear $f(x, x)$. ♦

Toda forma quadrática real, racional ou complexa, portanto, pode ser descrita como $\mathbf{x}^{\mathsf{T}} Q \mathbf{x}$, onde Q é uma matriz. É claro também que toda forma quadrática é bilinear simétrica.

★ **Exemplo 12.10.** Não é verdade que formas quadráticas em qualquer corpo podem ser representadas por matrizes simétricas. Por exemplo, em $\mathbb{Z}_2$, a forma

$$x_1x_1 \oplus x_1x_2$$

não pode ser representada por matriz simétrica. Ela pode, no entanto, ser representada pela matriz triangular

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}.$$ ◀

Definição 12.11 (matrizes definidas e semidefinidas)**.** Uma matriz A com autovalores $\lambda_1, \ldots, \lambda_n$ é

i) *definida positiva* se $\lambda_i > 0$,

ii) *definida negativa* se $\lambda_i < 0$,

iii) *semidefinida positiva* se $\lambda_i \geq 0$,

iv) *semidefinida negativa* se $\lambda_i \leq 0$,

v) *indefinida* se tem autovalores positivos e negativos. ♦

Exemplo 12.12. Considere as matrizes

$$A = \begin{pmatrix} -2 & 3 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 5 \\ 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & -4 \\ 0 & -1 \end{pmatrix}.$$

A tem autovalores -2 e 1, portanto é indefinida. B tem autovalores 1 e 2, portanto é definida (e semidefinida) positiva. C tem autovalores 0 e -1, portanto é semidefinida negativa. ◀

O teoerma 12.13 explicita propriedades importantes de matrizes definidas e semidefinidas. Sua demonstração é pedida no exercício 272.

Teorema 12.13. *Uma matriz A é*

i) definida positiva *se* $\mathbf{x}^T A\mathbf{x} > 0, \forall \mathbf{x} \neq 0$;

ii) definida negativa *se* $\mathbf{x}^T A\mathbf{y} < 0, \forall \mathbf{x} \neq 0$;

iii) semidefinida positiva *se* $\mathbf{x}^T A\mathbf{x} \geq 0, \forall \mathbf{x}$;

iv) semidefinida negativa *se* $\mathbf{x}^T A\mathbf{y} \leq 0, \forall \mathbf{x}$;

v) indefinida *se* $\mathbf{x}^T A\mathbf{x}$ *pode ser positivo ou negativo.*

Disto podemos concluir que

Corolário 12.14. *O determinante de uma matriz (semi)-definida positiva é positivo, e o determinante de uma matriz (semi)-definida negativa é negativo.*

Corolário 12.15. *Matrizes definidas (positivas ou negativas) não são singulares.*

Exemplo 12.16. A matriz

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

é definida positiva, porque para qualquer vetor $\mathbf{x} = (x_1, x_2)^T \neq \mathbf{0}$,

$$\begin{aligned} \langle \mathbf{x}, A\mathbf{x} \rangle &= \mathbf{x}^T A\mathbf{x} \\ &= 3x_1^2 + 3x_2^2 + 2x_1x_2 \\ &= 2x_1^2 + 2x_2^2 + (x_1^2 + 2x_1x_2 + x_2^2) \\ &= 2x_1^2 + 2x_2^2 + (x_1 + x_2)^2, \end{aligned}$$

que é a soma de três quadrados, que sempre será positiva. ◀

Exemplo 12.17. Uma matriz com elementos não-negativos não necessariamente é semidefinida positiva. A matriz

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$

não é semidefinida positiva: seja $\mathbf{x} = (1, -5)^T$. Então,

$$\begin{aligned} \langle \mathbf{x}, A\mathbf{X} \rangle &= \mathbf{x}^T (A\mathbf{x}) \\ &= (1, -5) \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -5 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \\ &= (1, -5)(-3, 1)^T = -8. \end{aligned}$$ ◀

Exemplo 12.18. Uma matriz definida positiva não necessariamente tem todos os elementos positivos. Por exemplo,

$$A = \begin{pmatrix} 5 & -1 \\ -1 & 5 \end{pmatrix}$$

é positiva, porque para $\mathbf{x} > \mathbf{0}$, temos

$$\begin{aligned} \mathbf{x}^T A\mathbf{x} &= 5x_1^2 + 5x_2^2 - 2x_1x_2 \\ &= 4x_1^2 + 4x_2^2 + \left(x1^2 - 2x_1x_2 + x_2^2\right) \\ &= 4x_1^2 + 4x_2^2 + \left(x1 + x_2\right)^2 \\ &> 0. \end{aligned}$$

◀

O Exercício 273 pede a demonstração do Teorema 12.19.

Teorema 12.19. *Se A e B são definidas positivas e $k \in \mathbb{R}^+$, então também são definidas positivas $A + B$ e kA.*

Na demonstração do Teorema 12.20 usamos o fato de uma matriz ser semidefinida positiva para determinar uma desigualdade a respeito do determinante de matrizes com valores positivos. O Exercício 274 pede a demonstração do mesmo resultado para o valor absoluto do determinante.

Teorema 12.20. *Seja A um operador descrito por uma matriz com valores estritamente positivos. Então*

$$\det A \leq \prod_i a_{ii}.$$

Demonstração. Tomamos a representação de A como matriz. Suas entradas diagonais são maiores que zero, portanto podemos definir

$$d_i = \frac{1}{\sqrt{a_{ii}}},$$

ou seja, d_i é o inverso da raiz do i-ésimo elemento da diagonal de A.

Seja D a matriz contendo somente entradas diagonais d_i. Então

$$B = DAD$$

é simétrica e semidefinida positiva. Além disso, a diagonal de B somente contém uns.

Usando as propriedades de determinantes, temos

$$\begin{aligned} \det B &= \det A \det(DD) \\ \det B &= \det A \left(\frac{1}{\prod \sqrt{a_{ii}}}\right)^2 \\ \det B &= \frac{\det A}{\prod a_{ii}} \\ \prod a_{ii} \det B &= \det A, \end{aligned}$$

e só precisamos mostrar portanto que $\det B \leq 1$.

Sejam $b_1, \ldots, b_n$ os autovalores de B, *que são todos não negativos*, porque B é semidefinida positiva. A média aritmética destes valores não é maior que a geométrica, ou seja,

$$\sqrt[n]{\prod b_i} \leq \frac{\sum b_i}{n}$$
$$\prod b_i \leq \left(\frac{\sum b_i}{n}\right)^n$$
$$\det B \leq \left(\frac{\operatorname{Tr} B}{n}\right)^n$$

Como a diagonal de B só contem uns, $\operatorname{Tr} B = n$, e temos

$$\det B \leq 1. \qquad \blacksquare$$

Exemplo 12.21. A matriz

$$A = \begin{pmatrix} 5 & 1 \\ 1 & 5 \end{pmatrix}$$

é positiva. O produtório de sua diagonal é 25, e seu determinante é -24. ◀

Exemplo 12.22. A matriz

$$A = \begin{pmatrix} 3 & 2 & 5 \\ 1 & 2 & 4 \\ 1 & 1 & 4 \end{pmatrix}$$

só tem valores positivos. O produtório de sua diagonal é 24, e seu determinante é 7. ◀

12.3 Formas multilineares

Da mesma maneira que definimos e pudemos representar formas bilineares como matrizes, também é possível dar um tratamento semelhante a formas multilineares. Estas, no entanto, são mais naturalmente representáveis como *tensores*, que são semelhantes a matrizes, mas onde usamos mais de dois índices, como "a_{ijklmn}", por exemplo. Tensores ficam fora do escopo deste texto.

12.4 Aplicações

12.4.1 Classificação de cônicas e quádricas

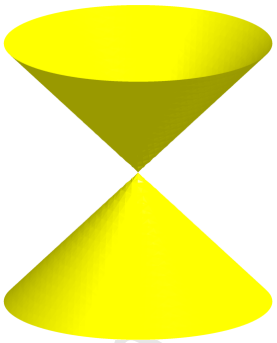
Cônicas, e quádricas e suas matrizes

Tomamos as cônicas e quádricas e examinamos as matrizes que as definem.

Uma *cônica*[1] é a interseção de um cone circular com um plano em $\mathbb{R}^3$.

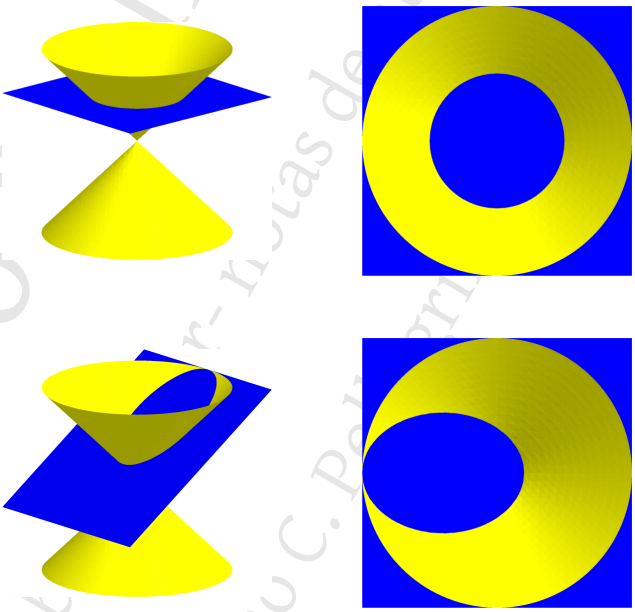
O cone circular é obtido pela revolução de uma reta não coincidente com o eixo das ordenadas, como ilustra a próxima figura.

[1] Ou *seção cônica*.



Examinaremos a seguir as cônicas e quádricas, de um ponto de vista geométrico. Na seçãoseguinte trataremos de sua classificação de acordo com propriedades de duas formas quadráticas.

- *elipse ou circunferência:* obtida com um plano, *não* paralelo à geratriz do cone, e que o intercepta somente em uma de suas metades. Nas figuras a seguir, os planos que interceptam o cone são dados por $z = 3/2$ (definindo uma circunferência) e $x + 3z/2 = 3/2$ (definindo uma elipse).



A equação da elipse é

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = k,$$

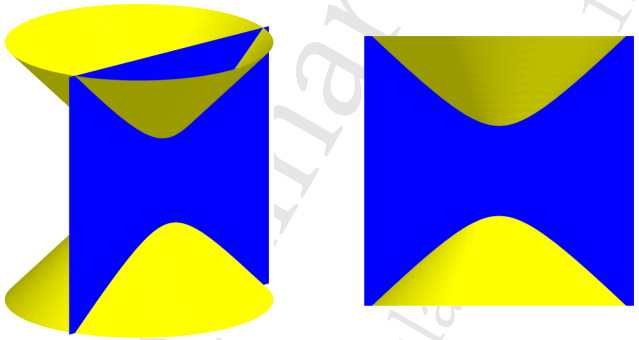
e a matriz que dá sua forma quadrática é

$$\begin{pmatrix} \frac{1}{a^2} & 0 \\ 0 & \frac{1}{b^2} \end{pmatrix}.$$

- *hipérbole:* obtida com um plano que intercepta o cone em suas duas metades

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = k$$

Na figura a seguir, o plano que intercepta o cone é dado por $y = 1$.

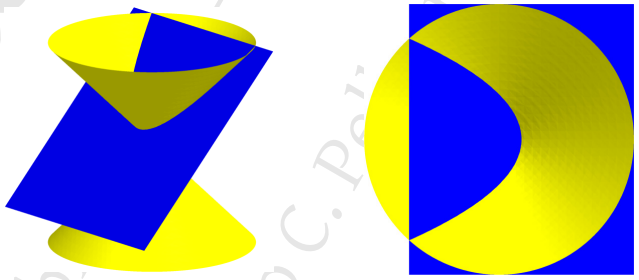


$$\begin{pmatrix} \frac{1}{a^2} & 0 \\ 0 & -\frac{1}{b^2} \end{pmatrix}$$

- *parábola:* quando o plano é paralelo à geratriz do cone.

$$ax^2 - y = k.$$

Na figura a seguir, o plano que intercepta o cone é dado por $2x + 2z = 2$ (portanto paralelo a ele).



A parábola, no entanto, não pode ser descrita somente como forma quadrática – ela tem um componente linear. Descrevemos a parábola como $\mathbf{x}^T A\mathbf{x} + \mathbf{b}y$, onde

$$A = \begin{pmatrix} \frac{1}{a^2} & 0 \\ 0 & 0 \end{pmatrix}, \quad \mathbf{b} = (0, 1)^T.$$

O fato de não conseguirmos representar a parábola sem componentes lineares relaciona-se com um importante fato: a parábola não tem um *centro*, ao redor do qual seja completamente simétrica (as outras

cônicas podem ser divididas em quatro partes que podem ser obtidas umas das outras por reflexões em dois eixos ortogonais). Trataremos disso mais adiante, já que também é verdade para parabolóides em qualquer dimensão.

Procedemos agora às quádricas, definidas em $\mathbb{R}^3$. Representaremos as formas quadráticas como matrizes de ordem *quatro*, mas identificando também a submatriz de ordem *três* que se obtém desconsiderando os termos lineares.

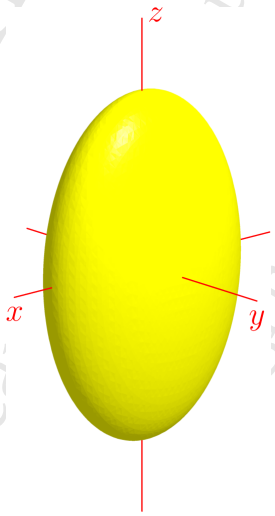
- *elipsóide*

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}+\frac{z^2}{c^2}=k,$$

com todos os termos positivos, e cuja matriz é

$$\left(\begin{array}{ccc:c} \frac{1}{a^2} & 0 & 0 & 0 \\ 0 & \frac{1}{b^2} & 0 & 0 \\ 0 & 0 & \frac{1}{c^2} & 0 \\ \hdashline 0 & 0 & 0 & -k \end{array}\right)$$

A figura a seguir mostra um elipsóide com $a=2, b=1, c=3$ e $k=2$.



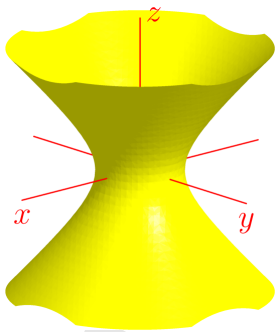
- *hiperbolóide de uma folha*

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}-\frac{z^2}{c^2}=k,$$

com dois termos positivos. Mostramos aqui somente o caso em que z é negativo, mas pode-se reordenar as variáveis. A matriz é

$$\left(\begin{array}{ccc:c} \frac{1}{a^2} & 0 & 0 & 0 \\ 0 & \frac{1}{b^2} & 0 & 0 \\ 0 & 0 & -\frac{1}{c^2} & 0 \\ \hdashline 0 & 0 & 0 & -k \end{array}\right)$$

A figura a seguir mostra um hiperbolóide de uma folha com $a=b=c=2$ e $k=1/2$.



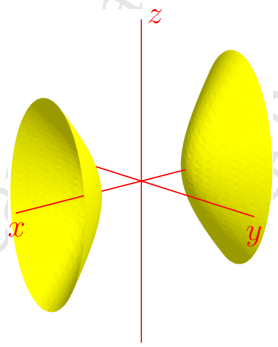
- *hiperbolóide de duas folhas*

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} - \frac{z^2}{c^2} = k,$$

com dois termos negativos, e cuja matriz é

$$\left(\begin{array}{ccc:c} \frac{1}{a^2} & 0 & 0 & 0 \\ 0 & -\frac{1}{b^2} & 0 & 0 \\ 0 & 0 & -\frac{1}{c^2} & 0 \\ \hdashline 0 & 0 & 0 & -k \end{array}\right)$$

A figura a seguir mostra um hiperbolóide de duas folhas com $a = c = 2$, $b = 1$ e $k = 1/2$.



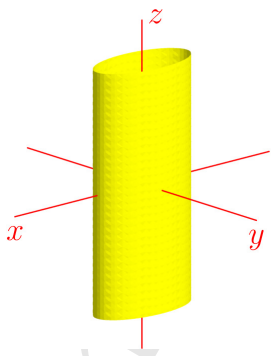
- *cilindro elíptico*

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = k,$$

com somente dois termos positivos e o terceiro igual a zero. A matriz desta forma é

$$\left(\begin{array}{ccc:c} \frac{1}{a^2} & 0 & 0 & 0 \\ 0 & \frac{1}{b^2} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & -k \end{array}\right)$$

A figura a seguir mostra um cilindro elíptico com $a = 2$,$b = 1$ e $k = 1/2$.



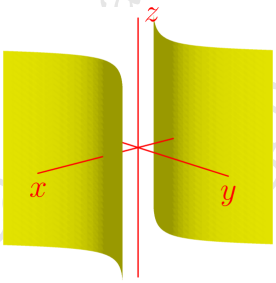
- *cilindro hiperbólico*

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = k,$$

com um termo positivo e um negativo. A matriz é

$$\left(\begin{array}{cccc} \frac{1}{a^2} & 0 & 0 & 0 \\ 0 & -\frac{1}{b^2} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -k \end{array}\right)$$

A figura a seguir mostra um cilindro hiperbólico com $a = b = 2$ e $k = 1/2$.



Assim como não podemos descrever parábolas sem adicionar à equação quadrática um termo linear, o mesmo acontece com todos os paraboloides.

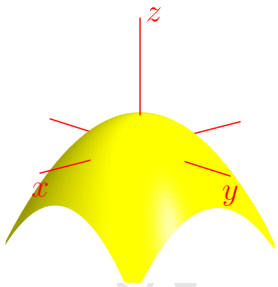
- *parabolóide elíptico*

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} - cz = k$$

Em forma matricial, temos

$$\left(\begin{array}{cccc} \frac{1}{a^2} & 0 & 0 & 0 \\ 0 & \frac{1}{b^2} & 0 & 0 \\ 0 & 0 & 0 & c \\ 0 & 0 & 0 & -k \end{array}\right).$$

A figura a seguir mostra um parabolóide elíptico com $a = b = 2$ e $c = k = 1$.



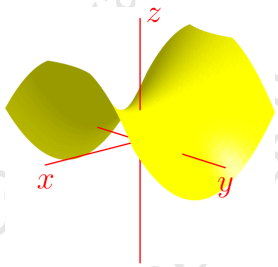
- *parabolóide hiperbólico*, que é simétrico ao redor de um ponto de sela, e é definido pela equação

$$-\frac{x^2}{a^2}+\frac{y^2}{b^2}+cz=k$$

A matriz que o representa é

$$\left(\begin{array}{ccc:c} -\frac{1}{a^2} & 0 & 0 & 0 \\ 0 & \frac{1}{b^2} & 0 & 0 \\ 0 & 0 & 0 & c \\ \hdashline 0 & 0 & 0 & -k \end{array}\right).$$

A figura a seguir mostra um parabolóide hiperbólico com $a=b=2$ e $c=k=1$.



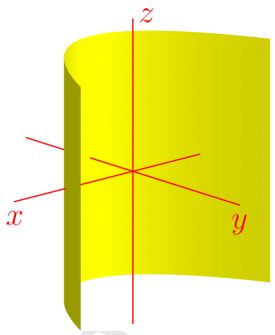
- *cilindro parabólico*, definido pela equação

$$ax^2-cy=k$$

A matriz que representa um cilindro parabólico é

$$\left(\begin{array}{ccc:c} \frac{1}{a^2} & 0 & 0 & 0 \\ 0 & 0 & 0 & c \\ 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & -k \end{array}\right).$$

A figura a seguir mostra um cilindro parabólico com $a=2$ e $c=1$ e $k=2$.



Uma superfície tem um *centro* se pode ser obtida pela reflexão de um de seus octantes em $\mathbb{R}^3$ (ou ortantes em $\mathbb{R}^n$).

Definição 12.23 (centro de superfície)**.** Seja uma superfície qualquer em $\mathbb{R}^n$. Se existe um ponto $\mathbf{x}$ tal que, para quaisquer $\delta_1, \ldots, \delta_n$ e qualquer índice i, se

$$(x_1 + \delta_1, x_2 + \delta_2, \ldots, \underbrace{x_i + \delta_i}, \ldots, x_n + \delta_n)$$

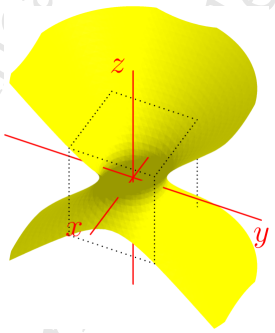
pertence à superfície, então

$$(x_1 + \delta_1, x_2 + \delta_2, \ldots, \underbrace{x_i - \delta_i}, \ldots, x_n + \delta_n)$$

também pertence (ou seja, podemos trocar o sinal de qualquer δ_i), então $\mathbf{x}$ é o *centro* da superfície. ♦

Elipsóides, hiperbolóides e seus respectivos cilindros são superfícies com centro – ou seja, estas superfícies são compostas de partes simétricas ao redor da origem.

Exemplo 12.24. Ilustramos na figura a seguir um hiperbolóide de uma folha, com $a = b = c = 2$, e $k = 1/2$:



Apenas alguns dos pontos simétricos são mostrados.

Como a figura não está transladada, seu centro é $(0, 0, 0)^T$. Assim, queremos que

$$\frac{(0+\delta_1)^2}{2^2} + \frac{(0+\delta_2)^2}{2^2} - \frac{(0+\delta_3)^2}{2^2} - 1/2 = 0$$

implique em

$$\frac{(0 \pm \delta_1)^2}{2^2} + \frac{(0 \pm \delta_2)^2}{2^2} - \frac{(0 \pm \delta_3)^2}{2^2} - 1/2 = 0$$

mas isto sempre é verdade, porque teremos $\delta_i^2 = (-\delta_i)^2$. ◀

O mesmo não acontece com os parabolóides – estes não tem centro, por causa da presença do termo linear, que se comporta de maneira diferente para argumentos positivos e negativos.

Determinando o tipo de uma forma quadrática

Dada uma forma quadrática qualquer, definida por uma matriz A, queremos saber que tipo de forma ela representa, geometricamente. Podemos fazê-lo facilmente por inspeção, se houver apenas termos da forma $a_k x_i^2$, mas não tanto quando há termos da forma $a_k x_i x_j$.

Exemplo 12.25. Como já vimos na seção 12.4.1, a equação $\frac{x^2}{2} + \frac{y^2}{3} + \frac{z^2}{2} = 1$ define um elipsóide, e a equação $\frac{x^2}{2} - \frac{y^2}{3} - \frac{z^2}{2} = 2$ define um hiperbolóide de duas folhas.

No entanto, não é imediatamente fácil determinar que tipo de figura é definida pelas equações $xy + z^2 = 1$ e $xy - yz + z^2 = 2$, por causa da presença dos termos xz na primeira equação e dos termos xy e yz na segunda. ◀

Uma observação importante que podemos fazer é que as quádricas que vimos serem fáceis de classificar são representadas por matrizes diagonais, e *sua classificação depende da quantidade de autovalores positivos, negativos e iguais a zero*.

Assim, para classificar uma forma quadrática não diagonal, deveremos obter seus autovalores. Podemos fazer ainda mais – sabemos que uma forma Q qualquer é similar a uma matriz diagonal D: $Q = P^{-1}DP$. Se obtivermos P, podemos descrever a quádrica em questão através de uma simples mudança de base.

Definimos então a *inércia* de uma matriz, que nos informará diretamente o tipo de uma quádrica qualquer, dada sua matriz.

Definição 12.26 (inércia de uma matriz)**.** A *inércia* de uma matriz M é a tripla $\text{In}(M) = (p, n, z)$, onde p, n, z são as quantidades de autovalores positivos, negativos e zero da matriz. ♦

A inércia das duas matrizes que identificamos nas formas quadráticas determinam o tipo de forma geométrica que elas definem. Da descrição das cônicas e quádricas e suas matrizes, imediatamente percebemos que a classificação é como se dá nas tabelas a seguir.

Para as cônicas, temos uma única matriz de ordem 2, e sua inércia determina completamente a forma geométrica.

(p, n, z)	classificação
$(2, 0, 0), (0, 2, 0)$	elipse
$(1, 1, 0)$	hipérbole
$(1, 0, 1), (0, 1, 1)$	parábola

Para as quádricas, denotamos por $(p, n)_4$ os autovalores positivos da matriz de ordem 4, e por $(p, n)_3$ os

da submatriz de ordem 3.

$(p,n)_4$	$(p,n)_3$	classificação
$(4,0)$	$(3,0)$	elipsóide
$(2,2)$	$(2,1)$	hiperbolóide (1 folha)
$(3,1)$	$(2,1)$	hiperbolóide (2 folhas)
$(3,1)$	$(2,0)$	parabolóide elíptico
$(2,2)$	$(1,1)$	parabolóide hiperbólico
$(2,1)$	$(2,0)$	cilindro elíptico
$(2,1)$	$(1,0)$	cilindro parabólico
$(2,1)$	$(1,1)$	cilindro hiperbólico

Separamos, na tabela, as quádricas com centro; em seguida, as sem centro (o posto da matriz maior é completo, mas o da menor, não); e em seguida, os cilindros (ambas as matrizes são singulares).

Exemplo 12.27. Os exemplos que demos anteriormente de cônicas e quádricas ilustram a classificação (demos a descrição de cada uma delas como matriz diagonal, de onde pode-se trivialmente extrair os autovalores). ◀

Claramente, dada uma elipse ou elipsóide, podemos determinar uma região limitada de $\mathbb{R}^2$ (ou $\mathbb{R}^3$) que o contenha. O mesmo vale para qualquer forma quadrática semidefinida positiva, conforme o teorema 12.28, cuja demonstração é pedida no exercício 275.

Teorema 12.28. *Uma matriz é semidefinida positiva se e somente se a figura definida por sua forma quadrática em $\mathbb{R}^n$ pode ser contida em uma região limitada.*

Eixos principais

Como formas quadráticas são representadas por matrizes diagonais, podemos sempre diagonalizá-las. O processo de diagonalização é simplesmente uma mudança de base, e isso significa que podemos tomar uma equação quadrática qualquer, descrevê-la como matriz, e diagonalizá-la para obter uma equação na forma reduzida.

Em toda forma quadrática podemos identificar eixos principais ortogonais. Quando a forma quadrática está na forma reduzida, os eixos principais serão colineares com a base canônica. Em outros casos, precisamos realizar uma mudança de base para encontrar os eixos principais. Usando esta nova base, a forma quadrática pode ser descrita na forma reduzida.

No resto desta seção trataremos tres casos diferentes:

- A forma quadrática pode ter termos mistos, mas não tem componente linear (por exemplo, $2x^2 - xy + \frac{y^2}{5}$). Neste caso conseguiremos transformá-la na forma reduzida $\sum_i a_i x_i^2 = c$.
- Há uma componente linear, mas ela podem ser eliminada por uma translação (por exemplo, $x^2 - x$), e também a levaremos à forma reduzida.
- Há uma componente linear, e a forma não pode ser descrita sem ela – neste caso temos uma parábola ou parabolóide (por exemplo, $2x^2 - y - 2$).

O teorema que nos garante que podemos eliminar os termos mistos encontrando os eixos principais é o *Teorema dos Eixos Principais* Podemos enunciá-lo de maneira bastante concisa, como a seguir.

Teorema 12.29. *(dos eixos principais) Toda matriz simétrica real tem autovalores reais e uma base formada por autovetores ortonormais.*

No entanto, será mais interessante enunciá-lo listando também suas consequências.

Teorema 12.30. *(dos eixos principais) Seja A a matriz simétrica representando uma forma quadrática. Existe uma base na qual a mesma forma quadrática é descrita por uma matriz diagonal D, e a matriz P que realiza esta mudança de base é ortogonal.*

A mudança de variáveis que permite escrever a forma quadrática na forma reduzida é dada por $P^{-1}\mathbf{x}$, ou, uma vez que P é ortogonal, $P^T\mathbf{x}$. Após a mudança de base, a forma será descrita por

$$\lambda_1 x_1^2 + \lambda_2 x_2^2 + \cdots + \lambda_n x_n^2$$

onde os λ_i são os autovalores de A.

Exemplo 12.31. Considere a equação quadrática

$$4xy = 1$$

A matriz associada a esta equação é

$$Q = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$$

Diagonalizamos a matriz, obtendo $Q = PDP^{-1}$, *com os vetores de P ortonormais*:

$$D = \begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix}, \quad P = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

Observando os autovalores já sabemos que se trata de uma hipérbole. A matriz $P^{-1} = P^T$ muda da nova base onde D descreve a hipérbole para a base original, portanto

$$\begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} x' + y' \\ -x' + y' \end{pmatrix},$$

e a mudança de base pode ser descrita pela troca de variáveis

$$x = \frac{x' + y'}{\sqrt{2}}$$
$$y = \frac{-x' + y'}{\sqrt{2}}.$$

Substituímos x e y na equação original, e obtemos

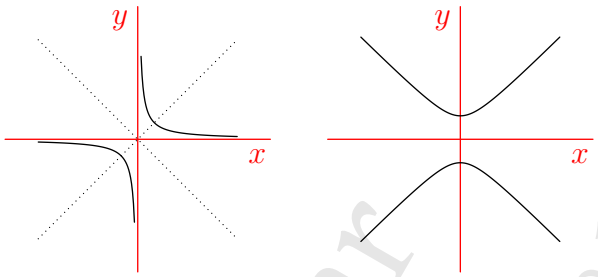
$$-2(x')^2 + 2(y')^2 = 1,$$

e observamos que obtivemos os autovalores de A como coeficientes, exatamente como nos garante o teorema dos eixos principais.

Se observarmos a matriz de vetores ortonormais $\frac{1}{\sqrt{2}}P$, notaremos que

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \cos(\frac{\pi}{4}) & -\operatorname{sen}(\frac{\pi}{4}) \\ \operatorname{sen}(\frac{\pi}{4}) & \cos(\frac{\pi}{4}) \end{pmatrix},$$

e a mudança de base de uma hipérbole para outra é uma rotação por um ângulo $\pi/4$, como mostram os gráficos das duas funções, a seguir.



A primeira mostra $4xy = 1$, e a segunda, $2y^2 - 2x^2 = 1$. As linhas pontilhadas na prineira figura são os eixos principais, determinados pelos autovetores da matriz A. ◀

A forma quadrática do exemplo anterior não tinha componentes lineares. Quando tivermos a componente linear,

i) Se a matriz A tiver inversa, então podemos calcular a constante $\frac{1}{2}A^{-1}\mathbf{b}$ e realizamos a translação

$$\mathbf{z} = \mathbf{x} + \frac{1}{2}A^{-1}\mathbf{b}$$

A forma quadrática passa a ser escrita então como

$$\mathbf{z}^T A\mathbf{z} = c + \frac{1}{4}\mathbf{b}^T A^{-1}\mathbf{b},$$

e uma vez que o lado direito é uma constante, podemos classificá-la e escrever sua equação como se não houvesse a parte linear.

ii) Se a matriz A for singular, a forma é um parabolóide, e podemos apenas eliminar os termos mistos, mas os termos lineares permanecerão.

faltam nesta subseção mais exemplos!

Uma discussão em maior profundidade das superfícies definidas por formas quadráticas pode ser encontrada no livro de Georgi Shilov [Shi77].

12.4.2 Classificação de equações diferenciais parciais [formas definidas, eixos principais]

Uma equação diferencial parcial de segunda ordem com coeficientes constantes pode ser descrita[2][3] por uma matriz A, um vetor $\mathbf{b}$ e uma constante p:

$$\sum_{i,j} a_{ij} u_{x_i x_j} + \sum_i b_i u_{x_i} + pu = 0$$

[2] Ou, mudando a notação,

$$\sum_{i,j} a_{ij} \frac{\partial^2 u}{\partial x_i \partial x_j} + \sum_i b_i \frac{\partial u}{\partial x_i} + pu = 0.$$

[3] Ou ainda, pode-se usar uma única matriz de ordem $n+1$ (da mesma forma que fizemos na seção 12.4.1). Nesta seção, no entanto, os termos lineares realmente não nos importam, portanto a representação por matriz de ordem n é mais interessante.

Exemplo 12.32. Se u é uma função de *três* variáveis, então a equação

$$3u_{xx} + 2u_{yy} - u_{yz} - u_y = 0$$

é descrita por

$$A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & -1/2 \\ 0 & -1/2 & 0 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}. \qquad \blacktriangleleft$$

Exemplo 12.33. A equação

$$\frac{\partial^2 u}{\partial x^2} + 2\frac{\partial^2 u}{\partial x \partial z} + \frac{\partial^2 u}{\partial y \partial z} + 3\frac{\partial u}{\partial z} = 0$$

é descrita por

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & -1/2 \\ 1 & -1/2 & 0 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}. \qquad \blacktriangleleft$$

Desta forma, classificamos as equações diferenciais parciais como:

- **elíptica** se A é positiva definida;
- **hiperbólica** se A é indefinida, tendo um autovalor com sinal diferente dos outros;
- **ultrahiperbólica** se A é indefinida, com ao menos dois autovalores positivos e dois negativos;
- **parabólica** se A tem um autovalor zero.

As características de cada um dos tipos de equações são completamente diferentes – elas representam fenômenos de diferentes naturezas, e os métodos de análise e solução para cada tipo são também totalmente diversos.

Exemplo 12.34. O exemplo mais simples de equação parabólica é a equação do calor,

$$\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial u}{\partial t} = 0,$$

com $A = \operatorname{diag}(1, 1, 0)$ e uma derivada de ordem um. Equações parabólicas surgem tipicamente na descrição de fenômenos de propagação (como o calor em material sólido, por exemplo). Estas equações também são chamadas de *equações de difusão*.

O exemplo mais simples de equação elíptica é com $A = \mathcal{I}$, $\mathbf{b} = \mathbf{0}$, e $z = 0$ – a equação de Laplace:

$$\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial^2 u}{\partial z^2} = 0$$

É comum que a equação de Laplace (e das equações elípticas em geral) surja na modelagem de sistemas em equilíbrio. Por exemplo, um sistema onde a entrada e a saída de energia são em mesma quantidade, a dimensão do tempo pode ser desprezada, e temos então a equação do calor, sendo removido o último termo.

O exemplo mais simples de equação hiperbólica é com $A = \text{diag}(1, 1, \ldots, 1, -1)$ – a equação da onda:

$$\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} - \frac{\partial^2 u}{\partial t^2} = 0.$$

Equações hiperbólicas lineares descrevem fenômenos ondulatórios (uma corda vibrando ou a superfície de tambor, por exemplo). ◀

A seguir temos o teorema dos eixos principais, aplicado às EDPs de segunda ordem.

Teorema 12.35. *Toda equação diferencial parcial de segunda ordem com coeficientes constantes envolvendo uma função de n variáveis pode ser reduzida, por uma transformação linear, a uma das seguintes formas:*

- **elíptica:** $\sum_i u_{x_i x_i} + \ldots = 0$
- **hiperbólica:** $\sum_{i=1}^{n-1} u_{x_i x_i} - u_{x_n x_n} + \ldots = 0$
- **ultrahiperbólica:** $\left(\sum_{i=1}^{k} u_{x_i x_i}\right) - \left(\sum_{i=k+1}^{n} u_{x_i x_i}\right) + \ldots = 0$
- **parabólica:** $\sum_{i=1}^{k} u_{x_i x_i} + \ldots = 0$, *com* $k < n$.

onde os termos denotados por "..." são de ordem um ou zero.

Os métodos usados para resolver cada tipo de EDP também são determinados pelo tipo da equação. Uma descrição destes métodos fica fora do escopo deste texto, mas o leitor pode consultar o livro de Walter Strauss [Str08] e, para uma abordagem mais intuitiva e menos formal, o de Stanley Farlow [Far82], além da bibliografia mencionada no Apêndice δ.

12.4.3 Máximos e mínimos de funções em $\mathbb{R}^n$ [formas definidas]

Uma combinação convexa de vetores (ou pontos) é semelhante a uma combinação linear, exceto que os coeficientes refletem uma escolha de frações de cada vetor, com a soma das frações igual à unidade. Por exemplo, 0.2 do vetor $\mathbf{v}_1$, 0.7 do vetor $\mathbf{v}_2$ e 0.1 do vetor $\mathbf{v}_3$.

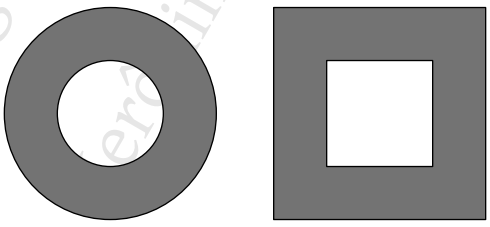
Definição 12.36 (combinação convexa)**.** Uma *combinação convexa* é uma combinação linear onde os coeficientes são positivos e somam 1. ⧫

Exemplo 12.37. A combinação $0.2x_1 + 0.5x_2 + 0.3x_3$ é convexa, porque os coeficientes são todos positivos, e $0.2 + 0.5 + 0.3 = 1$. ◀

Definição 12.38 (conjunto convexo)**.** Seja $A \subseteq \mathbb{R}^n$. Se, para todos $x, y \in A$, todas as combinações convexas de x e y pertencerem a A, então A é um conjunto *convexo.* ⧫

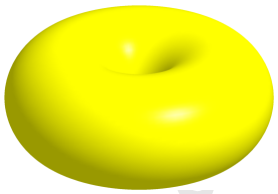
Exemplo 12.39. Em $\mathbb{R}^2$, os interiores de uma circunferência, elipse ou poliedro são conjuntos convexos.

Já os conjuntos de pontos mostrados na figura a seguir não são convexos.



◀

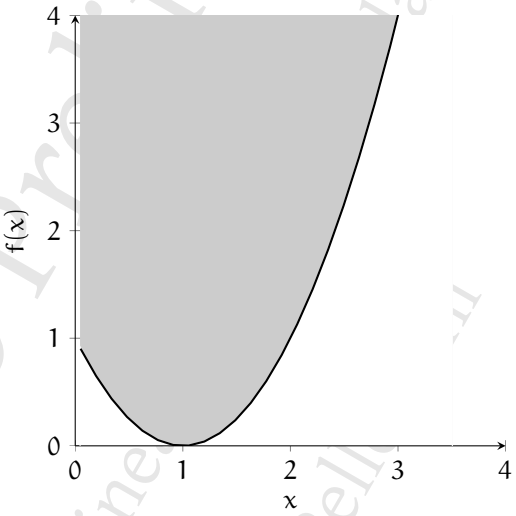
Exemplo 12.40. O conjunto de pontos no interior de um cubo ou elipsóide em $\mathbb{R}^3$ é convexo.
Já os pontos dentro de um toro, por exemplo, não formam um conjunto convexo.



◀

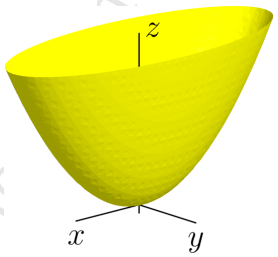
Definição 12.41 (epigrafo)**.** O *epigrafo* de uma função $f : \mathbb{R}^n \to \mathbb{R}$ é o conjunto de pontos acima de seu gráfico: $\operatorname{epi} f = \{(x, y) : x \in \mathbb{R}^n, y \in \mathbb{R}, y \geq f(x)\}$. ♦

Exemplo 12.42. A figura a seguir mostra o epigrafo da função $f(x) = x^2 - 2x + 1$.



◀

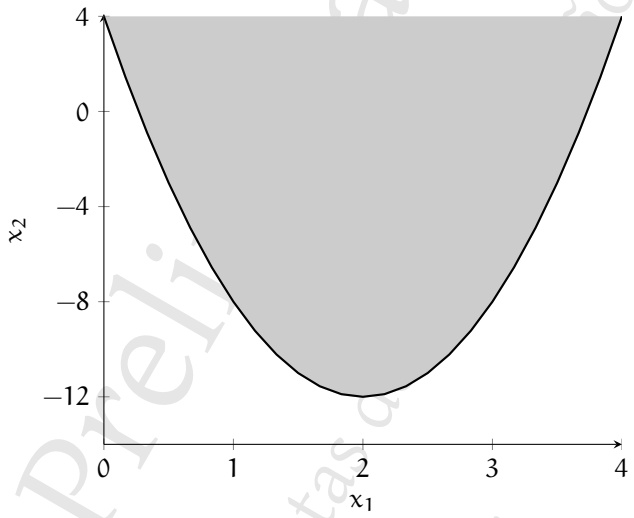
Exemplo 12.43. A figura a sguir mostra a função $f(x, y) = \frac{x^2}{2} + 3y^2$. Seu epigrafo é toda a região acima da superfície mostrada.



◀

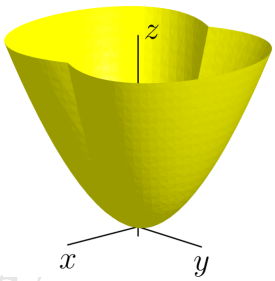
Definição 12.44 (função convexa)**.** Uma função é convexa se seu epigrafo é convexo. ♦

Exemplo 12.45. Seja $f(x) = ax^2 + bx + c$ uma função quadrática. Se $a > 0$, então f é convexa. Se $a < 0$, $-f$ é convexa. Por exemplo, a função $4x^2 - 16x - 4$, mostrada na figura, é convexa.

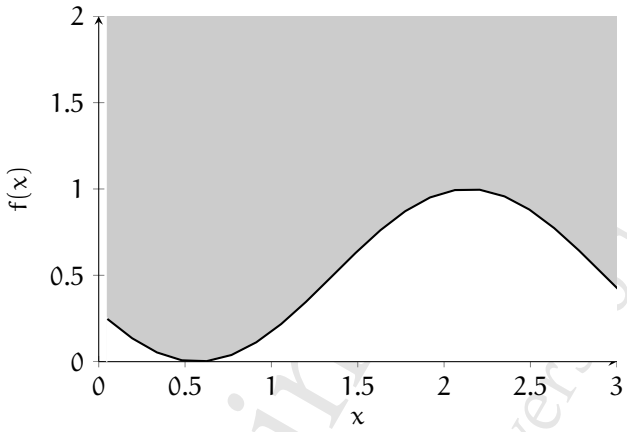


◀

Exemplo 12.46. A figura a sguir mostra a função não convexa $f(x, y) = \frac{2x^2}{|y|+1} + y^2$. É fácil perceber que seu epigrafo não é convexo.



Já a figura a seguir mostra a função $f(x) = \cos(x + 1)^2$, que também não é convexa.



◀

Definição 12.47 (ponto crítico)**.** Seja $f : \mathbb{R}^n \to \mathbb{R}$. Um *ponto crítico* de f é um ponto $\mathbf{x} \in \mathbb{R}^n$ tal que todas as derivadas parciais de f em $\mathbf{x}$, se existirem, são iguais a zero. ♦

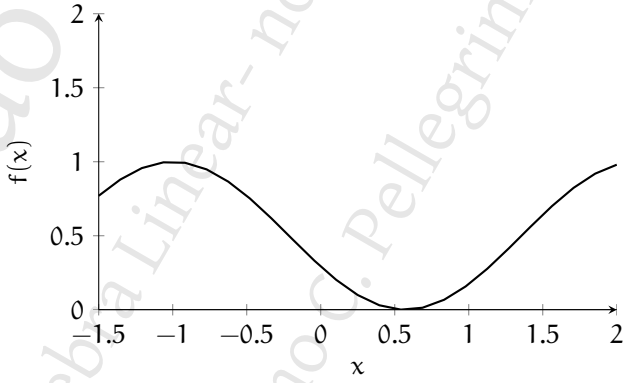
Exemplo 12.48. Considere a função $f(x) = \cos(x+1)^2$. O ponto $x = -1$ é um ponto crítico para f, já que

$$\frac{d}{dx} f(x) = -2\cos(x+1)\,\mathrm{sen}(x+1),$$

e portanto

$$\frac{d}{dx} f(-1) = 0.$$

O mesmo acontece com $x = (\pi - 2)/2 = 0.570796\ldots$. A figura a seguir mostra os dois pontos críticos.



◀

Exemplo 12.49. Um parabolóide elíptico tem um único ponto crítico, no topo ou fundo. ◀

Definição 12.50 (matriz Hessiana)**.** Seja $f : \mathbb{R}^n \to \mathbb{R}$ duas vezes diferenciável. A matriz Hessiana de f em x, denotada por $H_f(x)$ ou $\nabla^2 f(x)$ é a forma bilinear

$$\nabla^2(\mathbf{x})_{i,j} = \frac{\partial^2 f(\mathbf{x})}{\partial x_i \partial x_j},$$

ou

$$\nabla^2 f(\mathbf{x}) = \begin{pmatrix} \frac{\partial^2 f}{\partial^2 x_1}(\mathbf{x}) & \frac{\partial^2 f}{\partial x_1 \partial x_2}(\mathbf{x}) & \dots & \frac{\partial^2 f}{\partial x_1 \partial x_n}(\mathbf{x}) \\ \frac{\partial^2 f}{\partial x_2 \partial x_1}(\mathbf{x}) & \frac{\partial^2 f}{\partial^2 x_2}(\mathbf{x}) & \dots & \frac{\partial^2 f}{\partial x_2 \partial x_n}(\mathbf{x}) \\ \vdots & \vdots & \ddots & \\ \frac{\partial^2 f}{\partial x_n \partial x_1}(\mathbf{x}) & \frac{\partial^2 f}{\partial x_n \partial x_2}(\mathbf{x}) & \dots & \frac{\partial^2 f}{\partial^2 x_n}(\mathbf{x}) \end{pmatrix}. \quad \blacklozenge$$

Exemplo 12.51. Seja $f : \mathbb{R}^3 \to \mathbb{R}^3$, tal que

$$f(x, y, z) = xy + z^2.$$

A Hessiana de f é

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}. \quad \blacktriangleleft$$

Exemplo 12.52. Seja $g : \mathbb{R}^3 \to \mathbb{R}^3$, tal que

$$g(x, y, z) = xy^3z^2 + \cos(z).$$

A Hessiana de g é

$$\begin{pmatrix} 0 & 3y^2 & 0 \\ 3y^2 & 6xy & 0 \\ 0 & 0 & 2 - \cos(z) \end{pmatrix}.$$

Este exemplo mostra que a Hessiana é, na verdade, função de x, y e z. $\blacktriangleleft$

Teorema 12.53. *Uma função $f : \mathbb{R}^n \to \mathbb{R}$ duas vezes diferenciável é convexa se e somente se sua Hessiana é semidefinida positiva.*

Corolário 12.54. *Uma função $f : \mathbb{R}^n \to \mathbb{R}$ duas vezes diferenciável é convexa se e somente se o lugar geométrico (conjunto de pontos) definidos pela sua Hessiana pode ser contido em uma região limitada de $\mathbb{R}^n$.*

Teorema 12.55. *Seja $\mathbf{x}$ um ponto crítico de uma função $f : \mathbb{R}^n \to \mathbb{R}$, e H a Hessiana de f. Se H é semidefinida positiva, $\mathbf{x}$ é máximo local. Se H é semidefinida negativa, $\mathbf{x}$ é mínimo local. Se H é indefinida, então $\mathbf{x}$ é ponto de sela.*

Corolário 12.56. *Seja $f : \mathbb{R}^n \to \mathbb{R}$ e $\mathbf{x}$ um ponto crítico de f. Se a Hessiana de f é semidefinida positiva* para todo ponto, *então $\mathbf{x}$ é máximo global de f.*

12.4.4 Otimização quadrática

Problemas de otimização pedem que seja encontrado um ponto no qual uma dada função qualquer tem valor ótimo (máximo ou mínimo), respeitando certas restrições.

Um programa quadrático é um problema de otimização onde o objetivo é maximizar ou minimizar uma função quadrática, respeitando restrições descritas como desigualdades lineares.

Definição 12.57. Um *programa quadrático* é definido como

$$\min z(\lambda, \mathbf{x}) = \lambda \mathbf{c}^T \mathbf{x} + \frac{1}{2} \mathbf{x}^T Q \mathbf{x}.$$

$$\begin{aligned} \text{s.a. : } A\mathbf{x} &\leq \mathbf{b} \\ \mathbf{x} &\geq 0 \end{aligned}$$

onde λ é um parâmetro escalar; $\mathbf{c}$ e $\mathbf{x}$ são vetores com n elementos; e Q é uma matriz semidefinida positiva $n \times n$; A uma matriz $m \times n$; e $\mathbf{b}$ é um vetor com m elementos. ♦

Q define uma forma quadrática; se não for semidefinida positiva, a função não será convexa.

Exemplo 12.58. Um investidor quer montar uma carteira de ativos. Para cada par de ativos i e j, ele conhece as médias μ_i a variância σ_{ii} e a covariância σ_{ij}. Ele quer construir uma carteira que lhe dê um rendimento médio mínimo r, minimizando o risco.

A função a ser minimizada (o risco) é $\sum_i \sum_j \sigma_{ij} x_i x_j$, uma função quadrática. E as restrições são:

- Cada x_i representa uma fração do valor total investido, e a soma das frações deve ser um: $\sum_i x_i = 1$.
- O rendimento médio deve ser $\geq r$, ou seja, $\sum_i \mu_i x_i \geq r$

$$\begin{aligned} \min & \sum_i \sum_j \sigma_{ij} x_i x_j \\ \text{s.a.:} & \sum_i x_i = 1 \\ & \sum_i \mu_i x_i \geq r \\ & \mathbf{x} \geq \mathbf{0} \end{aligned}$$

◀

Não tratamos aqui dos algoritmos para solução de programas quadráticos. Exposições detalhadas de programação linear e não-linear, incluindo programação quadrática, são dadas nos livros de Luenberger [LY10] e de Nocedal [NW06].

Exercícios

Ex. 270 — Determine as matrizes das formas bilineares:

$$\begin{aligned} f(x, y) &= xy - 2x + 3y \\ g(x, x) &= 3x^2 + x \end{aligned}$$

Ex. 271 — Prove a proposição 12.6.

Ex. 272 — Prove o teorema 12.13.

Ex. 273 — Prove o teorema 12.19.

Ex. 274 — O Teorema 12.20 nos garante que para qualquer matriz quadrada A com valores positivos, temos $\det A \leq \prod a_{ii}$. Prove que o mesmo vale para o valor absoluto do determinante – ou seja,

$$|\det A| \leq \prod a_{ii}.$$

Ex. 275 — Prove o teorema 12.28.

★ **Ex. 276 —** Sejam A e B dois operadores definidos positivos em $\mathbb{R}^n$. Defina a relação $A < B$ se e somente se $(B - A)$ é positivo. Mostre que:

i) $<$ é transitiva.

ii) Se $A < B$ e $X < Y$, então $A + B < X + Y$.

iii) Se X é invertível e $A < B$, então $XAX^{-1} < XBX^{-1}$.

Ex. 277 — Mostre a representação matricial da função quadrática usada no exemplo 12.58.

Ex. 278 — Descreva geometricamente as formas quadráticas com $\text{In}(A) = (1, 0, 1)$ e $\text{In}(B) = (1, 0, 2)$.

Ex. 279 — Na seção 12.4.1 exibimos a classificação das cônicas e quádricas com equações $\mathbf{x}^T A\mathbf{x} + \mathbf{b} = k$, com $k > 0$. Descerva geometricamente os casos degenerados, onde $k = 0$. Para as cônicas, explique como esses casos degenerados são obtidos pela interseção de plano e cone.

Ex. 280 — Classifique as seguintes funções quadráticas:

i) $x^2 - xy + zy - \frac{z^2}{3} = 5$

ii) $x^2 + xy = 1$

iii) $xz + z^2 - x^2 = 3$

iv) $xy - xz + zy - x^2 + \frac{z^2}{2} = 1$

Ex. 281 — Mostre que nenhuma função polinomial com grau ímpar maior ou igual a 3 e em uma variável é convexa em $\mathbb{R}$.

Ex. 282 — Seja $f(a, b) = e^a + \log(b)$ é convexa em todo $\mathbb{R}^2$? E $g(a, b) = e^a - \log(b)$?

Ex. 283 — $f(a, b) = \log(a)b$ é convexa?

Ex. 284 — Onde $f(\mathbf{x}) = x_1^2/x_2$ é convexa?

★ **Ex. 285 —** Seja $\mathbb{R}[x]$ o conjunto de todos os polinômios em x com coeficientes reais. Seja S o subconjunto de $\mathbb{R}[x]$ que são positivos no intervalo $[0, 1]$. Mostre que S é convexo.

★ **Ex. 286 —** Escreva a forma quadrática em $\mathbb{Z}_2^3$ representada pela matriz a seguir.

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

★ **Ex. 287 —** Quantas formas quadráticas distintas existem em $\mathbb{Z}_2^n$?

Capítulo 13

Geometrias: Afim e Projetiva

Uma das maneiras de descrever a Álgebra Linear é como o estudo da geometria de várias dimensões. Até este ponto, tratamos da Geometria Euclidiana, mas há geometrias diferentes, que surgem quando não usamos os cinco postulados de Euclides[1]:

I um segmento de reta é determinado por dois pontos;

II qualquer segmento pode ser extendido em duas direções, dando origem a uma reta;

III um círculo pode ser descrito por um segmento de reta, tomando uma das extremidades como centro e o comprimento do segmento como raio;

IV ângulos retos são congruentes;

V dada uma reta r e um ponto P fora dela, há um único ponto que passa por P e nunca intercepta r.

Neste Capítulo iniciamos uma exploração de duas geometrias. Primeiro, a Geometria Afim, que é uma descrição mais interessante da Geometria Euclidiana (nela ainda valem os postulados de Euclides); e depois, a Geometria Projetiva, onde o postulado V (das retas paralelas) já não vale, porque não há nesta geometria retas paralelas – *todas* as retas se encontram em algum ponto.

13.1 Geometria Afim

Nos interessam neste Capítulo algumas transformações que não estudamos anteriormente por não serem lineares, apesar de serem simples e importantes. Em particular, não pudemos, no Capítulo 3, tratar de translações, que são um tipo de *isometria*.

Isometrias são movimentos rígidos, ou transformações que preservam as distancias entre pontos – por exemplo, translações são isometrias. Quando tratamos de transformações lineares, observamos que a translação não é linear.

A Geometria Afim generaliza a Geometria Euclidiana separando pontos de vetores: os vetores não tem posição fixa no espaço (sua visualização "depende de um referencial"), e pontos são posições fixas (são "referenciais" qua podemos usar para visualizar vetores).

[1] O quinto postulado na verdade foi descrito por Euclides de forma diferente, mas o enunciado que damos é equivalente a ele.

Um ponto pode ser descrito por um vetor e um referencial (o ponto que convencionamos chamar de "origem"). Se trocarmos o referencial, teremos realizado uma translação. Poderemos representar translações naturalmente como matrizes, e consequentemente como *transformações afim*. Começamos, portanto, definindo isometrias.

Definição 13.1 (isometria)**.** Sejam V e W espaços vetoriais com produto interno. uma transformação $T : V \to W$ é uma *isometria* (ou *movimento rígido*) se, quando aplicada a um conjunto de vetores, preserva as distâncias entre eles, ou seja, para todos $\mathbf{x}$ e $\mathbf{y}$ em V,

$$d_V(\mathbf{x}, \mathbf{y}) = d_W(T(\mathbf{x}), T(\mathbf{y})),$$

onde d_W denota a distância no espaço W e d_V denota a distância em V. ♦

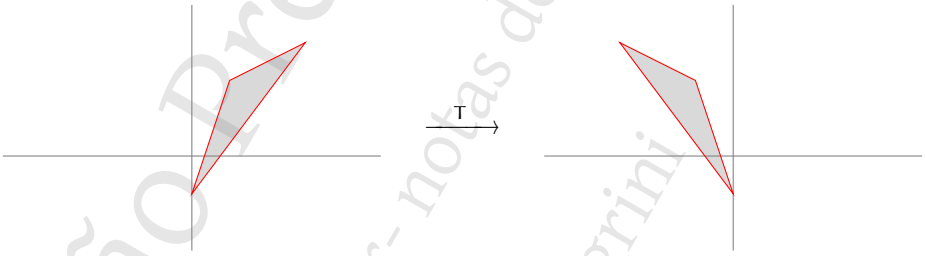
Usualmente teremos $V = W$, e podemos dizer que f é isometria se para todos $\mathbf{x}, \mathbf{y} \in V$, $d(f(\mathbf{x}), f(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})$.

Exemplo 13.2. Rotações, reflexões e translações são isometrias.

Refletir um conjunto de pontos por um hiperplano não muda as distâncias entre os pontos. Por exemplo, considere a reflexão em $\mathbb{R}^2$ pelo eixo das ordenadas,

$$T\big[\,(x_1, x_2)^T\,\big] = (-x_1, x_2)^T.$$

A figura a seguir mostra um exemplo da aplicação desta transformação em uma imagem.



Notamos na figura que a distância entre os pontos transformados não muda. Verificaremos agora algebricamente que T preserva distâncias entre quaisquer dois pontos. Usamos a noção usual de distância para $\mathbb{R}^2$, já vista no Capítulo 7. Verificaremos que

$$d\big[\,(x_1, x_2)^T, (y_1, y_2)^T\,\big] = d\big[T(x_1, x_2)^T, T(y_1, y_2)^T\big].$$

De fato, temos

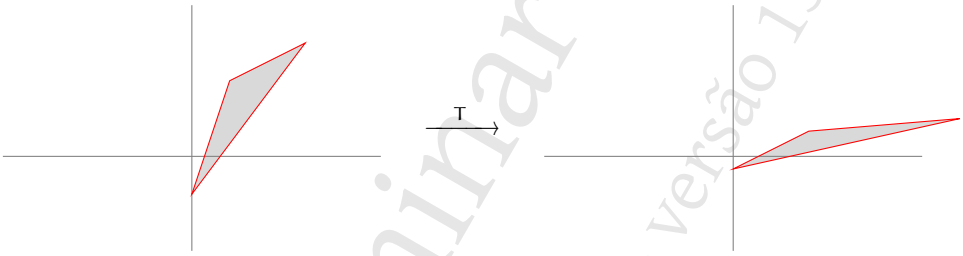
$$\begin{aligned} d\big[\,(x_1, x_2)^T, (y_1, y_2)^T\,\big] &= \sqrt{\langle (x_1, x_2)^T, (y_1, y_2)^T \rangle} \\ &= \sqrt{(x_1, x_2)^T (y_1, y_2)^T} \\ &= \sqrt{x_1 y_1 + x_2 y_2} \\ &= \sqrt{(-x_1)(-y_1) + x_2 y_2} \\ &= \sqrt{(-x_1, x_2)^T (-y_1, y_2)^T} \\ &= \sqrt{\langle (-x_1, x_2)^T, (-y_1, y_2)^T \rangle} \end{aligned}$$

$$= \mathrm{d}\big[\mathsf{T}(x_1, x_2)^\mathsf{T}, \mathsf{T}(y_1, y_2)^\mathsf{T}\big].$$

Pode-se facilmente verificar que o mesmo vale para traslações e rotações. ◀

Exemplo 13.3. Mudança de escala e cisalhamento não são isometrias.

Considere a transformação $\mathsf{T}(x_1, x_2)^\mathsf{T} = (2x_1, x_2/3)^\mathsf{T}$, que realiza mudança de escala nos dois eixos. A operação é ilustrada na figura a seguir.



$$\begin{aligned}
\mathrm{d}\big[\,\mathsf{T}(x_1, x_2)^\mathsf{T}, \mathsf{T}(y_1, y_2)^\mathsf{T}\,\big] &= \mathrm{d}\big[\,(2x_1, x_2/3)^\mathsf{T}, (2y_1, y_2/3)^\mathsf{T}\,\big] \\
&= \sqrt{\langle (2x_1, x_2/3)^\mathsf{T}, (2y_1, y_2/3)^\mathsf{T} \rangle} \\
&= \sqrt{(2x_1, x_2/3)^\mathsf{T} (2y_1, y_2/3)^\mathsf{T}} \\
&= \sqrt{4x_1y_1 + x_2y_2/9} \\
&\neq \sqrt{x_1y_1 + x_2y_2} \\
&= \mathrm{d}\big[(x_1, x_2)^\mathsf{T}, (y_1, y_2)^\mathsf{T}\big].
\end{aligned}$$

A mudança de escala claramente muda a distância entre pontos, a não ser no caso trivial onde o fator de escala é um.

Facilmente podemos obter o mesmo resultado para a operação de cisalhamento, como pede o exercício 289. ◀

Nem toda transformação linear, no entanto, é uma isometria – basta considerar $\mathsf{T}(\mathbf{v}) = \mathbf{0}$, por exemplo.

Teorema 13.4. *Em $\mathbb{R}^n$, qualquer isometria T que preserve a origem, ou seja, tal que $\mathsf{T}(\mathbf{0}) = \mathbf{0}$, é uma rotação.*

Teorema 13.5. *Se T é uma matriz de rotação, então* $\det \mathsf{T} = 1$.

A demonstração do teorema é simples pra $\mathbb{R}^2$:

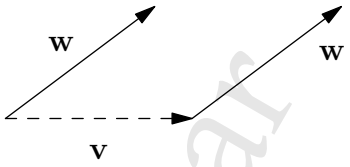
$$\det \mathsf{T} = \det \begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{pmatrix} = \operatorname{sen}^2\theta + \cos^2\theta = 1.$$

O exercício 290 pede a demonstração para $\mathbb{R}^n$.

As transformações lineares em $\mathbb{R}^n$ não representam todas as isometrias, porque translações não são lineares. A geometria afim surge quando tentamos incluir as translações entre as transformações entre espaços vetoriais.

As translações não são lineares porque as transformações lineares são da forma $A\mathbf{x}$, onde apenas trocamos cada coordenada de $\mathbf{x}$ por uma combinação linear das dela com outras. Uma transformação linear não pode somar valores às coordenadas: de outra forma, teríamos $\mathsf{T}(\mathbf{0}) \neq \mathbf{0}$, por exemplo.

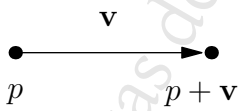
Isso está relacionado ao conceito de vetor: como vetores são independentes de origem (ou de "referencial"), não faz sentido transladá-los. Um vetor **w** transladado por um vetor **v** resultará nele mesmo, como mostra a figura a seguir (note que os dois vetores **w** na figura são idênticos, porque vetores independem de referencial – ou de "origem").



13.1.1 Espaço Afim

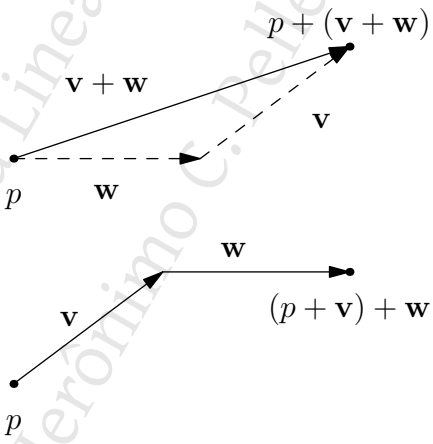
A Geometria Afim resolve dois problemas que percebemos na Geometria Euclideana: primeiro, pontos e vetores não mais se confundem; e em segundo lugar (como consequência da separação de pontos e vetores), podemos representar translações como transformações afim, que definiremos mais adiante.

Um *espaço afim* é uma representação de $\mathbb{R}^n$, sem dar à origem uma posição privilegiada, separando os conceitos de *ponto* e *vetor*. Tendo pontos e vetores como noções diferentes, podemos definir a operação de *soma de ponto com vetor*. Note que se somarmos o mesmo vetor a diferentes pontos, todos serão transladados pela mesma distância e na mesma direção. Esta é exatamente a operação de translação que queríamos.



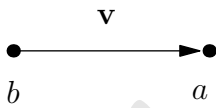
Somando um ponto a um vetor, obtemos outro ponto. Naturalmente, queremos que esta operação obedeça algumas propriedades:

i) deve valer a associatividade na soma de pontos com vetores: $(p + \mathbf{v}) + \mathbf{w} = p + (\mathbf{v} + \mathbf{w})$;



ii) o vetor **0** do espaço vetorial, quando somado a qualquer ponto p, resulta no próprio p;

iii) deve ser possível subtrair um ponto de outro, resultando em um único vetor – ou seja, para dois pontos quaisquer a e b, há um único $\mathbf{v}$ tal que $a = b + \mathbf{v}$ ou, usando a notação de subtração, $a - b = \mathbf{v}$.



Como definimos apenas uma operação (a soma), não tratamos de distributividade. Formalizamos estas idéias na definição a seguir.

Definição 13.6 (espaço afim)**.** Um *espaço afim* sobre um corpo K é uma estrutura $(V, P, +)$, sendo V um espaço vetorial sobre K e P um conjunto de pontos. A operação $+$ obedece às seguintes propriedades: para todos os pontos a, b e vetores $\mathbf{v}$, $\mathbf{w}$,

i) $a + \mathbf{0} = a$;

ii) $(a + \mathbf{v}) + \mathbf{w} = a + (\mathbf{v} + \mathbf{w})$;

iii) existe um único vetor $\mathbf{u}$ tal que $b = a + \mathbf{u}$; denotamos este vetor por $\mathbf{ab}$, ou por $(\mathbf{b} - \mathbf{a})$. ♦

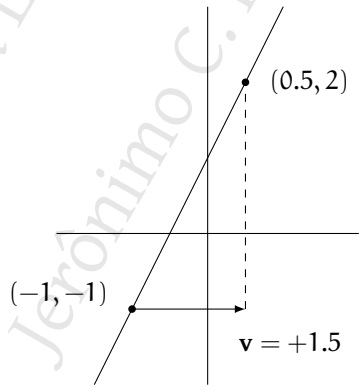
Veja que "herdamos" de V as operações de soma de vetores e de multiplicação de vetor por escalar. Além destas, definimos a operação de soma de ponto com vetor.

Exemplo 13.7. Considere o par $(P = \mathbb{R}^2, V = \mathbb{R}^2)$, onde chamamos os elementos em P de pontos e os elementos em V de vetores. Se usarmos nele a operação usual de soma de vetores, tanto para somar vetores como para somar pontos, temos um espaço afim. Da mesma forma, $(\mathbb{R}^n, \mathbb{R}^n)$ também é. ◀

Exemplo 13.8. Uma reta que não passa pela origem não é um espaço vetorial, mas podemos vê-la como espaço afim: tomamos os pontos de uma reta qualquer – por exemplo, a reta r dada por $y = 2x + 1$ (ou seja, para todo x real, $(x, 2x + 1) \in r$). Agora escolhemos o espaço vetorial $\mathbb{R}$. Definimos a operação $+ : r \times \mathbb{R} \to r$ da seguinte maneira: suponha que o vetor a ser adicionado seja o número real v. Então adicionamos o vetor à primeira coordenada (x), e determinamos a segunda.

$$\underbrace{(x, 2x + 1)}_{\text{ponto}} + \underbrace{(v)}_{\text{vetor}} = \Big(x + v,\, 2(x + v) + 1\Big)$$

A próxima figura ilustra a adição do vetor $(+1.5)$ ao ponto $(-1, -1)$.



Como a reta dada é um conjunto de pontos e $\mathbb{R}$ é um espaço vetorial, nos falta apenas mostrar que a operação de soma de ponto com vetor tem as propriedades descritas na definição 13.6.

i) Para qualquer ponto (x, y) da reta, trivialmente $(x, y) + \mathbf{0} = (x, y)$.

ii) Seja $a = (x, 2x + 1)$ um ponto da reta r, e v, w dois números reais. Então

$$\begin{aligned}[a + v] + w &= [(x, 2x + 1) + v] + w \\ &= (x + v, 2(x + v) + 1) + w \\ &= (x + v + w, 2(x + v + w) + 1) \\ &= (x + [v + w], w(x + [v + w]) + 1) \\ &= (x, 2x + 1) + [v + w] \\ &= a + [v + w].\end{aligned}$$

iii) Sejam $a = (x, 2x + 1)$ e $b = (w, 2w + 1)$ dois pontos da reta r. Então, se $b = a + u$, temos

$$\begin{aligned}(w, 2w + 1) &= (x, 2x + 1) + u \\ (w, 2w + 1) &= (x + u, 2(x + u) + 1),\end{aligned}$$

de onde percebemos que $w = x + u$, e portanto existe um único

$$u = w - x.$$

Agora podemos afirmar que $(r, \mathbb{R}, +)$ é um espaço afim. ◀

Exemplo 13.9. A equação

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

define um parabolóide hiperbólico (que tem um ponto de sela centrado na origem), que chamaremos de P. Note que podemos reescrever a equação:

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

Os pontos deste objeto geométrico podem ser tratados como um espaço afim: usaremos P, o espaço vetorial $\mathbb{R}^2$, e a seguinte operação de soma de pontos com vetores:

$$(x,\, y,\, -x^2 + y^2) + (a, b) = \left(x + a,\, x + b,\, [-(x + a)^2 + (y + b)^2]\right)$$

Geometricamente, usamos o plano $(x, y, 0)$ como "índice", e realizamos ali a soma de vetores aos pontos; depois calculamos a altura do ponto que queremos.

A operação de soma tem as propriedades necessárias para que $(P, \mathbb{R}^2, +)$ seja um espaço afim. ◀

Exemplo 13.10. Sabemos que o conjunto de soluções de um sistema linear *homogêneo* é um espaço vetorial. Já o conjunto de soluções de um sistema linear *não homogêneo* é um espaço afim.

Seja A uma matriz $m \times n$, e seja $A\mathbf{x} = \mathbf{b}$ um sistema não homogêneo, e $A\mathbf{x} = \mathbf{0}$ o sistema homgêneo associado. Observamos que $\mathbf{b}$ e $\mathbf{0}$ tem m linhas.

Denominamos o conjunto de soluções do sistema não homogeneo por B, e o espaço vetorial das soluções do sistema homogeneo por H:

$$B = \{\mathbf{x} : A\mathbf{x} = \mathbf{b}\}$$
$$H = \{\mathbf{x} : A\mathbf{x} = \mathbf{0}\}$$

os elementos de B e H são vetores coluna com n linhas.

Identificamos os elementos de B com pontos, e usamos H como espaço vetorial; nosso espaço afim será portanto $(B, H), +$, onde $+$ é a soma usual de vetores. Sejam $\mathbf{x}, \mathbf{y} \in B$. Então:

i) Seja $\mathbf{0} \in H$ o vetor zero (lembramos que $\mathbf{0}$ sempre é solução para o sistema homogeneo). Trivialmente, $\mathbf{x} + \mathbf{0} = \mathbf{x}$.

ii) Sejam $\mathbf{ab} \in H$. Também é trivial que $\mathbf{x} + (\mathbf{a} + \mathbf{b}) = (\mathbf{x} + \mathbf{a}) + \mathbf{b}$, porque $\mathbf{x}$, $\mathbf{a}$ e $\mathbf{b}$ são vetores em $\mathbb{R}^n$, e a adição de vetores é associativa.

iii) Existe um único $\mathbf{a} \in H$ tal que

$$\mathbf{x} = \mathbf{a} + \mathbf{y}.$$

Certamente a existe e é único, porque é a soma de dois vetores, $\mathbf{x}$ e $-\mathbf{y}$. Resta mostrar que $\mathbf{a}$ pertence a H.

$$\begin{aligned} \mathbf{x} &= \mathbf{a} + \mathbf{y} \\ A\mathbf{x} &= A\mathbf{a} + \mathbf{y} \\ A\mathbf{x} - A\mathbf{y} &= A\mathbf{a} \\ \mathbf{b} - \mathbf{b} &= A\mathbf{a}, && (\text{Se } \mathbf{x}, \mathbf{y} \in B, \text{então } A\mathbf{x} = b, A\mathbf{y} = b) \\ \mathbf{0} &= A\mathbf{a}. \end{aligned}$$

E assim vemos que $\mathbf{a}$ é solução para o sistema homogeneo, e terminamos a demonstração: $(B, H, +)$ é um espaço afim. ◀

Exemplo 13.11. ◀

13.1.2 Subespaço afim

Definição 13.12 (subespaço afim)**.** (S, W) é subespaço afim de (P, V) se $S \subseteq P$ e (S, W) é um espaço afim. ♦

Exemplo 13.13. Evidentemente, se (P, V) é espaço afim, então (P, V) é subespaço de si mesmo; e tanto $(\{p\}, \emptyset)$ como $(\emptyset, \emptyset)$ são subespaços de (P, V). ◀

Exemplo 13.14. ◀

Lema 13.15. *Se (S, W) é subespaço afim de (P, V) então W é subespaço vetorial de V.*

13.1.3 Dependencia afim, baricentros

Ao estudar espaços vetoriais, definimos o conceito de combinação linear. Em espaços afim não as usamos, porque elas dependem de *coordenadas* dos vetores, que são sempre relativas a uma origem. Esclarecemos com um exemplo.

Sejam $P_1 = (1,1)$ e $P_2 = (3,1)$ dois pontos no espaço afim $(\mathbb{R}^2, \mathbb{R}^2)$. Queremos calcular a combinação linear $2P_1 + P_2$. Se computarmos simplesmente $2\times$ coordenadas de P_1 com coordenadas de P_2, estaremos usando coordenadas *relativas ao vetor zero* – mas havíamos dito que o zero não tem papel privilegiado no espaço afim! Precisamos de um terceiro ponto como referência.

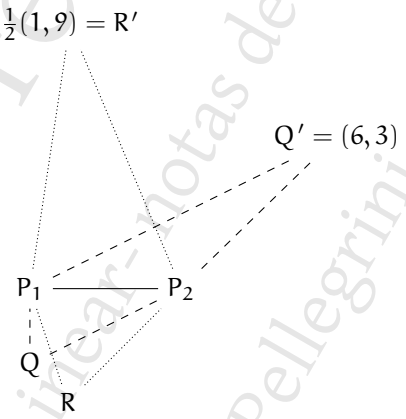
Tomamos então duas outras referencias, $Q = (1,0)$ e $R = (3/2, -1/2)$, e observamos que

$$\begin{aligned} 2QP_1 + 3QP_2 &= 2(0,1) + (2,1) \\ &= (0,2) + (2,1) \\ &= (6,3). \end{aligned} \qquad \begin{aligned} 2RP_1 + 3RP_2 &= 2(-1/2, 3/2) + (3/2, 3/2) \\ &= (-1,3) + (3/2, 3/2) \\ &= \frac{1}{2}(1,9). \end{aligned}$$

ou seja,

$$2QP_1 + 3QP_2 \neq 2RP_1 + 3RP_2.$$

A combinação linear de pontos depende do referencial. A figura a seguir ilustra o que acabamos de calcular.



Para garantir que a combinação de pontos sempre será a mesma, sem depender da referência, basta exigir que a soma dos coeficientes seja um.

Teorema 13.16. *Sejam $p_1, \ldots, p_n$ pontos em um epsaço afim, e $\lambda_1, \lambda_2, \ldots, \lambda_n$ escalares cuja soma é um. Então para quaisquer dois pontos q, r no mesmo espaço,*

$$q + \sum_i \lambda_i \mathbf{qp_i} = r + \sum_i \lambda_i \mathbf{rp_i}$$

Demonstração. Para quaisquer pontos q e r,

$$q + \sum_i \lambda_i \mathbf{qp_i} = q + \sum_i \lambda_i (\mathbf{qr} + \mathbf{rp_i})$$

$$
\begin{aligned}
&= q + \left(\sum_i \lambda_i\right)\mathbf{qr} + \sum_i \lambda_i \mathbf{rp_i} \\
&= q + \mathbf{qr} + \sum_i \lambda_i \mathbf{rp_i} \\
&= r + \lambda_i \mathbf{rp_i}.
\end{aligned}
$$

■

Temos agora justificativa para definir o análogo de combinação linear para espaços afim.

Definição 13.17 (combinação afim)**.** Uma *combinação afim* ou *baricentro* dos vetores $\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_n}$ é uma combinação linear destes vetores onde a somatória dos coeficientes é um, ou seja, uma combinação afim é

$$\sum_i a_i \mathbf{v}_i,$$

com

$$\sum_i a_i = 1.$$

♦

Exemplo 13.18. Sejam

$$\mathbf{u} = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}, \quad \mathbf{v} = \begin{pmatrix} 0 \\ 2 \\ 2 \end{pmatrix}, \quad \mathbf{w} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Então

$$\frac{1}{5}\begin{pmatrix} 3 \\ 8 \\ 7 \end{pmatrix} = \frac{1}{5}\mathbf{u} + \frac{2}{5}\mathbf{v} + \frac{2}{5}\mathbf{w}$$

é combinação afim de $\mathbf{u}$, $\mathbf{v}$ e $\mathbf{w}$, mas

$$\frac{1}{6}\begin{pmatrix} 5 \\ 11 \\ 9 \end{pmatrix} = \frac{1}{3}\mathbf{u} + \frac{1}{3}\mathbf{v} + \frac{1}{2}\mathbf{w}$$

não é combinação afim de $\mathbf{u}$, $\mathbf{v}$ e $\mathbf{w}$, porque a somatória dos coeficientes não é um. ◄

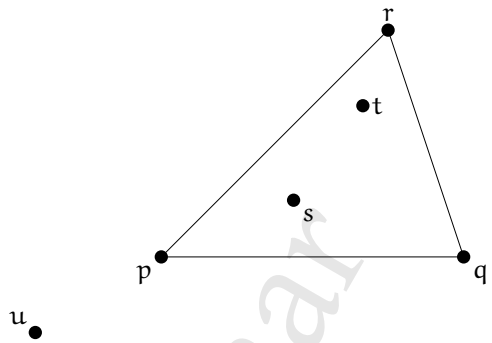
Exemplo 13.19. Os pontos $p = (1,1), q = (1,3), r = (2,4)$ definem um triângulo. Podemos calcular vários baricentros desses pontos:

$$
\begin{aligned}
s &= \frac{1}{2}(1,1) + \frac{1}{4}(5,1) + \frac{1}{4}(4,4) = \frac{1}{4}(11,7) \\
t &= \frac{1}{6}(1,1) + \frac{1}{6}(5,1) + \frac{2}{3}(4,4) = \frac{1}{3}(11,9)
\end{aligned}
$$

Note que podemos usar coeficientes negativos, e que isso significa que geometricamente, um baricentro pode estar "fora" da região delimitada pelo conjunto de pontos[2].

$$u = 3/2(1,1) - \frac{1}{6}(5,1) - \frac{2}{6}(4,4) = \frac{1}{3}(-2,0)$$

[2] Se exigirmos que os coeficientes sejam positivos, teremos uma *combinação convexa*.



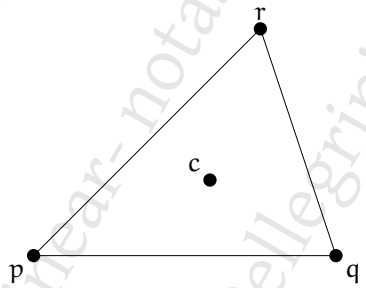
O ponto u ficou fora do triângulo porque foi calculado com coeficientes negativos. ◀

Definição 13.20 (centróide)**.** O *centróide* de um conjunto de pontos $p_1, p_2, \ldots, p_n$ é o baricentro desses pontos com coeficientes $1/n$. ♦

Exemplo 13.21. Os pontos $(1,1), (1,3), (2,4)$ definem um triângulo, e calculamos diversos baricentros dele no exemplo 13.19. O *centróide* dos pontos, no entanto, é

$$c = \frac{1}{3}(1,1) + \frac{1}{3}(5,1) + \frac{1}{3}(4,4) = \left(\frac{10}{3}, 2\right).$$

A próxima figura mostra o centróide.



◀

13.1.4 Dependência afim, coordenadas e bases

Definição 13.22 (dependência afim)**.** Um conjunto de pontos $p_1, \ldots, p_n$ é afim-independente se para algum ponto p_i, os vetores $\mathbf{p_i p_1}, \mathbf{p_i p_2}, \ldots, \mathbf{p_i p_n}$ são linearmente independentes. ♦

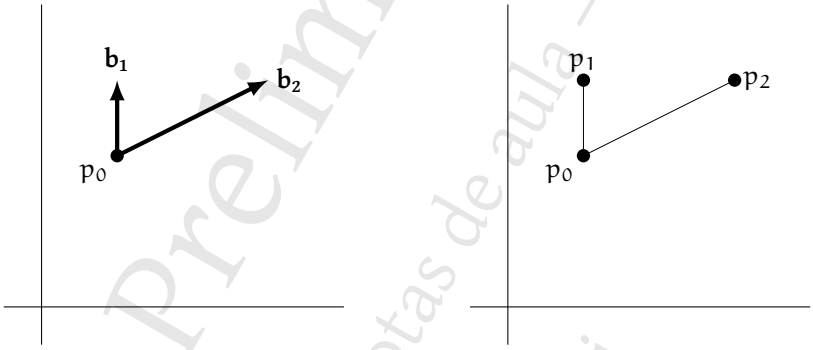
Lema 13.23. *Seja $p_1, \ldots, p_n$ um conjunto de pontos. Se para algum dos pontos, p_i, a família de vetores $\mathbf{p_i p_j}$, com $j \neq i$ forem LI, então para todo i, a família de vetores $\mathbf{p_i p_j}$, com $j \neq i$ é LI.*

Teorema 13.24. *Suponha que um vetor é o baricentro de $p_1, \ldots, p_n$ com coeficientes $\lambda_1, \ldots, \lambda_n$. Então esses coeficientes são únicos se e somente se os pontos $p_1, \ldots, p_n$ são afim-independentes.*

Uma vez que um ponto é unicamente descrito pelos coeficientes de uma combinação afim, indepentede do ponto que usemos como referência, podemos usar estes coeficientes como coordenadas. No entanto, como percebemos anteriormente, as coordenadas são dependentes dos pontos usados para computar o baricentro. Precisamos de algo análogo ao conceito de *base* de um espaço vetorial.

Construiremos então o conceito de base para espaços afim.

Suponha que nosso espaço afim é $(\mathbb{R}^2, \mathbb{R}^2)$. E, espaços vetoriais, nossas coordenadas eram com relação a uma *base* apenas. No espaço afim, como vetores não dependem da referencia fixa na origem, se quisermos um sisetma de coordenadas que nos permita descrever vetores *e pontos*, a intuição nos indica que uma "base" para este espaço deve incluir (i), um ponto de referência (que fará o papel da origem); e (ii), algo que se pareça com uma base para $\mathbb{R}^2$. Na figura a seguir, à esquerda, p_0 é a origem, e $\mathbf{b_1}$, $\mathbf{b_2}$ formam uma base para $\mathbb{R}^2$. Vale lembrar que os vetores foram dispostos partindo de p_0 apenas por conveniência, porque eles não tem "posição fica" no espaço. Na figura da direita, vemos que ao invés de um ponto e dois vetores, podemos usar três pontos para descrever a base do espaço afim – e que, neste exemplo $\mathbf{b_1} = \mathbf{p_p p_1}$ e $\mathbf{b_2} = \mathbf{p_0 p_2}$.



Este raciocínio, generalizado para espaços vetoriais quaisquer, é condensado na definição 13.25.

Definição 13.25 (base afim)**.** Seja (P, V) um espaço afim. Uma *base afim* para (P, V) com origem p_0 consiste de um ponto $p_0 \in P$ e uma base para o espaço vetorial V.

Pode-se denotar a base por $(p_0, \mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n})$, onde p_0 é um ponto e os $\mathbf{b_i}$ são vetores, ou por $(p_0, p_1, \ldots, p_n)$, onde p_0 é a origem e os vetores da base de V são $\mathbf{p_0 p_1}, \mathbf{p_0 p_2}, \ldots, \mathbf{p_0 p_n}$. ♦

Agora, com o conceito de base, já nos é possível definir coordenadas afim.

Definição 13.26 (coordenadas baricêntricas)**.** Seja $B = (p_0, p_1, \ldots, p_n)$ uma base afim. Se um ponto p é baricentro de $p_1, \ldots, p_n$ com origem p_0, e com coeficientes $\lambda_1, \ldots, \lambda_n$, denominamos esses coeficientes de *coordenadas baricêntricas*, ou *coordenadas afim* de p na base B. ♦

13.1.5 Transformações Afim

Trataremos agora de transformações afim. Além das transformações lineares, que já podemos realizar no espaço afim, podemos transladar pontos somando vetores a eles.

Uma *transformação afim* é uma transformação dos pontos de um espaço afim os pontos de outro – ou seja, se os espaços são (P, V) e (P', V'), uma transformação afim terá P como domínio e P' como contradomínio.

A transformação $T : P \to P'$, de pontos em pontos, define uma outra transformação de vetores em vetores: se

$$T(a) = x,$$
$$T(b) = y.$$

Então definimos uma transformação S em V, tal que

$$S(b - a) = T(b) - T(a)$$

Para que T seja afim, S deve ser linear.

Definição 13.27 (transformação afim)**.** Sejam (P, V) e (Q, W) dois espaços afim. Uma função $T : P \to Q$ é uma *transformação afim* se é linear em vetores, ou seja, a transformação $S : V \to W$, tal que $S(b - a) = T(b) - T(a)$ é linear. ♦

O exercício 297 pede a demonstração do teorema 13.29.

Teorema 13.28. *Sejam $A = (V, P)$ e $B = (W, P)$ dois espaços afim. Uma função $T : A \to B$ é uma transformação afim se e somente se preserva baricentros, ou seja,*

$$T(\lambda_1 p_1 + \lambda_2 p_2 + \cdots + \lambda_k p_k) = \lambda_1 T(p_1) + \lambda_2 T(p_2) + \cdots + \lambda_k T(p_k),$$

para qualquer inteiro $k > 0$ e escalares λ_i tais que $\sum_i \lambda_i = 1$.

Exemplo 13.29. Considere o espaço afim $(\mathbb{R}^2, \mathbb{R}^2)$. A transformação dada por

$$f\left[\ (x, y)^T\ \right] = (x, y + 2)^T$$

é uma translação. Verificamos que é uma transformação afim. Mostramos apenas o caso com dois pontos; o caso geral pode ser verificado semelhantemente por indução.

$$\begin{aligned}
af\left[\ (p, q)^T\ \right] + bf\left[\ (x, y)^T\ \right] &= a(p, q + 2)^T + b(x, y + 2)^T \\
&= (ap, aq + 2a)^T + (bx, by + 2b)^T \\
&= (ap + bx, aq + by + 2a + 2b)^T \\
&= (ap + bx, aq + by + 2)^T && (a + b = 1) \\
&= f\left[\ (ap + bx, aq + by)^T\ \right] \\
&= f\left[\ a(p, q)^T + b(x, y)^T\ \right].
\end{aligned}$$ ◄

Exemplo 13.30. A transformação dada por

$$f\left[\ (x, y)^T\ \right] = (-y, 2x)$$

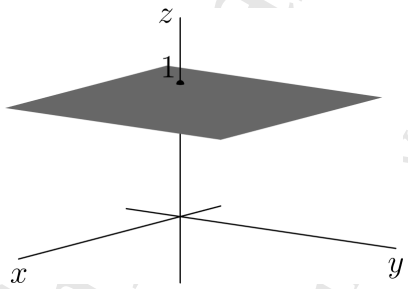
é linear, e deve portanto ser afim. Verificamos:

$$\begin{aligned}
af\left[\ (p, q)^T\ \right] + bf\left[\ (x, y)^T\ \right] &= a(-q, 2p)^T + b(-y, 2x)^T \\
&= (-aq, 2ap)^T + (-by, 2bx)^T \\
&= (-aq - by, 2ap + 2bx)^T \\
&= f\left[\ (ap + bx, aq + by)^T\ \right] \\
&= f\left[\ a(p, q)^T + b(x, y)^T\ \right].
\end{aligned}$$ ◄

13.1.6 Coordenadas afim e matrizes

Queremos poder representar nossas transformações como matrizes, mas enquanto as transformações lineares operam como multiplicação por matriz ($T\mathbf{x} = \mathbf{y}$), transformações afim tem uma parte aditiva ($T\mathbf{x} + \mathbf{z} = \mathbf{y}$). É possível, no entanto, mudar nossa representação de forma que todas as transformações operam da mesma forma, como multiplicação de matrizes.

Suponha que nosso espaço afim seja $(\mathbb{R}^2, \mathbb{R}^2)$. Visualizaremos $\mathbb{R}^2$ como subconjunto de $\mathbb{R}^3$: considere o plano onde $z = 1$, ilustrado na figura:



As transformações lineares em $\mathbb{R}^3$ que levam pontos deste plano nele mesmo são da forma

$$\begin{pmatrix} a_{11} & a_{12} & p \\ a_{21} & a_{22} & q \\ 0 & 0 & 1 \end{pmatrix}$$

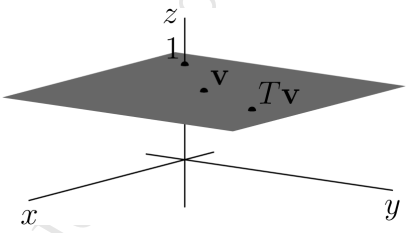
Estas transformações são lineares em $\mathbb{R}^3$, mas *podem transladar pontos dentro deste plano!*

Exemplo 13.31. Considere por exemplo a transformação

$$T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

Aplicamos esta transformação ao ponto $\mathbf{v} = (2, 2, 1)^T$:

$$T\mathbf{v} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ 1 \end{pmatrix}$$



◀

A idéia que expusemos, da representação do espaço afim $(\mathbb{R}^2, \mathbb{R}^2)$ como um plano em $\mathbb{R}^3$, pode ser extendida para dimensões mais altas. De maneira geral, o espaço afim $(\mathbb{R}^n, \mathbb{R}^n)$ e suas transformações afim podem ser descritos como um hiperplano de dimensão n em $\mathbb{R}^{n+1}$, e transformações lineares que agem somente naquele hiperplano.

De maneira geral, uma transformação afim em espaço afim de dimensão n pode ser descrita por uma matriz quadrada de ordem $n+1$.

Teorema 13.32. *Toda transformação afim f pode ser descrita em forma matricial como*

$$f(\mathbf{v}) = A\mathbf{v} + \mathbf{w},$$

onde A é uma matriz quadrada e $\mathbf{w}$ é um vetor.

Além disso, toda função da forma $f(\mathbf{v}) = A\mathbf{v} + \mathbf{w}$ define uma única transformação afim.

Suponha que tenhamos uma transformação afim $T\mathbf{v} + \mathbf{w}$. Se reescrevermos o vetor $\mathbf{v}$ como

$$\mathbf{v}' = (v_1, v_2, \ldots, v_n, 0)^T,$$

a translação $\mathbf{w}$ como

$$\mathbf{w}' = (w_1, w_2, \ldots, w_n, 1)^T,$$

podemos reescrever atransformação como

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & w_1 \\ a_{21} & a_{22} & & a_{2n} & w_2 \\ \vdots & & \ddots & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} & w_n \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix},$$

e teremos

$$A\mathbf{v}' = T\mathbf{v} + \mathbf{w}.$$

Com o acréscimo de uma linha e uma coluna representamos transformações afim como uma única matriz.

Uma transformação afim é composta de uma parte linear e uma translação (a parte afim). Na representação matricial, as primeiras n linhas e colunas da matriz são a parte linear, e a $n-1$-ésima coluna representa a translação.

$$\left(\begin{array}{c|c} L & A \\ \hline \mathbf{0} & 1 \end{array}\right)$$

Exemplo 13.33. A transformação

$$T = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}$$

realiza uma translação equivalente à adição do vetor $(2,3)^T$. De fato, se $\mathbf{x}$ é representado usando coordenadas homogêneas, e portanto $\mathbf{x} = (x_1, x_2, 1)^T$, então

$$T\mathbf{x} = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} x_1 + 2 \\ x_2 + 3 \\ 1 \end{pmatrix}$$ ◀

Exemplo 13.34. Uma transformação estritamente linear (sem translação) terá $A = \mathbf{0}$. Por exemplo,

$$R = \begin{pmatrix} \cos\theta & -\operatorname{sen}\theta & 0 \\ \operatorname{sen}\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

é uma rotação por um ângulo θ, representada como transformação no espaço afim. Temos A igual ao vetor zero, e L igual à matriz da transformação linear que efetua rotação por θ. ◀

Exemplo 13.35. Uma translação pura terá L igual à identidade, e em A teremos o vetor usado para transladar os pontos. Por exemplo,

$$S = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 5 \\ 0 & 0 & 1 \end{pmatrix}$$

é uma translação que adiciona 2 à primeira coordenada e 5 à segunda. ◀

Exemplo 13.36. A combinação dos dois exemplos anteriores é uma rotação seguida de uma translação, representada por

$$T = S \circ R = SR = \begin{pmatrix} \cos\theta & -\operatorname{sen}\theta & 2 \\ \operatorname{sen}\theta & \cos\theta & 5 \\ 0 & 0 & 1 \end{pmatrix}.$$

Se calcularmos $R \circ S$, imediatamente percebemos que rotação e translação não são, de forma geral, comutativas:

$$RS = \begin{pmatrix} \cos\theta & -\operatorname{sen}\theta & 2\cos\theta - 5\sin\theta \\ \operatorname{sen}\theta & \cos\theta & 2\sin\theta + 5\cos\theta \\ 0 & 0 & 1 \end{pmatrix}.$$

◀

O teorema 13.38 nos garante que a composição de duas transformações afim sempre será também outra transformação afim.

Teorema 13.37. *A composição de duas transformações afim é uma transformação afim.*

Demonstração. Sejam f e g duas transformações afim:

$$f(\mathbf{x}) = A\mathbf{x} + \mathbf{w}$$
$$g(\mathbf{x}) = B\mathbf{x} + \mathbf{u}.$$

A composta $f \circ g$ é

$$\begin{aligned} (f \circ g)(\mathbf{x}) &= A\big[g(\mathbf{x})\big] + \mathbf{w} \\ &= A\big[B\mathbf{x} + \mathbf{u}\big] + \mathbf{w} \\ &= AB\mathbf{x} + (A\mathbf{u} + \mathbf{w}), \end{aligned}$$

que é afim. ■

Da demonstração do teorema 13.38 também observamos que transformações afim não são sempre comutativas, já que $A\mathrm{B}\mathbf{x}$ pode ser diferente de $\mathrm{B}A\mathbf{x}$.

Teorema 13.38. *A inversa de uma transformação afim, se existir, também será uma transformação afim.*

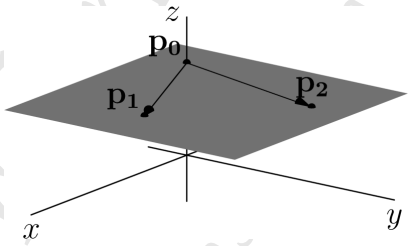
Demonstração. Uma transformação afim pode se escrita como $f(\mathbf{x}) = A\mathbf{x} + \mathbf{w}$. Sua inversa, quando existir, será

$$\begin{aligned} f^{-1}(\mathbf{u}) &= A^{-1}(\mathbf{u} - \mathbf{w}) \\ &= A^{-1}\mathbf{u} - A^{-1}\mathbf{w}. \end{aligned}$$

que claramente também é uma transformação afim. ■

13.1.7 ?

Na figura a seguir, as setas indicam dois vetores que poderiam gerar este plano.



No entanto, as setas *não são* os $\mathbf{p_1}$ e $\mathbf{p_2}$, que são pontos! Os vetores que servem de base para o subespaço de dimensão dois (o plano) são $(\mathbf{p_1} - \mathbf{p_0})$ e $(\mathbf{p_2} - \mathbf{p_0})$.

Para descrever completamente este espaço afim, precisamos de

i) um ponto, que servirá de referência para a descrição dos outros pontos;

ii) uma base para o subespaço onde nossos pontos e vetores estarão.

Assim, para formar uma base para um espaço afim precisamos de $n + 1$ pontos, *cujas coordenadas podem também representar vetores LI* $\mathbb{R}^{n+1}$. Agora definimos o conceito de *dependencia afim*, para determinar exatamente que propriedade esses $n + 1$ vetores devem ter.

Teorema 13.39. *Seja* $(+_0, \mathbf{v_1}, \ldots, \mathbf{v_n})$ *base para um espaço afim* A*, e* T *uma transformação afim de* A *em* A*. Então a transformação* T *é unicamente e completamente caracterizada por* $T(\mathbf{v_1}), \ldots, T(\mathbf{v_n})$*.*

Demonstração. Uma transformação no epsaço afim $(\mathbb{R}^n, \mathbb{R}^n)$ é descrita como um operador linear em $\mathbb{R}^{n+1}$. Este, por sua vez, é caracterizado por $n + 1$ valores em uma base. A base do espaço afim tem exatamente $n + 1$ vetores, então basta descrever a transformação linear em $\mathbb{R}^{n+1}$. ■

Exemplo 13.40. Seja $B = ((0,0,1),(1,0,1),(0,1,1))$ uma base para o espaço afim $(\mathbb{R}^2, \mathbb{R}^2)$, e T uma transformação nesse espaço tal que

$$\begin{aligned} T(0,0,1)^T &= (1,2,1)^T \\ T(1,0,1)^T &= (0,1,1)^T \end{aligned}$$

$$T(0,1,1)^T = (2,4,1)^T$$

Como todo vetor é combinação linear da base, então

$$(x,y,z) = a(0,0,1) + b(1,0,1) + c(0,1,1).$$

com

$$\begin{aligned} a &= z - y - x \\ b &= x \\ c &= y \end{aligned}$$

Então

$$\begin{aligned} T(x,y,z) &= T(a(0,0,1) + b(1,0,1) + c(0,1,1)) \\ &= aT(0,0,1) + bT(1,0,1) + cT(0,1,1) \\ &= a(1,2,1) + b(0,1,1) + c(2,4,1) \\ &= (z-y-x, 2z-2y-2x, z-y-x) + (0,x,x) + (2y,4y,y) \\ &= (-x+y+z, -x+2y+2z, z). \end{aligned}$$

Como $z = 1$,

$$T(x,y,1)^T = (-x+y+1, -x+2y+2, 1)^T$$

A matriz da transformação é

$$T = \left(\begin{array}{cc:c} -1 & 1 & 1 \\ -1 & 2 & 2 \\ \hdashline 0 & 0 & 1 \end{array}\right)$$

Percebemos que a translação associada a esta transformação é dada pelo vetor $(1,2)^T$, que aparece na última coluna da matriz. Isto está de acordo com os valores dados inicialmente para a transformação: $T(0,0,1)^T = (1,2,1)^T$. ◀

Exemplo 13.41. Seja $B = ((1,1,1),(1,0,1),(0,1,1))$ uma base para o espaço afim $(\mathbb{R}^2, \mathbb{R}^2)$, e T uma transformação nesse espaço tal que

$$\begin{aligned} T(1,1,1) &= (1,0,1) \\ T(1,0,1) &= (0,2,1) \\ T(0,1,1) &= (3,3,1) \end{aligned}$$

Como todo vetor é combinação linear da base, então

$$(x,y,z) = a(1,1,1) + b(1,0,1) + c(0,1,1).$$

Disso obtemos

$$\begin{aligned} a &= x + y - z \\ b &= -y + z \\ c &= -x + z \end{aligned}$$

Agora podemos determinar T:

$$\begin{aligned}
T(x,y,z) &= T(a(1,1,1)+b(1,0,1)+c(0,1,1)) \\
&= aT(1,1,1)+bT(1,0,1)+cT(0,1,1) \\
&= a(1,0,1)+b(0,2,1)+c(3,3,1) \\
&= (x+y-z)(1,0,1)+(-y+z)(0,2,1)+(-x+z)(3,3,1) \\
&= (x+y-z,0,z+y-z)+(0,-2y+2z,-y+z)+(-3x+3z,-3x+3z,-x+z) \\
&= (-2x+y+2z,-3x-2y+5z,z).
\end{aligned}$$

Observamos que, como esperado, o último componente é simplesmente z. Como z sepre é um, temos

$$T(x,y,1)^T = (-2x+y+2,-3x-2y+5,1)^T.$$

A matriz desta transformação é

$$T = \left(\begin{array}{cc:c} -2 & 1 & 2 \\ -3 & -2 & 5 \\ \hdashline 0 & 0 & 1 \end{array}\right)$$

◀

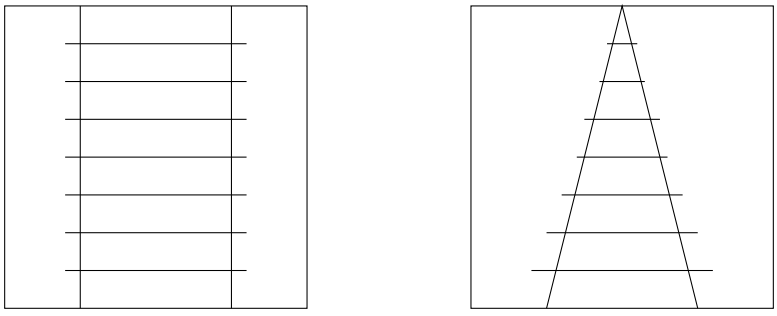
13.2 Geometria Projetiva

(Esta seção é somente um rascunho!)

Iniciamos esta seção com uma descrição intuitiva do que é a Geometria Projetiva, para posteriormente formalizarmos os conceitos de plano projetivo e transformação projetiva.

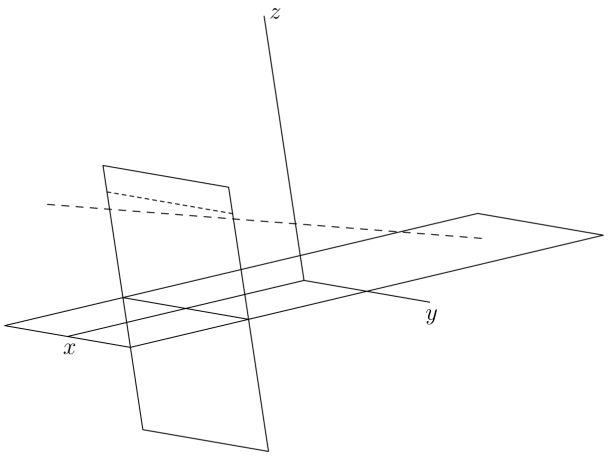
13.2.1 Noções intuitivas

Exemplo 13.42. Na figura a seguir temos, à esquerda, uma representação de uma linha férrea. À direita, a mesma linha férrea desenhada em perspectiva, de forma que os trilhos, que são paralelos, encontram-se em um ponto que supomos estar "no infinito", e os dormentes são desenhados cada vez menores à medida que ficam mais distantes do observador.



◀

A Geometria Projetiva nos permite obter uma imagem em perspectiva, de forma que, por exemplo, duas retas paralelas se encontrem "no infinito".



Definição 13.43 (plano do objeto, da imagem e linha de terra)**.** O plano π_0, que vemos na horizontal na figura, é chamado de *plano do objeto*, e o plano π_1, que está na vertical, é o *plano da imagem*. A linha $\pi_0 \cap \pi_1$, formada pela interseção entre os dois planos, é chamada de "linha de Terra". ♦

No plano do objeto, temos os objetos desenhados sem projeção (ou seja, sem o uso de "perspectiva"). No plano da imagem, temos uma projeção dos objetos, de forma que apareçam "em perspectiva".

Os pontos do plano do objeto são projetados no plano da imagem. A fim de definir como se dá a projeção dos pontos, definimos inicialmente um ponto O, que chamamos de *centro da perspectiva*.

Definição 13.44 (linha de projeção)**.** Para cada ponto P em π_0, traçamos uma reta r passando por P e por O. Esta reta passará pelo plano π_1 (a não ser que seja paralela a ele – não tratermos deste caos agora), e o ponto por onde ela passar, $\pi_1 \cap$ r, é a *linha de projeção* de P em π_1. ♦

Definição 13.45 (linha de fuga, ponto de fuga principal)**.** Se traçarmos um plano q perpendicular a π_1 e passando por O, a interseção q $\cap\, \pi_1$ deste novo plano com o plano da imagem $\mathtt{pi}_1$ será uma reta chamada de *linha de fuga*, ou *linha do horizonte*.

Se traçarmos uma reta s perpendicular a π_1 e passando por O, a interseção s $\cap\, \pi_1$ desta reta com o plano da imagem π_1 será um ponto, chamado de *ponto de fuga principal*. ♦

Mudar a posição do ponto de perspectiva O é como mudar a posição do observador (ou da câmera).

A figura a seguir mostra tres retas paralelas no plano do objeto projetadas no plano da imagem.

13.2.2 Coordenadas Homogeneas

13.2.3 Transformações Projetivas

$$\left(\begin{array}{c|c} L & A \\ \hline P & 1 \end{array}\right)$$

13.3 Aplicações

Leitura Adicional

O leitor encontrará mais informações sobre as Geometrias Afim e Projetiva nos livros de Gallier [Gal01], de Coxeter [Cox08] e de Samule e Levy [SL88]. Os livros de Kostrikin [KM89] e de Shafarevich e Remizov [SR09] também apresentam as Geometrias Afim e Projetiva. O livro de Gomes e Velho [GV08] aborda a aplicação em Computação Gráfica.

Outra abordagem para geometria que pode ser útil é a Álgebra Geométrica, descrita nos livros de Emil Artin [Art88], Alan MacDonald [Mac11] e de Dorst, Fontijne e Mann [DFM07].

Exercícios

Ex. 288 — No exemplo 13.2 mostramos que a reflexão por um dos eixos é uma isometria. Mostre que as reflexões por quaisquer retas que contenham a origem são também isometrias.

Ex. 289 — Nos exemplos 13.2 e 13.3 mencionamos que rotações e translações são isometrias, e que cisalhamento não é isometria, mas não demos demonstração disso. Elabore as demonstrações.

Ex. 290 — Prove o Teorema 13.5.

Ex. 291 — Prove que em um espaço afim, para todos os pontos p, q,

i) $p - p = \mathbf{0}$

ii) $(q - p) = -(p - q)$

iii) $p = q$ se e somente se $(p - q) = \mathbf{0}$

Ex. 292 — No Capítulo1, vimos que os conjuntos de soluções (i) de um sistema linear homogeneo; e (ii) de uma EDO linear homogênea são espaços vetoriais. No presente Capítulo, no exemplo 13.10, provamos que as soluções para um sistema linear não homogêneo formam um espaço afim. Ë natural perguntar se o conjunto de soluções para uma EDO linear *não homogenea* é um espaço afim. Prove que sim ou que não.

Ex. 293 — Seja P^p o conjunto de todos os polinômios cuja *soma* dos expoentes seja par, e P^i aqueles com soma de expoentes ímpar. Prove que $(P^i, P^a, +)$ é um espaço afim.

Ex. 294 — A transformação $f[(x, y)^T] = (1, 1)$ é afim? Mostre que sim ou que não.

Ex. 295 — Prove que transformações afim preservam

i) planos (planos são levados em planos);

ii) paralelismo entre retas e entre planos;

iii) razão entre volumes de paralelepípedos contidos em outros paralelepípedos: se um paralelepípedo A está contido em B, entao vol A/ vol B é igual a vol $f(A)$/ vol $f(B)$.

iv) o mesmo que pede o item (iii), mas para triângulos.

Ex. 296 — Prove que, dados dois triângulos quaisquer A e B em $\mathbb{R}^2$, existe uma transformação afim que leva A em B (e consequentemente, transformações afim não preservam ângulos).

Ex. 297 — Prove o teorema 13.29.

Ex. 298 — Descreva algebricamente a transformação T no espaço afim $(\mathbb{R}^3, \mathbb{R}^3)$, com

$$T(1,0,0,1) = (1,1,1,1)$$
$$T(0,1,0,1) = (0,1,1,1)$$
$$T(0,0,1,1) = (0,0,3,1)$$

Capítulo 14

Série de Fourier

Em espaços vetoriais de dimensão finita sabemos como descrever vetores como combinação linear de alguma base daquele espaço. Como todo espaço de dimensão finita é isomorfo a $\mathbb{R}^n$ e conhecemos bases para $\mathbb{R}^n$, sempre temos como determinar uma base para estes espaços. No entanto, apresentamos no exemplo 2.35 o espaço de polinômios em $\mathbb{R}$, com a base infinita $1, x, x^2, x^3, \ldots$. Claramente, estes polinômios geram todos os polinômios em $\mathbb{R}^n$. Neste capítulo mostraremos que há espaços de funções para os quais podemos determinar bases, compostas de infinitas senóides e cossenóides, e usamos estas bases para descrever certas funções periódicas como combinações lineares infinitas.

14.1 Funções Periódicas

Definição 14.1 (Função periódica)**.** Uma função f com domínio D é *periódica com período* T se existe $T \in D$ tal que $f(x) = f(x+T)$. O menor T positivo tal que esta equação é satisfeita é chamado de *período mínimo* de f.

A *frequência* de f é o inverso de seu período: $\phi = T^{-1}$

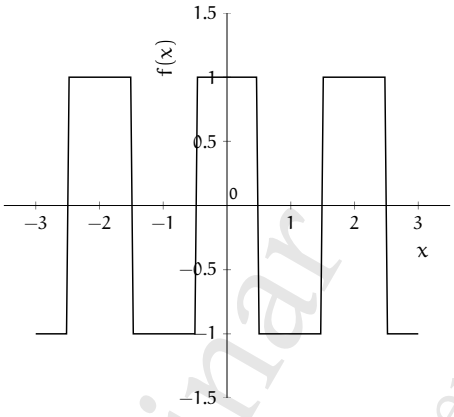
A *frequência angular* de f é

$$\omega = 2\pi\phi = \frac{2\pi}{T}$$ ♦

Suponha que o domínio de uma função periódica f seja o tempo. Enquanto o período é a quantidade de tempo necessária para que o valor da função se repita, a frequência é a quantidade de vezes que os valores se repetem em uma unidade de tempo. Muitas vezes os fenômenos periódicos estão associados a ângulos em uma circunferencia. Neste caso é mais conveniente usar a *frequência angular*, que é a quantidade de vezes em que os valores da função se repetem no decorrer de uma volta completa na circunferência.

Exemplo 14.2. O período das funções seno e cosseno é 2π, e suas frequências angulares são $(2\pi/2\pi) = 1$. O período da função tangente é π, e sua frequência angular é $1/2$. ◀

Exemplo 14.3. Mostramos a seguir o gráfico da função $f(x) = (-1)^{\lfloor x \rceil}$, onde $\lfloor x \rceil$ é o inteiro mais próximo de x.



O período de f é 2 (tome por exemplo o intervalo $(0.5, 2.5]$). A frequência de f é $1/2$, e a frequência angular é 2π. ◀

Exemplo 14.4. Há um exemplo muito simples, mas extremamente importante: seja $f(x) = k$ uma função constante. A função f é periódica, mas não podemos identificar seu período, porque $f(x) = f(x + T) = k$ para *todo* T. ◀

Teorema 14.5. *Se* $f_1, \ldots, f_n$ *são funções periódicas definidas no mesmo domínio* D*, com o mesmo período, e* $a_1, \ldots, a_n$ *constantes em* D*, a combinação linear*

$$h(x) = \sum_{i=1}^{n} a_i f_i(x)$$

é periódica, e seu período é o mesmo das f_i*.*

Teorema 14.6. *Se* f *é periódica com período* T*, e* $a \neq 0$*, então* $f(ax)$ *é periódica com período* T/a*.*

Teorema 14.7. *Sejam* $f_1, \ldots$ *são funções periódicas definidas no mesmo domínio* D*, com o mesmo período* T*, e* $a_1, a_2 \ldots \in D$*, Seja* $h(x)$ *definida pela série infinita*

$$h(x) = \sum_{i=1}^{\infty} a_i f_i(x).$$

Então, para os valores de x *para os quais a série converge,* $h(x)$ *é periódica, e seu período é o mesmo das* f_i*, ou seja,*

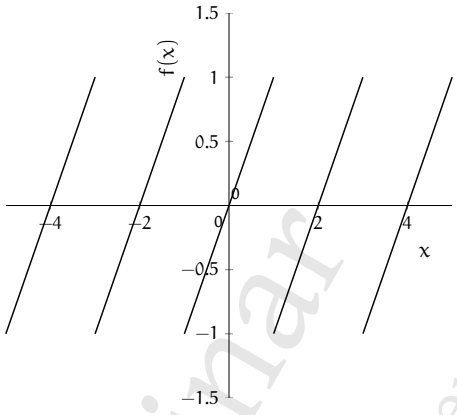
$$h(x) = h(x + T),$$

onde T *é o período das* f_i*.*

Se f não é periódica, podemos tomar seus valores em um intervalo $(a, b]$, e "repetí-los" no resto do domínio da função. À função resultante damos o nome de *extensão periódica* de f.

Definição 14.8 (extensão periódica)**.** Seja f uma função. A *extensão periódica* de f em um intervalo $(a, b]$ é uma função periódica g que tal que $g(x) = f(x)$ quando $x \in (a, b]$, com período $b - a$. ♦

Exemplo 14.9. A função $f(x) = x$ não é periódica. Sua extensão periódica no intervalo $(-1, +1]$ é mostrada na figura a seguir.

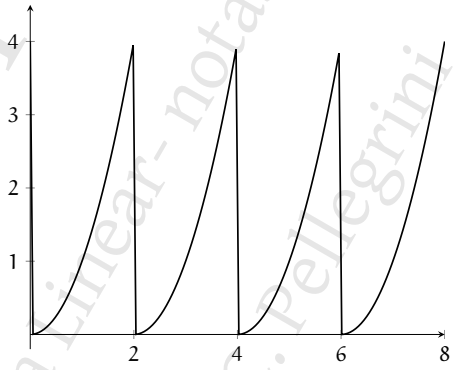


Esta função é dada por

$$g(x) = 2\left(\frac{1}{2} + x - \left\lfloor \frac{1}{2} + x \right\rfloor\right).$$

◀

Exemplo 14.10. A extensão periódica de x^2 no intervalo $[0, 2]$ é ilustrada na figura a seguir.



Observe que em $[0, 2]$ a função é idêntica a x^2, e nos outros períodos o comportamento se repete.

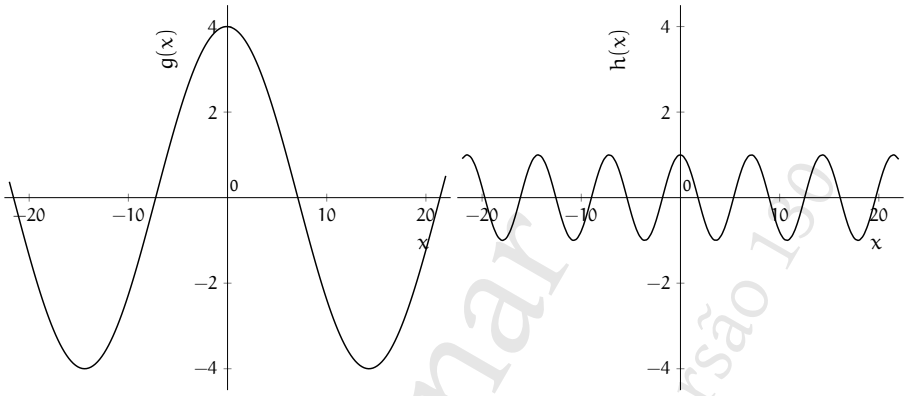
Esta função é dada por

$$g(x) = 2\left(\frac{x}{2} - \left\lfloor \frac{x}{2} \right\rfloor\right)^2.$$

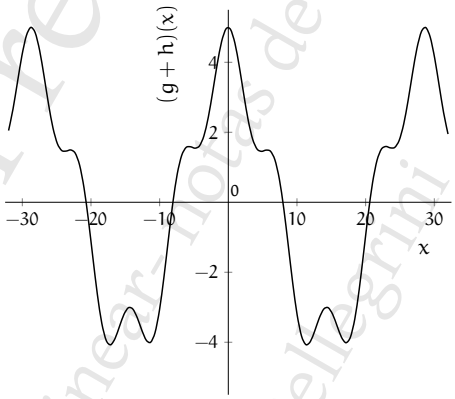
◀

Deve ficar clara a diferença entre a descrição de uma função no *domínio do tempo* e sua descrição no *domínio da frequência*.

A seguir mostramos os gráficos das funções $g(x) = 4\cos(2\pi 2x + 1)$ e $h(x) = \cos(2\pi 8x + 1)$.



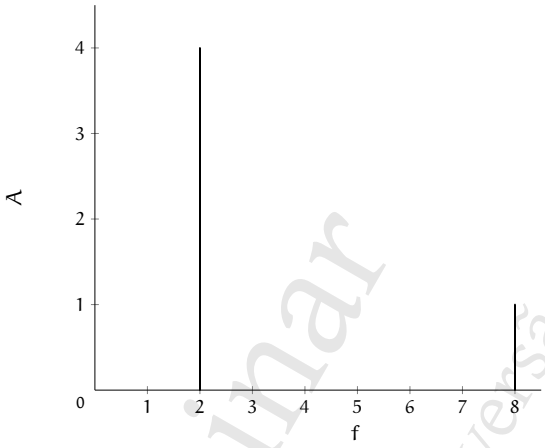
A primeira forma de onda tem frequência $\phi = 2$, amplitude $A = 4$ e deslocamento de fase $f = 1$. A segunda tem frequência $\phi = 8$, amplitude $A = 1$.



Temos agora duas funções somadas, ou *duas formas de onda sobrepostas*. Tendo já fixado a forma $A\cos(2\pi\phi x + f)$, com $f = 1$, podemos representar esta forma de onda como uma função cujo domínio são as frequências e cujo contradomínio são as amplitudes:

$$\begin{aligned} A(2) &= 4 \\ A(8) &= 1 \end{aligned}$$

Desta forma descrevemos a função no *domínio da frequência*.



Podemos também somar infinitas formas de onda – onde "somar infinitas funções" significa especificar uma série.

Por exemplo, considere a forma de onda

$$g_n(x) = a_n \cos(2\pi\omega_n(x) + f),$$

com

$$a_n = \frac{4}{(2n+1)\pi} \tag{14.1}$$

$$\omega_n(x) = (2n+1)x \tag{14.2}$$

$$f = -\frac{\pi}{2}.$$

Podemos somarmos infinitos termos como este,

$$G(x) = g_1(x) + g_2(x) + \cdots .$$

Note que x é um parâmetro, enquanto o n nas equações 14.1 e 14.2 é o índice do termo g_n:

$$\begin{aligned} g_n(x) &= a_n \cos(2\pi\omega_n(x) + f) \\ &= \frac{4}{(2n+1)\pi} \cos\left(2\pi(2n+1)x - \frac{\pi}{2}\right) \end{aligned}$$

A função que acabamos de definir, $G(x)$, é dada portanto pela série

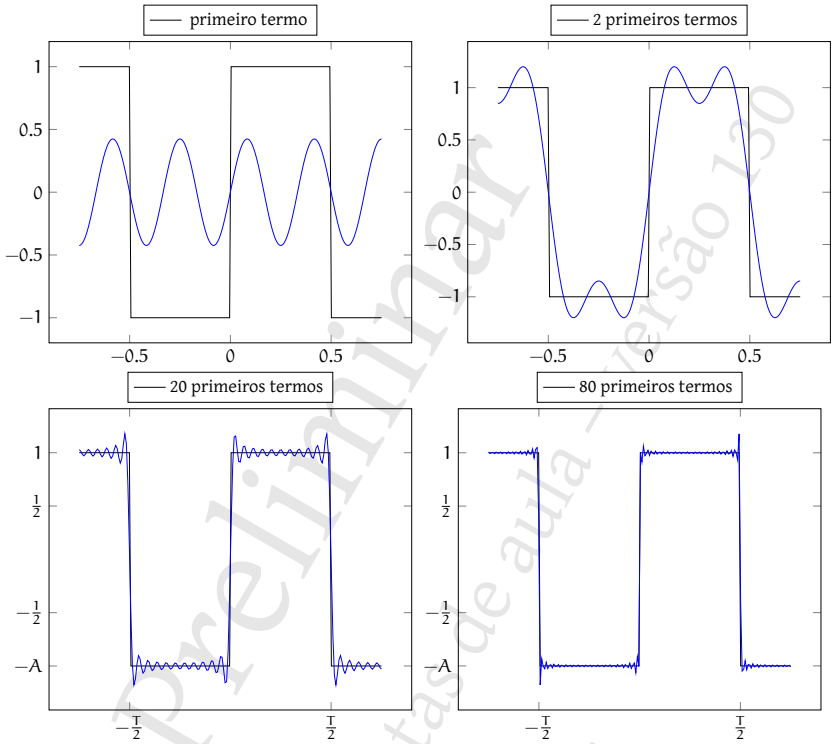
$$G(x) = \sum_{n=1}^{\infty} g_n(x) \tag{14.3}$$

$$= \sum_{n=1}^{\infty} \frac{4}{(2n+1)\pi} \cos\left(2\pi(2n+1)x - \frac{\pi}{2}\right). \tag{14.4}$$

Esta série, que é a soma de infinitas formas de onda, converge para a função

$$f(x) = \begin{cases} -1 & \text{se } x < \lfloor x + 1/2 \rfloor \\ +1 & \text{se } x \geq \lfloor x + 1/2 \rfloor. \end{cases} \tag{14.5}$$

Os gráficos a seguir mostram somatórios dos primeiros 1, 2, 20, e 80 termos da série mostrada na fórmula 14.4, e a função dada na equação 14.5.



A série 14.4 é chamada de *série de Fourier* da função 14.5.

14.2 Série de Fourier

Conhecendo as propriedades de combinações lineares de funções periódicas, podemos definir a série de Fourier, que descreve uma combinação linear infinita de funções de mesmo período. Lembramos que uma série apenas define um somatório, que pode ou não convergir.

Definição 14.11 (Série de Fourier)**.** A série

$$\frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos\left(\frac{2n\pi x}{T}\right) + b_n \operatorname{sen}\left(\frac{2n\pi x}{T}\right)$$

é composta de termos periódicos com o mesmo período T. Tomamos os valores de x para os quais a série converge, definimos uma função $f(x)$ com esses valores como domínio, e dizemos que esta é a *série de Fourier* para f.

Os coeficientes a_i, b_i da combinação linear são chamados de *coeficientes de Fourier*. ♦

Usando frequência angular ao invés de período, a série de Fourier para f é

$$f(x) \sim \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos(n\omega x) + b_n \operatorname{sen}(n\omega x)\,.$$

O símbolo $\sim$ significa que o lado direito é somente uma expansão *formal* (ou *simbólica*). Não usamos o símbolo $=$ porque não podemos garantir que a série converge em todos os casos.

Os lemas a seguir são úteis na solução de equações diferenciais.

Lema 14.12. *Se* $f(x)$ *é periódica com período* T*, sua derivada também tem período* T*.*

Lema 14.13. *Se* $f(x)$ *é periódica e tem expansão de Fourier complexa*

$$f(x) \sim \sum_{k=-\infty}^{+\infty} c_k e^{ikx}$$

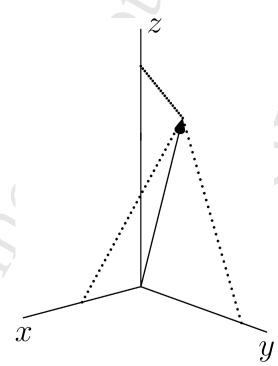
então

$$y'(x) \sim \sum_{k=-\infty}^{+\infty} ikc_k e^{ikx}.$$

14.3 Determinação de coeficientes

Evitaremos por ora determinar quais funções periódicas podem ser representadas por séries de Fourier, e abordaremos o problema de, dada uma função f com período T, determinar os coeficientes de Fourier para f.

A série de Fourier de uma função descreve a função como combinação linear de infinitas formas de onda. Estas infinitas formas de onda são uma base para um determinado espaço de funções. Usamos aqui uma analogia que poderá ajudar a compreender como obteremos os coeficientes da série de Fourier de uma função. Os componentes de um vetor em $\mathbb{R}^3$ são determinados por suas projeções ortogonais na base.



Por exemplo, se usarmos a base canônica $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ e soubermos os ângulos entre $\mathbf{v}$ e os vetores da base, além da magnitude de $\mathbf{v}$, teremos

$$\begin{aligned}
\langle \mathbf{e}_1, \mathbf{v} \rangle &= x = ||\mathbf{v}|| \cos \alpha \\
\langle \mathbf{e}_2, \mathbf{v} \rangle &= y = ||\mathbf{v}|| \cos \beta \\
\langle \mathbf{e}_3, \mathbf{v} \rangle &= z = ||\mathbf{v}|| \cos \gamma
\end{aligned}$$

Usaremos a mesema idéia para determinar os coeficientes de Fourier. No entanto, sabemos que o espaço das funções periódicas tem dimensão infinita, e que não tem, portanto, uma base finita. Já mostramos no

exemplo 7.45 que seno e cosseno são ortogonais no intervalo $[-\pi, \pi]$. O lema 14.14 mostra como obter infinitas funções ortogonais (e portanto LI) entre si. Estas funções são da forma $\cos\left(\frac{2n\pi x}{T}\right)$ e $\operatorname{sen}\left(\frac{2n\pi x}{T}\right)$, com n inteiro. Da mesma forma que descrevemos vetores em espaços de dimensão finita por combinações lineares, também usaremos combinações lineares destas funções para representar funções periódicas.

Lema 14.14. *Usando o produto interno usual para funções* [1]*, em um intervalo fixo* $[a, b]$*; e para quaisquer* m*,* n *inteiros positivos,*

$$\left\langle \cos\left(\frac{2m\pi x}{T}\right), \cos\left(\frac{2n\pi x}{T}\right)\right\rangle = \begin{cases} 0 & \text{se } m \neq n \\ T/2 & \text{se } m = n \end{cases}$$
$$\left\langle \operatorname{sen}\left(\frac{2m\pi x}{T}\right), \operatorname{sen}\left(\frac{2n\pi x}{T}\right)\right\rangle = \begin{cases} 0 & \text{se } m \neq n \\ T/2 & \text{se } m = n \end{cases}$$
$$\left\langle \operatorname{sen}\left(\frac{2m\pi x}{T}\right), \cos\left(\frac{2n\pi x}{T}\right)\right\rangle = 0.$$

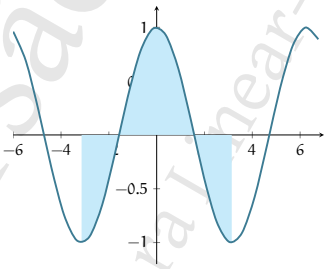
A demonstração do lema 14.14 é um exercício simples de Cálculo. Este lema nos diz que seno e cosseno são ortogonais (isto é semelhante a $\langle \mathbf{e}_1, \mathbf{e}_2\rangle = 0$ em $\mathbb{R}^3$), e que as senóides $\operatorname{sen}(n\pi x/T)$ tem norma $\sqrt{T/2}$ (isto é semelhante a $\|\mathbf{e}_1\|^2 = \langle \mathbf{e}_1, \mathbf{e}_1\rangle = 1$ em $\mathbb{R}^3$), assim como as cossenóides.

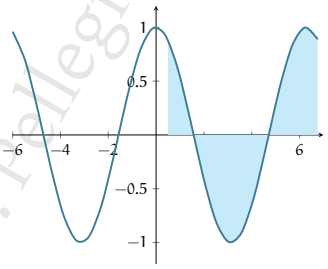
Observe que se $T = 2$, a norma de cada uma das funções é 1, e portanto temos uma *família ortonormal de funções*[2]. quando $T \neq 2$, temos uma *família ortogonal*. Uma família ortogonal é necessariamente composta de funções LI (pelo teorema 7.48).

Lema 14.15. *Seja* f *periódica com período* T*. Então para todos* a *e* b*,*

$$\int_a^{a+T} f(x)\,dx = \int_b^{b+T} f(x)\,dx$$

A intuição nos diz que o lema 14.15 vale; as figuras a seguir mostram gráficos de $\cos(x)$. Na primeira, é ilustrada a integral em $[-\pi, +\pi]$; na segunda, a integral de $[1/2, 1/2 + 2\pi]$. O exercício 300 pede uma demonstração rigorosa deste lema.





Enunciamos agora o teorema que nos dá os coeficientes de Fourier de uma função.

Teorema 14.16 (Fórmulas de Euler-Fourier)**.** *Seja* f *uma função com período* T *e frequência fundamental* ω*. Os coeficientes de Fourier tais que*

$$f(x) \sim \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos(n\omega x) + b_n \operatorname{sen}(n\omega x)$$

[1] O produto interno de funções contínuas foi definido no exemplo 7.6, página 7.6.
[2] Famílias ortogonais de funções também são chamadas de *sistemas ortogonais*.

são

$$\begin{aligned} a_0 &= \frac{2}{T}\int_0^T f(x)dx \\ a_n &= \frac{2}{T}\int_0^T f(x)\cos(n\omega x)dx \\ b_n &= \frac{2}{T}\int_0^T f(x)\,\mathrm{sen}(n\omega x)dx \end{aligned}$$

Demonstração. (i) Para a_0: integramos os dois lados da equação em $[0, T]$:

$$\begin{aligned} \int_0^T f(x)dx &= \int_0^T \left(\frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos(n\omega x) + b_n \,\mathrm{sen}(n\omega x)\right)dx \\ &= \frac{a_0 T}{2}, \end{aligned}$$

e portanto $a_0 = \frac{2}{T}\int_0^T f(x)dx$.

(ii) Para a_n: multiplicamos os dois lados por $\cos(m\omega x)$ e integramos em $[0, T]$:

$$\begin{aligned} \int_0^T f(x)\cos(m\omega x)dx = &\int_0^T \frac{a_0\cos(m\omega x)}{2}dx \\ &+ \sum_{n=1}^{\infty}\left(\int_0^T a_n \cos(n\omega x)\cos(m\omega x)dx + \int_0^T b_n \,\mathrm{sen}(n\omega x)\cos(m\omega x)dx\right) \end{aligned}$$

Pelo lema 14.14, a última integral desta fórmula é zero, e

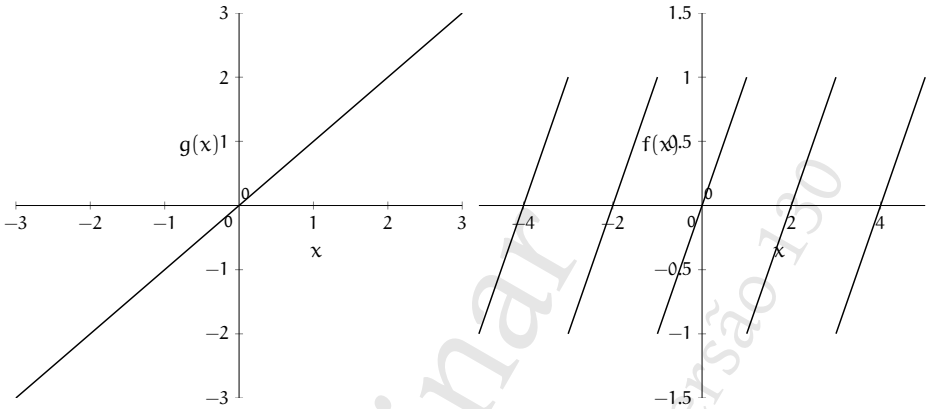
$$\int_0^T f(x)\cos(m\omega x)dx = \int_0^T \frac{a_0\cos(m\omega x)}{2}dx + \sum_{n=1}^{\infty}\int_0^T a_n \cos(n\omega x)\cos(m\omega x)dx$$

Novamente usando o lema 14.14, a integral dentro do somatório é nula quando $m \neq n$ e $T/2$ quando $m = n$. Usamos então $m = n$ e obtemos

$$\begin{aligned} \int_0^T f(x)\cos(n\omega x)dx &= \frac{a_0}{2n\omega}\Big[\mathrm{sen}(n\omega x)\Big]_0^T + \frac{a_n T}{2} \\ &= \frac{a_0}{2n\omega}(\mathrm{sen}(n\omega T) - \mathrm{sen}(0)) + \frac{a_n T}{2} \\ &= \frac{a_n T}{2}. \end{aligned}$$

(iii) Para b_n: usamos raciocínio análogo a (ii), multiplicando por $\mathrm{sen}(m\omega x)$, obtendo $b_n = \frac{2}{T}\int_0^T f(x)\,\mathrm{sen}(n\omega x)dx$. ■

Exemplo 14.17. Sejam $g(x) = x$, e $f(x)$ a expansão periódica de g para o intervalo $(-1, 1]$.



Calcularemos os coeficientes de f no intervalo $(-1, +1]$.

Precisamos da integral de g em um domínio de tamanho 2. Como sabemos que g é definida em função de f, usaremos f. No entanto, não podemos integrar f no intervalo $(0, 2]$ porque este intervalo não corresponde ao domínio fundamental que se repete para compor a função g. Tomamos o intervalo $(-1, 1]$.

$$\begin{aligned} a_0 &= \int_{-1}^{1} x\,dx = 0 \\ a_n &= \int_{-1}^{1} x\cos(nx\pi)\,dx = 0 \\ b_n &= \int_{-1}^{1} x\,\mathrm{sen}(nx\pi)\,dx = \frac{2\,\mathrm{sen}(\pi n)}{\pi^2 n^2} - \frac{\cos(\pi n)}{\pi n}. \end{aligned}$$

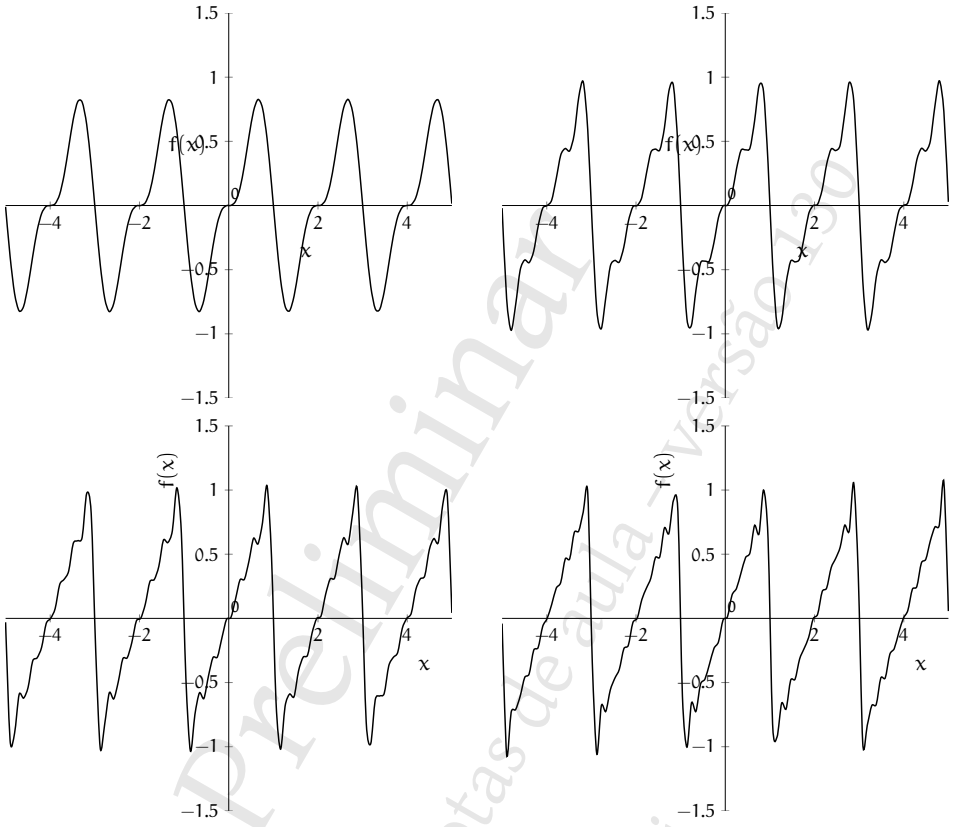
Todos os a_n são zero. Como n é inteiro, $\mathrm{sen}(n\pi) = 0$ e $\cos(n\pi) = -1^n$. Com isto podemos descrever os coeficientes b_n de maneira mais simples:

$$b_n = -\frac{2(-1)^n}{\pi n}.$$

A série de Fourier para $f(x)$ é

$$\begin{aligned} x &= \sum_{n=1}^{\infty} -\frac{2(-1)^n}{\pi n}\,\mathrm{sen}(nx\pi) \\ &= \frac{2}{\pi}\,\mathrm{sen}(\pi x) - \frac{2}{2\pi}\,\mathrm{sen}(2\pi x) + \frac{2}{3\pi}\,\mathrm{sen}(3\pi x)\frac{2}{4\pi}\,\mathrm{sen}(4\pi x) + \cdots \end{aligned}$$

Os gráficos das expansões de Fourier com n até 2, 4, 6 e 8 são mostrados a seguir.



◀

Exemplo 14.18. Consideramos novamente $f(x) = x$, mas desta vez no intervalo $[-\pi, \pi]$ (e consequentemente com período 2π). Temos

$$\begin{aligned}
a_0 &= \frac{1}{\pi}\int_{-\pi}^{\pi} x\,dx = 0\\
a_n &= \frac{1}{\pi}\int_{-\pi}^{\pi} x\cos(nx)\,dx = \frac{1}{\pi}\left(\frac{x\,\mathrm{sen}(nx)}{n} + \frac{\cos(nx)}{n^2}\right)\Big|_{x=-\pi}^{\pi} = 0\\
b_n &= \frac{1}{\pi}\int_{-\pi}^{\pi} x\,\mathrm{sen}(nx)\,dx = \frac{1}{\pi}\left(-\frac{x\cos(nx)}{n} + \frac{\mathrm{sen}(nx)}{n^2}\right)\Big|_{x=-\pi}^{\pi} = \frac{2(-1)^{n+1}}{n}.
\end{aligned}$$

e portanto

$$x = \sum_{n=1}^{\infty} \frac{2(-1)^{n+1}}{n}\,\mathrm{sen}(nx).$$

Substituindo $x = \pi/2$, temos

$$\frac{\pi}{2} = \sum_{n=1}^{\infty} \frac{2(-1)^{n+1}}{n}\,\mathrm{sen}(n\frac{\pi}{2})$$

$$\begin{aligned}\frac{\pi}{4} &= \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} \operatorname{sen}(n\frac{\pi}{2}) \\ &= 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots,\end{aligned}$$

a *série de Gregory*, que nos dá um método para aproximar[3] π. ◀

14.4 Forma exponencial

A *fórmula de Euler* nos permite escrever funções trigonométricas em termos de exponenciais[4][5].

Teorema 14.19 (fórmula de Euler). *Para qualquer ângulo $\theta \in \mathbb{R}$,*

$$e^{i\theta} = \cos(\theta) + i\operatorname{sen}(\theta),$$

e como consequência,

$$\begin{aligned}\operatorname{sen}(\theta) &= \frac{e^{i\theta} - e^{-i\theta}}{2i}, \\ \cos(\theta) &= \frac{e^{i\theta} + e^{-i\theta}}{2}.\end{aligned}$$

Usando a fórmula de Euler, observamos que

$$\begin{aligned}\operatorname{sen}(n\omega x) &= \frac{e^{in\omega x} - e^{-in\omega x}}{2i}, \\ \cos(n\omega x) &= \frac{e^{in\omega x} + e^{-in\omega x}}{2}.\end{aligned}$$

Substituindo na expansão de Fourier de uma função, obtemos a *forma exponencial* para a série de Fourier.

$$\begin{aligned}f(x) &\sim \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos(n\omega x) + b_n \operatorname{sen}(n\omega x) \\ &= \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \frac{e^{in\omega x} + e^{-in\omega x}}{2} + b_n \frac{e^{in\omega x} - e^{-in\omega x}}{2i}\end{aligned}$$

[3] A convergência da série de Gregory é bastante lenta.

[4] Observando com cuidado o Teorema, notamos que como consequência, temos também a conhecida identidade de Euler, $e^{i\pi} = \cos(\pi) + i\operatorname{sen}(\pi) = -1$.

[5] Uma demonstração simples usa a série de Taylor de e^{ix}:

$$\begin{aligned}e^{ix} &= \sum_{n=0}^{\infty} \frac{(ix)^n}{n!} \\ &= \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{2n!} + i \sum_{n=1}^{\infty} \frac{(-1)^{n-1} x^{2n-1}}{(2n-1)!} \\ &= \cos x + i \operatorname{sen} x\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2}\left(a_0 + \sum_{n=1}^{\infty} a_n e^{in\omega x} + a_n e^{-in\omega x} + \frac{b_n e^{in\omega x}}{i} - \frac{b_n e^{-in\omega x}}{i}\right) \\
&= \frac{1}{2}\left(a_0 + \sum_{n=1}^{\infty} a_n e^{in\omega x} + a_n e^{-in\omega x} + (-ib_n)e^{in\omega x} - (-ib_n)e^{-in\omega x}\right) \\
&= \frac{1}{2}\left(a_0 + \sum_{n=1}^{\infty} (a_n - ib_n)e^{in\omega x} + (a_n - b_n)e^{-in\omega x}\right)
\end{aligned}
$$

Observando que os dois termos dentro do somatório diferem somente pelo sinal de n, podemos reescrever de forma mais compacta

$$f(x) \sim \frac{1}{2}\left(\sum_{n=\infty}^{\infty} c_n e^{in\omega x}\right),$$

com

$$c_n = \begin{cases} a_{-n} + ib_{-n} & n < 0, \\ a_0 & n = 0 \\ a_n - ib_n & n > 0. \end{cases} \qquad \text{(porque } e^{i0\omega x} = 1\text{)}$$

Exemplo 14.20. A série de Fourier para $f(x) = x$ em $[-\pi, \pi]$, dada no exemplo 14.18, tem coeficientes

$$\begin{aligned} a_n &= 0 \\ b_n &= \frac{2(-1)^{n+1}}{n}. \end{aligned}$$

A forma exponencial desta série da Fourier é

$$f(x) \sim \frac{1}{2}\left(\sum_{n=\infty}^{\infty} -ib_n e^{in\omega x} - b_n e^{-in\omega x}\right)$$

Temos $\omega = 2\pi/2\pi = 1$, portanto

$$f(x) \sim \frac{1}{2}\left(\sum_{n=1}^{\infty} -\frac{2i(-1)^{n+1}}{n} e^{inx} - \frac{2(-1)^{n+1}}{n} e^{-inx}\right) \qquad \blacktriangleleft$$

14.5 Convergência

A convegência de séries é um tópico extenso e que envolve muitas sutilezas. Nesta seção abordamos apenas algumas idéias básicas relacionadas à convegência de séries de Fourier.

Apresentaremos tres diferentes *noções de convergência* – ou seja, definiremos de tres maneiras diferentes o que poderíamos entender por convergência para uma série de Fourier. Estas noções serão apresentadas da mais fraca para a mais forte. Há outras noções de convergência que não apresentamos aqui; o leitor pode encontrar um estudo mais extenso sobre convergência de séries na literatura de Análise [Rud76; Apo74], e sobre séries de Fourier na literaura de Análise Harmônica [PW12; BC11; Zyg03].

Para cada número $k \in \mathbb{N}^*$, podemos listar os k primeiros termos de uma série de Fourier. Com diferentes k obtemos diferentes funções. Por exemplo, a série de Fourier do exemplo 14.18 é $\sum_{n=1}^{\infty} \frac{2(-1)^{n+1}}{n} \operatorname{sen}(nx)$, e obtemos dela a seguinte sequência de funções, onde $f_i(x)$ é a i-ésima função da sequência, obtida com os i primeiros termos da série de Fourier.

$$\begin{aligned} f_1(x) &= 2\operatorname{sen}(x) \\ f_2(x) &= 2\operatorname{sen}(x) - \operatorname{sen}(2x) \\ f_3(x) &= 2\operatorname{sen}(x) - \operatorname{sen}(2x) + \frac{2}{3}\operatorname{sen}(3x) \\ &\vdots \end{aligned}$$

Formalizamos a seguir as definições de sequência e série de funções.

Definição 14.21 (Sequencias e Séries de funções)**.** Uma *sequencia de funções* (f_n) é uma função de $\mathbb{N}^*$ em um conjunto de funções, todas tendo o mesmo domínio e o mesmo contradomínio.

Uma *série de funções* é a sequência obtida do somatório dos primeiros termos de uma sequência de funções,

$$s_n = \sum_{i=1}^{n} f_i(x).$$

Em particular, a série infinita para a sequência (f_n) é

$$\sum_{i=1}^{\infty} f_i(x).$$ ♦

Exemplo 14.22. Definimos duas sequências de funções,

$$\begin{aligned} f_n(x) &= nx \\ g_n(x) &= (-1)^n x \\ h_n(x) &= \frac{x}{n} \end{aligned}$$

As sequências são:

$$\begin{array}{lll} f_1(x) = x & g_1(x) = -x & h_1(x) = x \\ f_2(x) = 2x & g_2(x) = +x & h_2(x) = x/2 \\ f_3(x) = 3x & g_3(x) = -x & h_3(x) = x/3 \\ \vdots & \vdots & \vdots \end{array}$$

As séries para f_n, g_n e h_n são

$$\sum f_n = \sum_{n=1}^{\infty} nx = x + 2x + 3x + \cdots$$

$$\sum g_n = \sum_{n=1}^{\infty} (-1)^n x = -x + x - x + x - \cdots$$

$$\sum h_n = \sum_{n=1}^{\infty} \frac{x}{n} = x + \frac{x}{2} + \frac{x}{3} + \cdots \qquad \blacktriangleleft$$

Exemplo 14.23. Além das séries de Fourier, discutidas neste capítulo, outro exemplo relevante é o da série de Taylor,

$$f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \frac{f^{(3)}(a)}{3!}(x-a)^3 + \cdots \qquad \blacktriangleleft$$

Temos já clara a definição de série de funções, e passamos agora a tratar da convergência destas séries. Há diferentes noções de convergência para séries de funções, e apresentamos algumas delas:

- *Convergência quase sempre*: a série deve convergir para a função em todos os pontos exceto por um número "pequeno" deles. O raciocínio é análogo àquele usado quando verificamos que pontos isolados não mudam o valor de uma integral, porque a área abaixo de um ponto é zero.
- *Convergência pontual*: uma série f_n converge para f se para cada x, $f_n(x) \to f(x)$.
- *Convergência uniforme*: a mais forte das noções de convergência; exigimos não somente que $f_n(x) \to f(x)$, mas que seja possível, para algum n, que a distância entre $f_n(x)$ e $f(x)$ seja tão pequena quanto queiramos, *para todo* x.

Quando usamos apenas os n primeiros termos da série de Fourier de uma função f, temos uma aproximação de f. Para medirmos a qualidade desta aproximação definimos uma noção de *erro*.

Definição 14.24 (Erro na aproximação de função por série)**.** Sejam f uma função e f_n uma sequência de funções. O *erro* na aproximação de f pela série

$$S_n(x) = \sum_{i=1}^{n} f_i(x)$$

no ponto x é a diferença entre $f(x)$ e $S_n(x)$,

$$E_n = |f(x) - S_n(x)|. \qquad \blacklozenge$$

Exemplo 14.25. A expansão de Taylor de $\operatorname{sen}(a)$ é

$$\operatorname{sen}(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \frac{x^9}{9!} - \ldots$$

Podemos aproximar $\operatorname{sen}(x)$ usando apenas alguns dos primeiros termos da série:

$$S_4(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!}$$

Comparamos o valor de $\operatorname{sen}(1)$ com $S_4(1)$:

$$\begin{aligned} \sin(1) &= 0.84147098480789\ldots \\ S_4(1) &= 0.84146825396825\ldots \end{aligned}$$

Os valores diferem na quinta casa decimal, e o erro para esta aproximação é menor que 0.00001. $\blacktriangleleft$

14.5.1 Convergência quase sempre

Sabemos como obter os coeficientes de Fourier para uma função f. Estes coeficientes determinam uma aproximação da função por uma série f_n.

Medimos a qualidade da aproximação em x pela norma

$$\|f(x) - S_n(x)\| = \sqrt{\int_a^b (f(x) - f_n(x))^2 dx}, \tag{14.6}$$

ou seja, integrando o quadrado do erro em x. Mostramos a seguir que, se tivermos uma família ortonormal $\{f_1, f_2, \ldots\}$ de funções e se for possível representar f como combinação linear das f_i, os coeficientes de Fourier minimizam o quadrado do erro.

Diremos que a série de Fourier para f *converge quase sempre* se a integral na igualdade 14.6 não é divergente.

Definição 14.26 (Convergência quase sempre)**.** A série f_n converge quase sempre para f no intervalo $[a, b]$ se

$$\lim_{n\to\infty} \int_a^b [f_n(x) - f(x)]^2 dx = 0. \tag{14.7}$$

♦

Da mesma forma que a modificação de um único ponto não altera o valor de uma integral, ao definir a convergência desta forma, permitimos a divergência de uma série em pontos isolados, e ainda assim a tratamos como convergente. Por isso o nome "quase sempre".

Exemplo 14.27. ◄

Queremos portanto que a integral na equação 14.7 não seja divergente. Observamos que $[f_n(x) - f(x)]^2 = f_n(x)^2 - 2f_n(x)f(x) + f(x)^2$, e o que precisamos portanto é que $\int_a^b |f_n(x)|^2 dx$ e $\int_a^b |f(x)|^2 dx$ sejam convergentes.

Definição 14.28 (Espaço L^2 de funções quadrado-integráveis)**.** Uma função real ou complexa f é *quadrado-integrável no intervalo* $[a, b]$ se

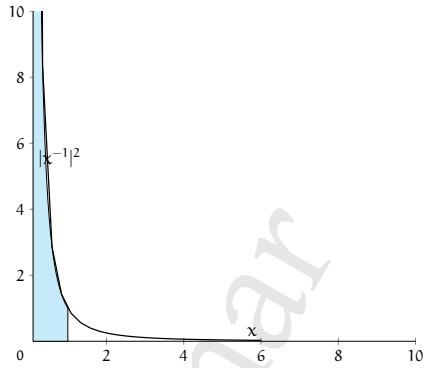
$$\int_a^b |f(x)|^2 dx < \infty.$$

O conjunto de todas as funções quadrado-integráveis em $[a, b]$ é denotado por $L^2[a, b]$. ♦

Assim como na definição de ℓ_2 no exemplo 7.13, usamos $|f|^2$, e não simplesmente f^2, porque f pode ser complexa.

Exemplo 14.29. A função real $f(x) = 4x^4 - x$ é quadrado-integrável no intervalo $[0, 1]$ ($f \in L^2[0, 1]$), porque $\int_0^1 |4x^4 - x|^2 dx = 7/9$.

Já a função $g(x) = 1/x$ não é quadrado-integrável no intervalo $[0, 1]$ (ou seja, $g \notin L^2[0, 1]$), porque a integral $\int_0^1 |x^{-1}|^2 dx$ é divergente (há uma assíntota vertical).



◀

Teorema 14.30. *A série de Fourier de* f *converge quase sempre se*

$$\sum_{n=1}^{\infty} (a_n^2 + b_n^2)$$

converge.

De acordo com o teorema 14.31 L^2 é um espaço vetorial. A demonstração é pedida no exercício 299.

Teorema 14.31. *Para quaisquer* a, b *reais ou complexos,* $L^2[a, b]$ *é um espaço vetorial com as operações usuais de soma de funções e multiplicação por escalar. Além disso, com o produto interno usual (exemplos 7.6 e 7.101), para toda função em* L^2, $\langle f, f\rangle < \infty$ *(ou seja, é finito).*

Os teoremas 14.32 e 14.33 indicam situações em que podemos concluir que uma série de Fourier converge quase sempre

Teorema 14.32. *Se* $f \in L^2[a, b]$*, então a série de Fourier de* f *converge quase sempre.*

Teorema 14.33. *Se tanto* a_n *como* b_n *são tais que*

$$a_n \leq \frac{p}{n}$$
$$b_n \leq \frac{q}{n}$$

onde p *e* q *são constantes, então a série de Fourier com coeficientes* a_n *e* b_n *converge quase sempre.*

14.5.2 Convergência pontual

A idéia básica de convergência pontual é que, à medida que incluímos mais termos na série, $f_n(x)$ tende a $f(x)$, para cada ponto x. Ao contrário da convergência quase sempre, não admitimos que $f_n(x)$ seja divergente de $f(x)$ para nenhum x.

Definição 14.34 (Convergência pontual)**.** Seja (f_n) uma série de funções. Se, para todo x no domínio de f_n,

$$\lim_{n\to\infty} |f_n(x) - f(x)| = 0$$

então a série *converge pontualmente* para f. ♦

Exemplo 14.35. Considere a série

$$\sum_{n=1}^{\infty} \frac{x}{2^{n-1}}.$$

A série converge pontualmente, porque para todo x

$$\lim_{n\to\infty} \frac{x}{2^{n-1}} = 2x \lim_{n\to\infty} \frac{1}{2^n} = 2x.$$

◀

Uma função contínua em partes é composta de várias funções, cada uma contínua em um intervalo, sem assíntotas verticais.

Definição 14.36 (Função contínua em trechos)**.** Uma função f é *contínua em partes* se seu domínio pode ser particionado em uma quantidade *finita* de intervalos disjuntos, e f é contínua em cada um dos intervalos, e o limite de f é finito em todo seu domínio. ♦

Exemplo 14.37. Em qualquer intervalo, a função escada é contínua em trechos
A função dada no exemplo 14.4 também é contínua em trechos em qualquer intevalo. ◀

Exemplo 14.38. Seja $f : \mathbb{R} \to \mathbb{R}$ definida da seguinte maneira.

$$f(x) = \begin{cases} 1 & \text{se } x \in \mathbb{Q} \\ 0 & \text{se } x \notin \mathbb{Q}. \end{cases}$$

A função f *não* é contínua em partes, porque a única partição que resulta em intervalos onde a função é contínua terá infinitas partes racionais e irracionais intercaladas. ◀

Teorema 14.39. *Seja uma função f com período T. Se tanto f como f' são contínuas em partes no intervalo $[-T/2, +T/2]$, então a série de Fourier para f converge pontualmente para f.*

Teorema 14.40. *Convergência pontual implica em convergência quase sempre.*

★ 14.5.3 Convergência uniforme

Há alguns problemas com a noção de convergência pontual: a função f para qual a série converge pode não ser contínua nem integrável, mesmo que cada função f_n da sequência seja. Além disso, embora $f_n(x)$ tenda a $f(x)$ para todo x, para um n fixo não temos garantia de que a distância $|f_n(x) - f(x)|$ é limitada para todo x. A noção de convergência uniforme resolve estes problemas

Definição 14.41 (Convergência uniforme)**.** Seja (f_n) uma série de funções. Se para todo ϵ existe um N_0 tal que para todo $N > N_0$ e para todo x no domínio de f_n,

$$|f_n(x) - f(x)| < \epsilon$$

então a série *converge uniformemente* para f. ♦

Exemplo 14.42. A série $\frac{x}{2^{n-1}}$, que mostramos convergir pontualmente no exemplo 14.35, não converge uniformemente em $\mathbb{R}$.

Intuitivamente, podemos observar o seguinte: esta série é

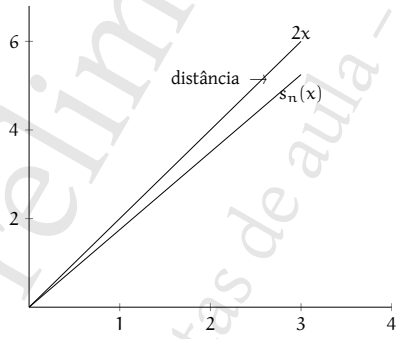
$$x + \frac{x}{2} + \frac{x}{4} + \frac{x}{8} + \cdots,$$

ou seja, a soma de infinitas funções lineares. Sua aproximação com n termos é

$$s_n(x) = x + \frac{x}{2} + \frac{x}{4} + \frac{x}{8} + \cdots + \frac{x}{2^n - 1}$$

claramente também uma função linear em x.

A distância entre a função linear $2x$ (que é para onde a série converge) e outra função linear ($s_n(x)$ neste exemplo) poderá ser tão grande quanto queiramos, bastando para isso escolher x suficientemente grande, como ilustra a figura a seguir.



A seguir damos o mesmo argumento, de forma mais rigorosa.

Seja $\epsilon > 0$. Se a convergrência fosse uniforme, haveria N_0 tal que para todo $N > N_0$,

$$\left| \left(x \sum_{i=1}^{N} \frac{1}{2^{i-1}} \right) - 2x \right| < \epsilon.$$

Suponha $x > 0$, e tentaremos escrever N em função de ϵ. Teríamos

$$x \left| \left(\sum_{i=1}^{N} \frac{1}{2^{i-1}} \right) - 2 \right| < \epsilon$$

$$\left| \left(\sum_{i=1}^{N} \frac{1}{2^{i-1}} \right) - 2 \right| < \frac{\epsilon}{x},$$

e o valor de N dependeria de x – mas a definição de convergência uniforme exige que exista um N_0 a partir do qual a distância entre a série e a função aproximada seja menor que ϵ, *para todo* x. Assim, a convergência não é uniforme. ◀

Exemplo 14.43. Seja $f_n : [0, 1] \to [0, 1]$, tal que

$$f_n(x) = x^n.$$

A série f_n converge pontualmente, porque

$$\lim_{n\to\infty} f_n(x) = \begin{cases} 0 & x \in [0,1) \\ 1 & x = 1. \end{cases}$$

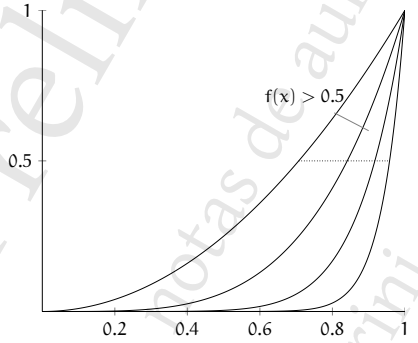
No entanto, mesmo $f(x) = x^n$ sendo contínua para qualquer n, a série converge para uma função descontínua – a descontinuidade está no ponto $f(x) = 1$.

Além disso, mostramos que apesar de convergir pontualmente, a sequência *não* converge uniformemente.

Seja $\epsilon > 0$ – por exemplo, $\epsilon = 1/2$. Suponha que a sequência tenha onvergência uniforme. Então existe algum N_0 tal que, para todo $N > N_0$, e para todo x,

$$|f(x) - f_N(x)| \leq \frac{1}{2}.$$

No entanto, para qualquer N_0, pode-se escolher um valor de x próximo o suficiente de 1 de forma que $f(x) > 1/2$, como se pode perceber observando o gráfico da função abaixo (são mostrados os gráficos de x^2, x^4, x^8 e x^{16}).



Assim teríamos $|f(x) - f_N(x)| = |f(x) - 0| = f(x) > \frac{1}{2}$. A sequência, portanto, não converge uniformemente. ◀

Exemplo 14.44. A série

$$f_n(x) = \frac{nx}{n^2 - x^2}$$

converge uniformemente no intervalo $[2, \infty]$ para

$$f(x) = \frac{x}{x-1}.$$

Observamos que

$$\frac{nx}{n^2 - x^2} = \frac{nx}{(n+1)(x-1)},$$

e portanto para $\epsilon > 0$ queremos

$$\left| \left(\frac{Nx}{(N+1)(x-1)} \right) - \left(\frac{x}{x-1} \right) \right| < \epsilon$$

para todo N maior que algum N_0.

Escrevemos ϵ em função de N_0. Presumimos $N > N_0$, e

$$\begin{aligned}
\left|\left(\frac{Nx}{(N+1)(x-1)}\right) - \left(\frac{x}{x-1}\right)\right| &= \left|\frac{x}{x-1}\left(\frac{N}{N+1} - 1\right)\right| \\
&= \left|\frac{x}{x-1}\right|\left|\left(\frac{N}{N+1} - 1\right)\right| && \left(\tfrac{x}{x-1} > 0\right) \\
&= \left|\frac{x}{x-1}\right|\left|-\frac{1}{N+1}\right| \\
&= \frac{x}{x-1}\frac{1}{N+1} && (N > 0) \\
&< \frac{x}{x-1}\frac{1}{N} \\
&< \frac{x}{x-1}\frac{1}{N_0} && (N > N_0) \\
&\leq \frac{2}{N_0} && (\text{porque } x \in [2, \infty]) \\
&< \epsilon.
\end{aligned}$$

Note que N_0 depende de ϵ, mas não de x. Desta forma, só precisamos que $2/N_0 < \epsilon$, ou $N_0 > 2/\epsilon$. ◀

Proposição 14.45. *Convergência uniforme implica em convergência pontual.*

Teorema 14.46. *Seja f uma função com expansão de Fourier dada por coeficientes a_n e b_n. Se a série*

$$\sum_{n=1}^{\infty} (|a_n| + |b_n|)$$

converge, então a série de Fourier para f converge uniformemente e f é contínua.

Exemplo 14.47. A expansão de Fourier para

$$f(x) = \frac{x-2}{2}$$

é

$$\begin{aligned}
a_n &= -\frac{\operatorname{sen}(\pi n)}{\pi n} \\
b_n &= \frac{\operatorname{sen}(\pi n) - \pi n \cos(\pi n)}{\pi n^2}
\end{aligned}$$

A série

$$\sum_{n=1}^{\infty} \left|-\frac{\operatorname{sen}(\pi n)}{\pi n}\right| + \left|\frac{\operatorname{sen}(\pi n) - \pi n \cos(\pi n)}{\pi n^2}\right|$$

converge, portanto a série de Fourier converge para uma função contínua. ◀

Teorema 14.48. *Se* f *é contínua em* $[-\pi, +\pi]$, $f(-\pi) = f(+\pi)$ *e a derivada de* f *é contínua em trechos, então a série de Fourier para* f *converge uniformemente.*

Teorema 14.49. *Se* a_n *e* b_n *são tais que*

$$a_n \leq \frac{p}{n^x}$$
$$b_n \leq \frac{q}{n^y},$$

com x, y, p, q *constantes e* $x, y > 1$*, então a série de Fourier com coeficientes* a_n *e* b_n *converge uniformemente.*

★ 14.6 Transformada de Fourier

Da mesma forma que pudemos aproximar funções periódicas por séries, podemos fazer o mesmo com funções não-periódicas. Para isso usamos a *transformada de Fourier*, que é uma generalização da série de Fourier quando o período da função tende ao infinito.

A transformada de Fourier é, portanto, semelhante à série de Fourier: dada uma função qualquer, sua transformada de Fourier será uma outra função, no domínio da frequência.

$$\mathbf{F}(f(x)) = F(\phi),$$

onde G mapeia frequencias ϕ em amplitude. Também é possível, dada G, obter a função através da *transformada inversa de Fourier*:

$$\mathbf{F}^{-1}(F(\phi)) = f(x).$$

A série de Fourier de uma função é um *somatório discreto*, com os coeficientes calculados a partir da função original. Quando a generalizamos, tomando seu limite quando o período tende ao infinito, este somatório torna-se uma integral[6]

Na forma exponencial, a série de Fourier de $f(x)$ tem coeficientes

$$c_n = \frac{1}{T}\int_{x_0-T/2}^{x_0+T/2} f(x)e^{-2\pi i n x/T}dx.$$

Desenvolvemos informalmente a definição da transformada de Fourier.Quando o período T tende a ∞, temos

$$\frac{1}{T} \to d\phi \qquad \text{(frequência tenderá a zero)}$$
$$\frac{n}{T} \to \phi$$
$$c_n \to \mathbf{F}(\phi)d\phi.$$

Como consequência disso chegamos à definição da transformada de Fourier, dada a seguir.

Definição 14.50 (transformada de Fourier)**.** Seja f uma função complexa. Sua transformada de Fourier é

$$\mathbf{F}(\phi) = \int_{-\infty}^{+\infty} f(x)e^{-2\pi i \phi x}dx.$$

[6] Vale lembrar a definição de integral como limite de somatório de n termos quando $n \to \infty$.

A *transformada inversa de Fourier* de $\mathbf{F}(\phi)$ é

$$f(x) = \int_{-\infty}^{+\infty} \mathbf{F}(\phi) e^{2\pi i \phi x} d\phi.$$

♦

Exemplo 14.51. A função a seguir não é periódica.

$$f(x) = e^{(-x^2)}$$

Sua transformada de Fourier é

$$\begin{aligned} \mathbf{F}(f(x)) = F(\phi) &= \int_{-\infty}^{+\infty} f(x) e^{-2\pi i \phi x} dx \\ &= \int_{-\infty}^{+\infty} e^{(-x^2)} e^{-2\pi i \phi x} dx \\ &= \sqrt{\pi} e^{-\pi^2 \phi^2} \end{aligned}$$

Isto significa que f pode ser descrita como uma soma de infinitas formas de onda, e que a amplitude da forma de onda com frequência ϕ é

$$A(\phi) = \sqrt{\pi} e^{-\pi^2 \phi^2}.$$ ◄

Exemplo 14.52. A função a seguir não é periódica.

$$f(x) = \frac{1}{x^2 + 1}$$

Sua transformada de Fourier é

$$\begin{aligned} \mathbf{F}(f(x)) = F(\phi) &= \int_{-\infty}^{+\infty} f(x) e^{-2\pi i \phi x} dx \\ &= \int_{-\infty}^{+\infty} \frac{1}{x^2 + 1} e^{-2\pi i \phi x} dx \\ &= \pi e^{-2\pi \phi}. \end{aligned}$$ ◄

Teorema 14.53. *A transformada de Fourier é um operador linear:*

$$\begin{aligned} \mathbf{F}(f + g) &= \mathbf{F}(f) + \mathbf{F}(g) \\ \mathbf{F}(\alpha f) &= \alpha \mathbf{F}(f). \end{aligned}$$

Teorema 14.54 (de Rayleigh)**.** *A energia total é a mesma nos dois domínios.*

$$\int_{-\infty}^{+\infty} |\mathbf{F}(x)|^2 dx = \int_{-\infty}^{+\infty} |\mathbf{F}^{-1}(\phi)|^2 d\phi$$

14.7 Aplicações

14.7.1 Equações diferenciais [série de Fourier]

Uma breve introdução às Equações Diferenciais é dada no Apêndice δ. Nesa seção abordamos alguns métodos para resolver estas equações usando séries de Fourier.

Resolvendo uma equação diferencial [série de Fourier]

Expandir uma função como série de Fourier pode ser útil em diversas situações. Por exemplo, ao resolver uma equação diferencial, pode ser interessante reescrever funções como suas séries de Fourier.

Para exemplificar, resolveremos a equação diferencial linear não homogênea

$$y'' + 3y = 2x,$$

com as condições de contorno

$$y(0) = 0$$
$$y(1) = 0.$$

Tomamos a função $2x$ e a expandimos como série de Fourier no intervalo $[0, 1]$ (que é o que nos interessa, conforme as condições de contorno dadas). Encontramos

$$2x = -\frac{4}{\pi}\sum_{n=1}^{\infty}\frac{(-1)^n \operatorname{sen}(n\pi x)}{n},$$

portanto já podemos reescrever a equação.

$$y'' + 3y = -\frac{4}{\pi}\sum_{n=1}^{\infty}\frac{(-1)^n \operatorname{sen}(n\pi x)}{n}.$$

Agora, presumimos que a expansão de Fourier para $y(x)$ só tem os termos senóides (os cossenóides tem coeficiente zero). Presumimos isto porque as condições de contorno exigem que $y(0) = y(1) = 0$, e isto só pode acontecer para uma série de senóides: $\operatorname{sen}(0\ n\pi) = \operatorname{sen}(1\ n\pi) = 0$, porque n é inteiro. Para cossenos não teríamos zero. A solução para esta equação deve ser então da forma

$$y(x) = \sum_{n=1}^{\infty} b_n \operatorname{sen}(n\pi x).$$

Substituímos na equação, e chegamos a

$$\overbrace{\frac{d^2}{dx^2}\sum_{n=1}^{\infty} b_n \operatorname{sen}(n\pi x)}^{y''} + \overbrace{3\sum_{n=1}^{\infty} b_n \operatorname{sen}(n\pi x)}^{3y} = \overbrace{-\frac{4}{\pi}\sum_{n=1}^{\infty}\frac{(-1)^n \operatorname{sen}(n\pi x)}{n}}^{2x}$$
$$\sum_{n=1}^{\infty} -\pi^2 n^2 b_n \operatorname{sen}(n\pi x) + 3\sum_{n=1}^{\infty} b_n \operatorname{sen}(n\pi x) = -\frac{4}{\pi}\sum_{n=1}^{\infty}\frac{(-1)^n \operatorname{sen}(n\pi x)}{n}$$

$$\sum_{n=1}^{\infty}(3-\pi^2n^2)b_n\,\mathrm{sen}(n\pi x)=\sum_{n=1}^{\infty}\frac{(-4)(-1)^n\,\mathrm{sen}(n\pi x)}{\pi n}$$

Só precisamos portanto garantir que os coeficientes de b_n nos dois lados da equação sejam iguais:

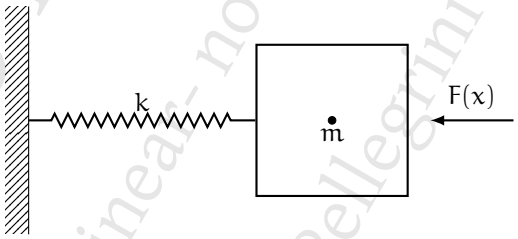
$$(3-\pi^2n^2)b_n=\frac{-4(-1)^n}{\pi n}$$
$$b_n=\frac{-4(-1)^n}{3\pi n-\pi^3n^3},$$

e temos finalmente a solução,

$$y(x)=\sum_{i=1}^{\infty}\frac{-4(-1)^n}{3\pi n-\pi^3n^3}\sin(n\pi x).$$

Oscilador harmônico forçado [série de Fourier]

Considere o sistema massa-mola a seguir. A massa m com $1kg$ está presa a uma mola com constante elástica $k=5$, e uma força F de $1N$ atua sobre a massa periodicamente, atuando por um segundo e parando no segundo seguinte.



Para simplificar a exposição, supomos que o movimento não é amortecido.

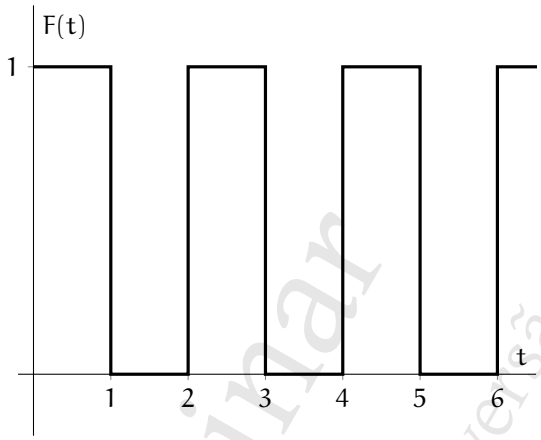
A posição x da massa é dada pela equação diferencial

$$x''+5x=F(t), \tag{14.8}$$

onde F é

$$F(t)=\begin{cases}0 & t\in[-1,0)\\ 1 & t\in[0,1].\end{cases}$$

O gráfico de F é mostrado a seguir.



A posição é claramente dada em *metros*, já que usamos kg para a massa e Newtons para a força.

Suponha que queiramos encontrar a solução geral (note que todas as soluções são periódicas) para esta equação diferencial.

Usaremos o seguinte Teorema, que enunciamos sem demonstração[7], e aplicaremos o *método dos coeficientes indeterminados*[8].

Teorema 14.55. *Sejam* y_1 *e* y_2 *duas soluções fundamentais para a equação homogênea*

$$y'' + ay' + by = 0,$$

ou seja, a solução geral da equação homogênea é

$$Py_1 + Qy_2,$$

onde P *e* Q *são constantes arbitrárias.*

Seja y_p *uma solução particular para a equação não homogênea*

$$y'' + ay' + by = f(x). \tag{14.9}$$

Então toda *solução para 14.9 é a soma de* y_p *com uma combinação linear de* y_1 *e* y_2*, ou seja, é da forma*

$$\alpha y_1 + \beta y_2 + y_p.$$

A partir deste Teorema, chegamos naturalmente no método dos coeficientes indeterminados, que consiste em

i) Encontrar a solução geral $Ay_1 + By_2$ para a equação associada homogênea;

ii) Encontrar *uma* solução y_p particular para a equação não-homogênea;

[7] O leitor encontrará a demonstração em livros sobre Equações Diferenciais Ordinárias (por exemplo, cap. 2 de [Cod61] – mas o leitor pode tentar demonstrá-lo: começe verificando que a diferença entre duas soluções da equação não-homogênea é solução para a homogênea.)

[8] O leitor familiar com este método observará que a parte interessante deste problema está na função $F(x)$, que se comporta como onda quadrada – isto torna o problema diferente dos exemplos iniciais usados na descrição do método em livros-texto, que normalmente não chegam a usar a expansão de Fourier de F.

iii) Descrever a solução geral da equação não-homogênea como $Ay_1 + By_2 + y_p$.

Começamos por (i), obtendo a solução geral de

$$x'' + 5x = 0, \tag{14.10}$$

que é a equação homogênea associada à equação 14.8. Como $m, k > 0$, a equação homogênea tem solução geral

$$A\cos\left(t\sqrt{\frac{k}{m}}\right) + B\,\mathrm{sen}\left(t\sqrt{\frac{k}{m}}\right).$$

Como temos $k = 5$ e $m = 1$, a solução geral de 14.10 é

$$y_c = A\cos\left(t\sqrt{5}\right) + B\,\mathrm{sen}\left(t\sqrt{5}\right).$$

Passamos para o passo (ii), e calculamos a expansão de Fourier de $F(t)$, obtendo

$$\begin{aligned} a_0 &= 1 \\ a_n &= 0 \\ b_n &= \frac{1-(-1)^n}{\pi n} = \begin{cases} 2/\pi n & n \text{ ímpar} \\ 0 & n \text{ par.} \end{cases} \end{aligned}$$

Usaremos a expansão de F e a compararemos com a da solução geral que queremos para x, assim temos

$$\begin{aligned} F(t) &\sim \frac{1}{2} + \sum_{i=1,\,(\text{ímpar})}^{\infty} \frac{2}{\pi n}\,\mathrm{sen}(n\pi t), \\ x(t) &\sim \frac{a_0}{2} + \sum_{i=1}^{\infty} a_n\cos(n\pi t) + b_n\,\mathrm{sen}(n\pi t). \end{aligned}$$

Claramente, $a_n = 0$ quando $n > 0$, e b_n só será diferente de zero para n ímpar. Substituímos a expansão de x no lado esquerdo da equação 14.8.

$$\begin{aligned} x'' + 5x &= \left(\frac{a_0}{2} + \sum_{i=1}^{\infty} b_n\,\mathrm{sen}(n\pi t)\right)'' + 5\left(\frac{a_0}{2} + \sum_{i=1}^{\infty} b_n\,\mathrm{sen}(n\pi t)\right) \\ &= \left(\sum_{i=1}^{\infty} (-n^2\pi^2) b_n\,\mathrm{sen}(n\pi t)\right) + \frac{5}{2}a_0 + 5\sum_{i=1}^{\infty} b_n\,\mathrm{sen}(n\pi t) \\ &= \frac{5}{2}a_0 + \sum_{i=1}^{\infty} (5-\pi^2 n^2) b_n\,\mathrm{sen}(n\pi t). \end{aligned}$$

Agora podemos escrever a equação inteira, substituindo as duas expansões:

$$\begin{gathered} x'' + 5x = F(t) \\ \frac{5}{2}a_0 + \sum_{i=1}^{\infty} (5-\pi^2 n^2) b_n\,\mathrm{sen}(n\pi t) = \frac{1}{2} + \sum_{i=1\,(\text{ímpar})}^{\infty} \frac{2}{\pi n}\,\mathrm{sen}(n\pi t), \end{gathered}$$

e temos igualdade com $5a_0 = 1$, ou $a_0 = 1/5$, e

$$5 - \pi^2 n^2 b_n \operatorname{sen}(n\pi t) = \frac{2}{\pi n} \operatorname{sen}(n\pi t$$
$$5 - \pi^2 n^2 b_n = \frac{2}{\pi n}$$
$$b_n = \frac{2}{\pi n(5 - \pi^2 n^2)}.$$

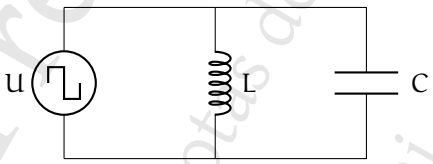
Com estes coeficientes, temos uma solução particular para 14.8:

$$x_p = \frac{1}{4} \sum_{i=1}^{\infty} \frac{2}{\pi n(2 - \pi^2 n^2)} \operatorname{sen}(n\pi t).$$

Podemos agora passar ao passo (iii) e somá-la à solução geral para a equação homogênea associada e finalmente teremos a solução geral para 14.8:

$$\left[A \cos\left(t\sqrt{5}\right) + B \operatorname{sen}\left(t\sqrt{5}\right)\right] + x_p.$$

Observe que a corrente elétrica no circuito LC descrito a seguir obedece a mesma equação que usamos para descrever a posição da massa no sistema massa-mola. A determinação da corrente em circuitos desse tipo é realizada da mesma forma.



$$L = 10H,$$
$$C = \frac{1}{2}F$$

Neste diagrama, U é uma fonte de energia de $1V$, que liga periodicamente (fica ligada por $1s$ e desligada por $1s$).

A equação que dá a corrente em função do tempo neste circuito é

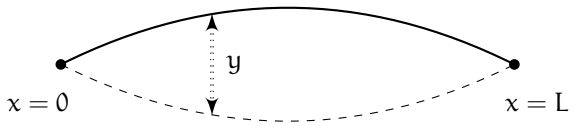
$$i'' + \frac{1}{LC} i = U(t),$$

e como $1/LC = 5$, temos

$$i'' + 5i = U(t).$$

★ 14.7.2 Equações diferenciais parciais: a equação da onda [série de Fourier]

Uma corda de violão está fixada em dois pontos que presumimos estarem alinhados com o eixo x. A distância entre as duas pontas é L. Quando a corda é tocada vibra, oscilando verticalmente.



Seja y a função que descreve o deslocamento vertical da corda em função do tempo t e do deslocamento horizontal x.

Quando a corda está vibrando, $y(x,t)$ obedece a *equação da onda*:

$$\frac{\partial^2 y}{\partial t^2} = c^2 \frac{\partial^2 y}{\partial x^2}$$

onde c é a velocidade em $t = 0$.

A corda não se move nas duas pontas, ou seja, $y = 0$ tanto em $x = 0$ como em $x = L$.

$$y(0,t) = 0 \tag{14.11}$$
$$y(L,t) = 0 \tag{14.12}$$

Além disso, sabemos a posição e a velocidade da corda no instante $t = 0$, ou seja,

$$y(x,0) = f(x) \tag{14.13}$$
$$\frac{\partial}{\partial t} y(x,0) = g(x) \tag{14.14}$$

Queremos determinar $y(x,y)$ em função de x e t. Usamos o método da *separação de variáveis*: presumimos que a função y pode ser decomposta em duas partes, $X(x)$ e $T(t)$, tais que

$$y(x,t) = X(x)T(t).$$

Assim, teremos duas funções diferentes, uma dependendo apenas de x e uma dependendo apenas de t. (Vale lembrar que este também foi o objetivo do uso da diagonalização de operadores na solução de sistemas de equações diferenciais).

Partindo da equação original, temos então

$$\begin{aligned}
\frac{\partial^2 y}{\partial t^2} &= c^2 \frac{\partial^2 y}{\partial x^2} \\
\frac{\partial^2}{\partial t^2} X(x)T(t) &= c^2 \frac{\partial^2}{\partial x^2} X(x)T(t) \\
X(x)T''(t) &= c^2 X''(x)T(t) \\
\frac{X''(x)}{X(x)} &= \frac{1}{c^2}\frac{T''(t)}{T(t)}.
\end{aligned}$$

Os dois lados da equação são iguais, e como o lado esquerdo não depende de t e o direito não depende de x, então nenhum dos dois pode depender de nenhuma variável – os dois lados descrevem a mesma *constante*.

$$\frac{X''(x)}{X(x)} = k = \frac{1}{c^2}\frac{T''(t)}{T(t)}.$$

Temos portanto duas equações diferenciais:

$$X''(x) - kX(x) = 0$$
$$T''(t) - c^2kT(t) = 0$$

Temos que stisfazer as condições de contorno dadas (Equações 14.11 e 14.12).

$$y(0,t) = 0 \;\Rightarrow\; X(0)T(t) = 0 \;\Rightarrow\; X(0) = 0$$
$$y(L,t) = 0 \;\Rightarrow\; X(L)T(t) = 0 \;\Rightarrow\; X(L) = 0$$

Agora voltamos a atenção para a equação

$$X''(x) - kX(x) = 0$$

$$X(0) = 0$$
$$X(L) = 0$$

Se $k > 0$, a solução para esta equação é $X(x) = 0$, que obviamente não nos interessa, porque implicaria em $X(x)T(t) = 0$, e portanto $y(x,t) = 0$ sempre.

Presumimos portanto que k é negativo, ou seja, $k = -p^2$ para algum p. Então a solução é

$$X(x) = A\cos(px) + B\,\mathrm{sen}(px),$$

- Como $X(0) = 0$, necessariamente temos $A = 0$.
- Como $X(L) = 0$, necessariamente temos $B\,\mathrm{sen}(pL) = 0$.

Assim, como $B \neq 0$, $\mathrm{sen}(pL) = 0$ implica em

$$pL = n\pi$$
$$p = \frac{n\pi}{L},$$

para qualquer n inteiro diferente de zero.

Esta seção está incompleta!

14.7.3 Música

★ 14.7.4 Compressão de dados [transformada de Fourier]

★ 14.7.5 Espectroscopia de infravermelho [transformada de Fourier]

Para uma exposição detalhada, veja os livros de Griffiths e Haseth [GH07] e de Davis, Abrams e Brault [DAB01].

Leitura Adicional

Há uma grande quantidade de bons textos que tratam de séries de Fourier mais extensivamente e em mais profundidade do que o fizemos neste Capítulo. Citamos os livros de Jackson [Jac04], Brown e Churchill [BC11], Davis [Dav89], Pereyra e Ward [PW12], e Zygmund [Zyg03].

Exercícios

Ex. 299 — Prove o teorema 14.31.

Ex. 300 — Prove o teorema 14.15.

Ex. 301 — As funções periódicas de mesmo período formam um espaço vetorial? (Prove que sim ou que não)

Ex. 302 — Calcule a série de Fourier que aproxima:

$$\begin{aligned} e(x) &= \cos(x),\ x \in [0, 2\pi] \\ f(x) &= \cos(x),\ x \in [0, \pi] \\ g(x) &= \Big| \lfloor x \rfloor x \Big|,\ x \in [-L, L],\quad L > 0 \\ h(x) &= \begin{cases} 1 & \text{se } 0 < x < \pi \\ -1 & \text{se } -\pi < x \leq 0, \end{cases} \\ i(x) &= |x|,\ x \in [-\pi, \pi] \end{aligned}$$

Ex. 303 — O que acontece com os coeficientes de Fourier para funções pares e ímpares?

Ex. 304 — Calcule a expansão de Fourier para

$$f(x) = \cos^m(x) + \operatorname{sen}^n(x).$$

★ **Ex. 305 —** No exemplo 14.43 mostramos que a série $f_n(x) = x^n$ converge pontualmente mas não uniformemente no intervalo fechado $[0, 1]$. Determine se a sequência converge uniformemente no intervalo *aberto* $[0, 1)$.

★ **Ex. 306 —** Prove que se $f \in L^2[a, b]$, então a sequência de coeficientes de Fourier para f, $a_0, a_1, b_1, \ldots$, pertence a ℓ^2.

Ex. 307 — Prove o Teorema 14.53.

★ **Ex. 308 —** Determine a transformada de Fourier de

a) $f(x) = e^{i\pi x^2}$
b) $g(x) = \cos(x^2)$

Ex. 309 — Seja

$$f(\omega t) = \begin{cases} \operatorname{sin}(\omega t) & \text{se } \operatorname{sin}(\omega t) > 0 \\ 0 & \text{se } \operatorname{sin}(\omega t) \leq 0 \end{cases}$$

i) Determine os coeficientes de Fourier para esta função.

ii) Verifique que a série converge para o valor correto em $t = 0$.

★ **Ex. 310 —** Diga se a série de Fourier calculada no Exercício 309 converge quase sempre, pontualmente ou uniformemente.

Ex. 311 — Os coeficientes em uma série de Fourier são as coordenadas de uma função periódica em uma base, $f_n(x) = \cos(2\pi nx/T)$, $g_n(x) = \operatorname{sen}(2\pi nx/T)$, com $n \in \mathbb{N}$. Mostre outra base para o mesmo espaço (das funções com período T).

Ex. 312 — Seja f uma função não periódica. Qual é o efeito de (1) expandirmos a *série* de Fourier de f usando domínio de integração $[a, b]$, (2) aplicarmos a *transformada* inversa de Fourier na função resultante?

Ex. 313 — Na seção 14.7.1, obtivemos como solução para a equação diferencial a função

$$y(x) = \sum_{i=1}^{\infty} \frac{-4(-1)^n}{3\pi n - \pi^3 n^3} \operatorname{sin}(n\pi x).$$

Mas y é descrita como uma série. Há alguma maneira de obter uma forma fechada para y?

Ex. 314 — Na Seção 14.7.1 obtivemos a solução geral para a equação diferencial que descreve um oscilador harmônico não amortecido. Suponha agora que o movimento é amortecido, e que a equação que o descreve é

$$x'' + 2x' + 5x = F(t).$$

Use a mesma técnica descrita naquela seção para obter a solução geral desta equação.

Ex. 315 — Prove que as séries de Fourier usadass no exemplo da Seção 14.7.1 converge. Faça o mesmo para as séries que usou no Exercício 314.

Ex. 316 — Resolva a equação do calor,

$$\frac{\partial u}{\partial t} - k\frac{\partial^2 u}{\partial x^2} = 0,$$

sujeita às condições

$$\begin{aligned} u(x, 0) &= f(x), \\ u(0, t) &= 0, \\ u(L, t) &= 0, \end{aligned}$$

com

a) $f(x) = 3\operatorname{sen}(\pi x/L)$

b) $f(x) = 2\operatorname{sen}(\pi x/L) - \cos(\pi x/L)$

Capítulo 15

Tensores

Este Capítulo é uma brevíssima introdução aos tensores, que são uma generalização de alguns dos objetos de que tratamos no resto deste livro – escalares, vetores e matrizes.

15.1 Espaço dual e funcionais lineares

Definição 15.1 (Funcional linear)**.** Seja V um espaço vetorial sobre um corpo K. Uma função linear de V em K é um *funcional linear*. ♦

Exemplo 15.2. A função $f : \mathbb{R}^3 \to \mathbb{R}$, dada por

$$f(x, y, z) = 2x - z$$

é um funcional linear em $\mathbb{R}^3$. ◀

Exemplo 15.3. A função $f : \mathbb{R}^3 \to \mathbb{R}$, dada por

$$f(x, y, z) = xyz + xy + yz + xz$$

não é um funcional linear em $\mathbb{R}^3$, porque não é linear. ◀

Exemplo 15.4. No espaço $C^0[0, 1]$, a integral

$$\int_0^1 f(x)dx$$

é um funcional linear, porque

$$\int_0^1 \alpha f(x)dx = \alpha \int_0^1 f(x)dx,$$
$$\int_0^1 f(x) + g(x)dx = \int_0^1 f(x)dx + \int_0^1 g(x)dx.$$ ◀

Claramente, funcionais lineares *em espaços de dimensão finita* são representados por vetores-linha, porque são transformações de V^n em V^1.

Exemplo 15.5. A função $f : \mathbb{R}^3 \to \mathbb{R}$, dada por

$$f(x, y, z) = x - 2y + 3z$$

é um funcional linear em $\mathbb{R}^3$, cuja representação como matriz é

$$F = \begin{pmatrix} 1 & -2 & 3 \end{pmatrix}.$$

Claramente, se $\mathbf{v} = (x, y, z)^T$, então

$$F\mathbf{v} = \begin{pmatrix} 1 & -2 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = x - 2y + 3z. \qquad \blacktriangleleft$$

Definição 15.6 (Espaço dual)**.** Seja V um espaço vetorial. O *espaço dual* de V é formado por todos os funcionais lineares definidos em V. Denotamos o espaço dual de V por V^*. ⧫

A dimensão do espaço dual de V é igual à de V – a demonstração disso é pedida no Exercício 317.

Teorema 15.7. *Seja V um espaço vetorial. Então* $\dim V^* = \dim V$.

Exemplo 15.8. O espaço dual de $\mathbb{R}^3$ é o espaço vetorial formado por todas as funções lineares em $\mathbb{R}^3$ – ou seja, por todos os vetores linha com 3 elementos. Este espaço claramente tem a mesma dimensão que $\mathbb{R}^3$, já que pode ser gerado por qualquer base de $\mathbb{R}^3$ com os vetores transpostos.

Por exemplo, como

$$B = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

é base de $\mathbb{R}^3$, então

$$\Big\{ (1,0,0),\ (0,1,0),\ (0,0,1) \Big\}$$

é base de $(\mathbb{R}^3)^*$. $\blacktriangleleft$

15.2 Covariância e contravariância

15.3 Notação de Einstein

Muitas vezes acontece de precisarmos descrever, em fórmulas, somas semelhantes ao produto interno em $\mathbb{R}^n$. Normalmente escrevemos

$$\sum_{i=1}^{n} \cdots a_i b_i \cdots$$

No entanto, quando há muitas destas somas em uma fórmula (como de fato acontece em Cálculo Tensorial), a quantidade de símbolos de somatório torna-se um problema. Quando trabalhamos com tensores, usamos a *notação de Einstein*:

- Se um índice i aparece exatamente duas vezes em um termo, uma vez como subscrito e uma em sobrescrito, presume-se a soma para todos os valores de i, que deve ficar claro pelo contexto.

- Um mesmo índice não pode aparecer mais de duas vezes na mesma fórmula.

Ou seja,

$$\cdots + a^i b_i + \cdots \;=\; \cdots + \sum_i a^i b_i + \cdots$$

Exemplo 15.9. Seja $B = \{\mathbf{b_1}, \ldots, \mathbf{b_n}\}$ uma base, e um vetor com coordenadas $a_1, a_2, \ldots, a_n$ nesta base. Sabemos que este vetor é

$$\begin{aligned}\mathbf{v} &= a^1\mathbf{b_1} + \cdots + a^n\mathbf{b_n} \\ &= \sum_{i=1}^{n} a^i\mathbf{b_i}.\end{aligned}$$

Usando a notação de Einstein, podemos dizer que

$$\mathbf{v} = a^i\mathbf{b_i},$$

onde fica implícita a soma para todos os valores de i. ◀

Exemplo 15.10. O traço de uma matriz quadrada é

$$\operatorname{Tr} A = a^i_i.$$ ◀

Exemplo 15.11. O produto interno usual em $\mathbb{R}^n$ é

$$\langle \mathbf{v}, \mathbf{w} \rangle = v^i w_i.$$ ◀

Exemplo 15.12. Sejam A e B duas matrizes compatíveis para multiplicação, de forma que AB é definido. Usando a notação usual, $C = AB$ é dado por

$$c^i_j = \sum_{k=1}^{q} a^i_k b^k_j.$$

Usando a notação de Einstein, o mesmo produto é descrito como

$$c^i_j = a^i_k b^k_j.$$ ◀

15.4 Tensores

15.4.1 Operações com tensores

Definição 15.13 (Produto tensorial)**.** ♦

Definição 15.14 (Contração)**.** ♦

★ 15.4.2 Produto tensorial de espaços vetoriais

15.5 Aplicações

Exercícios

Ex. 317 — Prove o Teorema 15.7.

Ex. 318 — Prove que todo tensor semidefinido positivo S tem raiz quadrada, ou seja, existe U tal que $U^2 = S$.

Apêndice α

Revisão: Sistemas Lineares e Matrizes

Este Apêndice trata de matrizes, operações básicas sobre elas e sistemas de equações lineares, a fim de possibilitar a revisão destes conceitos. Alguns tópicos, no entanto, são omitidos, uma vez que são abordados de maneira mais adequada no corpo do texto: a representação de sistemas de equações lineares na forma matricial e a regra de Cramer.

Os tópicos são apresentados de forma como poderiam ser apresentados no ensino médio, sem requisitos adicionais – e mesmo nesta revisão presume-se que o leitor está habituado à notação de somatório. As aplicações no final do Apêndice são também as que normalmente são dadas (ou que poderiam ser dadas) no ensino médio, mas seguem com referências bibliográficas mais avançadas para leitura adicional.

α.1 Sistemas de equações lineares

Definição α.1 (Sistema de equações lineares)**.** Um *sistema de equações lineares* é um conjunto de equações, cada uma representando uma relação linear entre várias variáveis. Uma *solução* para um sistema de equações lineares envolvendo variáveis $x_1, x_2, \ldots, x_n$ é um mapeamento de cada x_i para um valor, de forma que todas as equações do sistema sejam satisfeitas. Formalmente, descrevemos um sistema de equações lineares como

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ \vdots \qquad\qquad & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m \end{aligned}$$

onde os a_{ij} são os *coeficientes* e os x_j são as *incógnitas*.

Quando todos os b_i são zero, o sistema é *homogêneo*. ♦

É conveniente, quando trabalhamos com sistemas lineares, dispor as equações de forma que cada variável x_i apareça alinhada verticalmente em todas as equações.

Exemplo α.2. O sistema

$$\begin{cases} x_1 + x_2 + x_3 - x_4 = 2 \\ x_4 - x_3 = 3 \\ x_2 - x_3 = 2 \\ x_3 = 5 \end{cases}$$

é mais convenientemente visualizado com as variáveis alinhadas:

$$\begin{cases} x_1 + x_2 + x_3 - x_4 = 2 \\ \quad - x_3 + x_4 = 3 \\ x_2 - x_3 \quad = 2 \\ \quad x_3 \quad = 5 \end{cases}$$

◀

Exemplo α.3. Considere os dois sistemas lineares a seguir.

$$\begin{cases} 2x_1 - x_2 = 8 \\ x_1 + x_2 = 30 \end{cases} \qquad \begin{cases} 3x_1 + 8x_2 - x_3 = 0 \\ -x_1 - 3x_2 + 9x_3 = 0 \end{cases}$$

O primeiro sistema não é homogêneo, porque tem constantes 8 e 30 no lado direito das igualdades. Já o segundo é homogêneo, porque o lao direito das equações é zero. ◀

Definição α.4. Um sistema linear é chamado de *possível*, ou *consistente*, se tem solução, e de *impossível* ou *inconsistente* caso contrário. Um sistema consistente pode ter exatamente uma solução – e neste caso é chamado de *determinado* ou infinitas soluções – quando é chamado de *indeterminado.* ♦

Exemplo α.5. O sistema a seguir é consistente e determinado. As duas equações representam duas retas diferentes que se cruzam, portanto a solução é o ponto de $\mathbb{R}^2$ que satisfaz as duas equações – exatamente o ponto onde cruzam.

$$\begin{cases} 2x + y = 0 \\ x + y = 1 \end{cases}$$

O próximo sistema é consistente, mas indeterminado. As duas equações representam a mesma reta, portanto quaisquer valores de x e y que representem pontos desta (ou seja, com $y = 2x - 1$) reta são soluções.

$$\begin{cases} 2x - y = 1 \\ 4x - 2y = 2 \end{cases}$$

Finalmente, o sistema a seguir é inconsistente: as equações representam duas retas paralelas, e não há ponto em comum entre elas (não há (x, y) satisfazendo as duas equações).

$$\begin{cases} x + y = 1 \\ x + y = 3 \end{cases}$$

◀

Definição α.6 (Sistema lineares equivalentes)**.** Dois sistemas lineares são *equivalentes* se admitem exatamente as mesmas soluções. ♦

Exemplo α.7. Considere os sistemas a seguir.

$$\begin{cases} 3x + y = 0 \\ x - y = 5 \end{cases} \qquad \begin{cases} x + \frac{y}{3} = 0 \\ 4x \quad = 5 \end{cases}$$

Os dois sistemas são equivalentes, porque são ambos determinados e admitem apenas a mesma solução $x = 5/4, y = -15/4$. ◀

Definição α.8 (Forma escalonada por linhas de um sistema linear)**.** Suponha que um sistema linear esteja descrito de forma que as variáveis em cada equação aparecem sempre em uma mesma ordem. Este sistema está na *forma escalonada por linhas* (ou *triangular*) se em cada linha, a primeira variável com coeficiente diferente de zero não aparece (ou seja, tem coeficiente zero) nas outras linhas.

A primeira variável com coeficiente diferente de zero em uma linha é chamada de *pivô*. Se todos os pivôs são iguais a um, o sistema está na forma *escalonada reduzida por linhas*. ♦

Exemplo α.9. Os seguintes sistemas estão na forma escalonada. O último está na forma escalonada reduzida.

$$\begin{cases} -5x_1 - x_2 = 2 \\ \quad x_2 = 4 \end{cases} \qquad \begin{cases} -x_1 - x_2 + x_3 = 1 \\ \quad x_2 \quad = 0 \end{cases} \qquad \begin{cases} x_1 + x_2 + x_3 = 2 \\ \quad x_2 - x_3 = 1 \\ \quad x_3 = 10 \end{cases}$$ ◀

Exemplo α.10. Os sistemas a seguir *não* estão na forma escalonada.

$$\begin{cases} 2x_1 + x_2 = 0 \\ -3x_1 - 8x_2 = 1 \end{cases} \qquad \begin{cases} -x_1 - x_2 + x_3 = 0 \\ x_1 - x_2 + 3x_3 = 0 \\ 3x_2 + 2x_3 = 0 \\ 8x_3 = 0 \end{cases} \qquad \begin{cases} 4x_1 - x_2 + 2x_3 = 6 \\ -7x_2 + 5x_3 = 5 \\ 3x_2 - x_3 = 1 \end{cases}$$ ◀

α.1.1 Resolução de sistemas escalonados por linhas

Um sistema na forma escalonada por linhas pode ser resolvido facilmente através de substituição de variáveis:

i) Se a última linha contém uma única incógnita, seu valor já está determinado. Substituímos este valor nas linhas de cima e retiramos esta última linha do sistema, resultando em um novo sistema.

ii) Se a última linha contém mais de uma incógnita, o sistema é indeterminado.

iii) Se a última linha não tem variáveis e é da forma $0 = b_i$, com $b_i \neq 0$, o sistema é inconsistente.

Repetimos este processo até ter obtido os valores de todas as variáveis ou determinar que o sistema não tem solução.

Exemplo α.11. Considere o sistema triangular a seguir.

$$\begin{cases} x_1 + x_2 + x_3 = 2 \\ \quad -x_2 - x_3 = 1 \\ \quad 2x_3 = 10 \end{cases}$$

Resolveremos este sistema usando as regras (i), (ii) e (iii) mencionadas anteriormente.

$$\begin{cases} x_1 + x_2 + x_3 = 2 \\ \quad -x_2 - x_3 = 1 \\ \quad 2x_3 = 10 \end{cases} \xrightarrow{(i),x_3=5} \begin{cases} x_1 + x_2 + 5 = 2 \\ \quad -x_2 - 5 = 1 \end{cases} \xrightarrow{\text{reorganizando}} \begin{cases} x_1 + x_2 = -3 \\ \quad -x_2 = 6 \end{cases}$$

$$\xrightarrow{(i),x_2=-6} \quad x_1 - 6 = -3.$$

e $x_1 = 9$. A solução para o sistema é

$$\begin{aligned} x_1 &= 9 \\ x_2 &= -6 \\ x_3 &= 5 \end{aligned}$$ ◀

Exemplo α.12. Considere o sistema

$$\begin{cases} -2x_1 + x_2 + x_3 + x_4 = 1 \\ x_2 - 3x_3 + x_4 = 0 \\ x_3 = -4 \end{cases}$$

Tentaremos resolver usando as regras mencionadas.

$$\begin{cases} -2x_1 + x_2 + x_3 + x_4 = 1 \\ x_2 - 3x_3 + x_4 = 0 \\ x_3 = -4 \end{cases} \xrightarrow{(i),x_3=-4} \begin{cases} -2x_1 + x_2 + x_4 = 5 \\ x_2 + x_4 = -12 \end{cases} \xrightarrow{(ii)} \quad \perp$$

Aqui percebemos que o sistema tem infinitas soluções: x_2 e x_4 podem variar de forma que sua soma seja -12. Continuamos, para obter o valor de x_1. Determinamos que $x_2 = -x_4 - 12$:

$$-2x_1 + [-x_4 - 12] + x_4 = 5$$

Então

$$-2x_1 - 12 = 5,$$

e temos $x_1 = -17/2$. ◀

α.1.2 Resolução de sistemas lineares na forma geral

Pode-se resolver sistemas de equações lineares usando três operações elementares, que *não mudam* a solução do sistema, a fim de transformar o sistema original em um sistema na forma escalonada. As operações elementares são:

- Permutar a posição de duas equações.
- Multiplicar uma equação por uma constante.
- Somar um múltiplo de uma equação a outra.

Seja um sistema na forma

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ \vdots \qquad\qquad &= \vdots \end{aligned}$$

$$a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_m = b_m$$

Modificaremos uma coluna da matriz de cada vez. A modificação de uma coluna é uma *fase* do algoritmo. Na primeira fase, eliminamos x_1 de todas as linhas abaixo da linha 1; na segunda fase, eliminamos x_2 de todas as linhas abaixo da linha 2; e sucessivamente, eliminamos x_i de todas as linhas abaixo da linha i. O diagrama a seguir ilustra o processo – ali, os pontos ($\bullet$) representam coeficientes das variáveis.

$$\overbrace{\begin{array}{r}\bullet x_1 + \bullet x_2 + \bullet x_3 + \cdots + \bullet x_n = b_1\\ \bullet x_1 + \bullet x_2 + \bullet x_3 + \cdots + \bullet x_n = b_2\\ \bullet x_1 + \bullet x_2 + \bullet x_3 + \cdots + \bullet x_n = b_3\\ \bullet x_1 + \bullet x_2 + \bullet x_3 + \cdots + \bullet x_n = b_4\end{array}}^{\text{fase 1}} \longrightarrow \overbrace{\begin{array}{r}\bullet x_1 + \bullet x_2 + \bullet x_3 + \cdots + \bullet x_n = b_1\\ \bullet x_2 + \bullet x_3 + \cdots + \bullet x_n = b_2\\ \bullet x_2 + \bullet x_3 + \cdots + \bullet x_n = b_3\\ \bullet x_2 + \bullet x_3 + \cdots + \bullet x_n = b_4\end{array}}^{\text{fase 2}}$$

$$\longrightarrow \overbrace{\begin{array}{r}\bullet x_1 + \bullet x_2 + \bullet x_3 + \cdots + \bullet x_n = b_1\\ \bullet x_2 + \bullet x_3 + \cdots + \bullet x_n = b_2\\ \bullet x_3 + \cdots + \bullet x_n = b_3\\ \bullet x_3 + \cdots + \bullet x_n = b_4\end{array}}^{\text{fase 3}} \longrightarrow \overbrace{\begin{array}{r}\bullet x_1 + \bullet x_2 + \bullet x_3 + \cdots + \bullet x_n = b_1\\ \bullet x_2 + \bullet x_3 + \cdots + \bullet x_n = b_2\\ \bullet x_3 + \cdots + \bullet x_n = b_3\\ \cdots + \bullet x_n = b_4\end{array}}^{\text{próximas fases}}$$

Suponha que a linha i contenha x_i com coeficiente α. Suponha também que a linha j tenha coeficiente β para x_i – ou seja, as linhas i e j são

$$\begin{array}{c}\ldots + \alpha x_i + \ldots = b_i\\ \vdots \qquad \vdots\\ \ldots + \beta x_i + \ldots = b_j\end{array}$$

Para eliminar x_i da linha j, somamos $-\beta/\alpha$ vezes a linha i à linha j:

$$\begin{array}{c}\ldots + \alpha x_i + \ldots = b_i\\ \vdots \qquad\qquad \vdots\\ \ldots + ((-\beta/\alpha)\alpha x_i) + \beta x_i + \ldots = (-\beta/\alpha)b_i + b_j\end{array}$$

O resultado será a eliminação de x_i da linha j:

$$\ldots + 0x_i + \ldots = (-\beta/\alpha)b_i + b_j.$$

Este método é chamado de *eliminação de Gauss*.

Exemplo α.13. Transformaremos o sistema a seguir na forma escalonada.

$$\begin{cases} -2x_1 - x_2 + 7x_3 = 1\\ 3x_1 - 2x_2 + x_3 = -1\\ x_1 + x_2 + 3x_3 = 4\end{cases}$$

Somamos à segunda linha $3/2L_1$ e à terceira, $-1/2L_1$:

$$\begin{cases} -2x_1 - x_2 + 7x_3 = 1\\ -7/2x_2 + 23/2x_3 = 1/2\\ 3/2x_2 - 1/2x_3 = 7/2\end{cases}$$

Agora somamos à última linha $3/7L_2$, obtendo um sistema na forma escalonada:

$$\begin{cases} -2x_1 - x_2 + 7x_3 = 1 \\ -7/2x_2 + 23/2x_3 = 1/2 \\ 31/7x_3 = 26/7 \end{cases}$$ ◀

α.2 Matrizes

Definição α.14 (Matriz)**.** Uma *matriz* é uma coleção de objetos dispostos em uma grade, de forma que todas as linhas tem a mesma quantidade de colunas. Uma matriz com m linhas e n colunas é também chamada de "matriz $m \times n$", e é usualmente denotada com seus elementos dispostos de maneira retangular, entre parênteses, como a matriz A abaixo. Também é comum dispor os elementos da matriz entre colchetes, como a matriz B abaixo, que é $p \times k$.

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \quad B = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \vdots & & \ddots & \vdots \\ a_{p1} & a_{p2} & \dots & a_{pk} \end{bmatrix}.$$

Pode-se também denotar as matrizes acima por $A = [a_{ij}]$ e $B = [b_{gh}]$. Usualmente fica subentendido que os elementos de uma matriz M são $m_{11}, m_{12}, \dots$ ♦

É comum denotar matrizes por letras maiúsculas e seus elementos pela mesma letra, minúscula, com a linha e coluna em subscrito.

Exemplo α.15. A matriz A mostrada a seguir é 2×3.

$$A = \begin{pmatrix} 0 & 2 & 4 \\ 1 & 3 & 5 \end{pmatrix}$$

Temos $a_{11} = 0$, $a_{12} = 2$, etc. ◀

Definição α.16 (Classificação de matrizes)**.** Uma matriz é *quadrada* se seu número de linhas é igual ao seu número de colunas. Dizemos que uma matriz quadrada com n linhas e colunas é *de ordem* n. Uma matriz é *triangular superior* se os elementos abaixo de sua diagonal são todos zero. Similarmente, uma matriz é *triangular inferior* se seus elementos acima da diagonal são zero. Uma matriz que é tanto triangular superior como triangular inferior é uma *matriz diagonal*. Uma matriz com uma única coluna é um *vetor coluna*, e uma matriz com uma única linha é um *vetor linha*. Uma matriz A é *simétrica* se $a_{ij} = a_{ji}$ para toda linha i e coluna j (ou seja, a parte acima da diagonal é refletida na parte abaixo da diagonal). Uma matriz A é *anti-simétrica* se $a_{ij} = -a_{ij}$ para toda linha i e toda coluna j (ou seja, a parte acima da diagonal é refletida com sinal trocado na parte abaixo da diagonal, e a diagonal é zero). ♦

Exemplo α.17. A matriz A a seguir é quadrada. C é triangular superior. D é diagonal (e portanto triangular). E é simétrica e F é antisimétrica. G é um vetor coluna, e H é um vetor linha. J é anti-simétrica. B não é classificada de nenhuma dessas formas.

$$A = \begin{pmatrix} 2 & 4 & 6 \\ 8 & 10 & 12 \\ 14 & 16 & 18 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \quad C = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 2 & -2 \\ 0 & 0 & 3 \end{pmatrix} \quad D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

$$E = \begin{pmatrix} 0 & -1 & 1 \\ -1 & 2 & 7 \\ 1 & 7 & 5 \end{pmatrix} \quad F = \begin{pmatrix} 1 & -2 & 5 \\ 2 & 9 & -3 \\ -5 & 3 & 8 \end{pmatrix} \quad G = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} \quad H = \begin{pmatrix} 2 & 3 & 5 & 7 \end{pmatrix}$$

$$J = \begin{pmatrix} 0 & 3 & -1 \\ -3 & 0 & -7 \\ 1 & 7 & 0 \end{pmatrix}$$

◀

Usaremos a notação $\text{diag}(x_1, x_2, \ldots, x_n)$ para a matriz diagonal com elementos $x_1, x_2, \ldots, x_n$ na diagonal.

Exemplo α.18. A matriz $\text{diag}(1, 9, 2)$ é

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 9 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$ ◀

Definição α.19 (Matriz identidade)**.** Uma matriz quadrada onde os elementos da diagonal são iguais a 1 e os outros são iguais a 0 é chamada de *matriz identidade*. Denotamos a identidade por $\mathcal{I}$:

$$\mathcal{I} = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}$$ ♦

Exemplo α.20. As matrizes identidade de ordem 3 e de ordem 4 são mostradas a seguir.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$ ◀

α.2.1 Operações com matrizes

Duas matrizes podem ser somadas e multiplicadas, desde que os elementos das duas admitam as operações de adição e multiplicação, e o número de linhas e colunas permita as operações. Também é possível multiplicar uma matriz por um escalar, desde que seja possível multiplicar o escalar pelos elementos da matriz.

Definição α.21 (Soma de matrizes)**.** Sejam A e B matrizes, ambas $m \times n$. Então $A + B = C$, onde $c_{ij} = a_{ij} + b_{ij}$ – ou seja, cada elemento com coordenada i, j de A é somado com o elemento com coordenada i, j de B resultando no elemento de coordenada i, j em C. ♦

Exemplo α.22.

$$\begin{pmatrix} -1 & 0 & 3 \\ -3 & 2 & 2 \end{pmatrix} + \begin{pmatrix} 1 & -2 & 5 \\ 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 0 & -2 & 8 \\ -2 & 6 & 5 \end{pmatrix}$$ ◀

Exemplo α.23.

$$\begin{pmatrix} 1 & x & 2 \\ 3 & y & 5 \end{pmatrix} + \begin{pmatrix} a & 0 & -1 \\ b & 4 & -1 \end{pmatrix} = \begin{pmatrix} a+1 & x & 1 \\ b+3 & y+4 & 4 \end{pmatrix}$$ ◀

Definição α.24 (Multiplicação de matriz por escalar)**.** Seja A uma matriz cujos elementos pertencem a um corpo F. Seja $c \in F$ um escalar. Entào a multiplicação cA é igual à matriz obtida multiplicando cada elemento de A por c. ♦

Exemplo α.25. Seja $c = 3$ e

$$A = \begin{pmatrix} 0 & 1 & 2 \\ -3 & -4 & -5 \end{pmatrix}.$$

Então

$$cA = \begin{pmatrix} 0 & 3 & 6 \\ -9 & -12 & -15 \end{pmatrix}. \quad \blacktriangleleft$$

Exemplo α.26. Damos um exemplo usando matrizes com elementos em $\mathbb{C}$. Seja $c = 3 + 2i$ e

$$A = \begin{pmatrix} 1 & 0 \\ 2i & 3 - 2i \end{pmatrix}$$

Então

$$cA = \begin{pmatrix} 3 + 2i & 0 \\ -4 + 6i & 13 \end{pmatrix} \quad \blacktriangleleft$$

Definição α.27 (Multiplicação de matrizes)**.** Sejam A uma matriz $m \times p$ e B uma matriz $p \times n$. A multiplicação de A por B, que denotamos AB é a matriz C, $m \times n$, cujas entradas são

$$c_{ij} = \sum_{i=1}^{o} a_{io} b_{oj}. \quad ♦$$

Claramente, para que a multiplicação AB seja possível, o número de colunas de A deve ser igual ao número de colunas de B. Dizemos que neste caso A e B são *compatíveis* para multiplicação. Se A é $m \times p$ e B é $p \times n$, o resultado será uma matriz $m \times n$.

$$A_{m\times p} B_{p\times n} = (AB)_{m\times n}.$$

$$\begin{pmatrix} & \leftarrow\ p\ \rightarrow & \\ \uparrow & & \\ m & & \\ \downarrow & & \end{pmatrix} \begin{pmatrix} & \leftarrow\ n\ \rightarrow & \\ \uparrow & & \\ p & & \\ \downarrow & & \\ & & \end{pmatrix} = \begin{pmatrix} & \leftarrow\ n\ \rightarrow & \\ \uparrow & & \\ m & & \\ \downarrow & & \end{pmatrix}$$

Exemplo α.28. Multiplicamos uma matriz 3×3 por outra, 3×4, obtendo uma nova matriz 3×4.

$$\begin{pmatrix} 5 & 5 & 1 \\ 0 & 1 & 2 \\ 7 & 4 & 8 \end{pmatrix} \begin{pmatrix} 3 & 2 & 4 & 9 \\ 1 & 2 & 1 & 2 \\ 0 & 0 & 1 & -1 \end{pmatrix} = \begin{pmatrix} 20 & 20 & 26 & 54 \\ 1 & 2 & 3 & 0 \\ 25 & 15 & 40 & 63 \end{pmatrix}$$

Este exemplo destaca como cada elemento da nova matriz é calculado: o elemento na posição 2, 3 é calculado usando a linha 2 e a coluna 3:

$$\begin{aligned} c_{23} &= a_{21} b_{31} + a_{22} b_{22} + a_{23} b_{33} \\ &= (0)(4) + (1)(1) + (2)(1) = 3 \end{aligned} \quad \blacktriangleleft$$

Exemplo α.29. Uma mariz multiplicada por um vetor coluna resulta em um vetor coluna com o mesmo número de linhas da matriz.

$$\begin{pmatrix} 1 & 0 \\ 2 & -1 \\ 3 & -2 \end{pmatrix} \begin{pmatrix} 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \\ -1 \end{pmatrix}$$

O mesmo acontece quando um vetor linha é multiplicado por uma matriz – o resultado é um vetor linha com o mesmo número de colunas da matriz. ◀

Exemplo α.30. O produto de linha por coluna de mesmo tamanho sempre resulta em uma matriz com um único elemento:

$$\begin{pmatrix} -1 & 5 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \end{pmatrix}$$

No entanto, a multiplicação de vetor coluna de tamanho m por vetor linha de tamanho n resulta em uma matriz $m \times n$:

$$\begin{pmatrix} 2 \\ 1 \\ -1 \end{pmatrix} \begin{pmatrix} 3 & -2 \end{pmatrix} = \begin{pmatrix} 6 & -4 \\ 3 & -2 \\ -3 & 2 \end{pmatrix}$$ ◀

A multiplicação de uma matriz pela identidade resulta na mesma matriz: $A\mathcal{I} = A$.

Teorema α.31. *A operação de multiplicação de matrizes é* associativa *e* distributiva*:* $A(BC) = (AB)C$ *e* $A(B+C) = AB + AC$*, desde que* AB *e* AC *sejam definidos.*

Demonstração. Quanto à distributividade: suponha, sem perda de generalidade, que A é $m \times p$, e que B e C sejam $p \times n$. Sejam $D = A(B + C)$ e $E = AB + AC$. Então o elemento na posição i, j de F é igual ao elemento na mesma posição de E:

$$\begin{aligned} d_{ij} &= \sum_{i=1}^{p} a_{ip}(b_{pj} + c_{pj}) \\ &= \sum_{i=1}^{p} (a_{ip}b_{pj} + a_{ip}c_{pj}) \\ &= \sum_{i=1}^{p} a_{ip}b_{pj} + \sum_{i=1}^{p} a_{ip}c_{pj} \\ &= e_{ij}. \end{aligned}$$ ■

É importante observar, no entanto, que o produto de matrizes *não* é comutativo. Mesmo quando os produtos AB e BA são bem definidos (ou seja, ambas são quadradas e tem a mesma ordem), pode ser que $AB \neq BA$. Por exemplo, sejam

$$A = \begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 3 \\ -1 & 2 \end{pmatrix}.$$

Então

$$AB = \begin{pmatrix} -2 & 7 \\ 0 & -3 \end{pmatrix}, \quad BA = \begin{pmatrix} -3 & 0 \\ -3 & -2 \end{pmatrix}.$$

Definição α.32 (Potência de matriz)**.** Se A é uma matriz quadrada, então para qualquer inteiro $n > 0$, denotamos

$$A^n = \overbrace{AA\ldots A}^{\substack{n-1 \\ \text{multiplicações}}}.$$

Também definimos que $A^0 = \mathcal{I}$. ♦

Exemplo α.33. Seja

$$A = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}.$$

Então

$$A^2 = AA = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 2 \end{pmatrix}$$

$$A^3 = AA^2 = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 6 \\ 3 & 2 \end{pmatrix}$$

$$A^4 = A^2A^2 = \begin{pmatrix} 3 & 2 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 11 & 10 \\ 5 & 6 \end{pmatrix}$$ ◀

Quando $A = A^2$ (e portanto $A = A^n$ para todo inteiro $n > 0$), dizemos que A é *idempotente*.

Exemplo α.34. A matriz zero e a matriz identidade são idempotentes. ◀

Exemplo α.35. A matriz

$$\begin{pmatrix} 2 & -2 & -4 \\ -1 & 3 & 4 \\ 1 & -2 & -3 \end{pmatrix}$$

é idempotente, porque

$$A^2 = \begin{pmatrix} 2 & -2 & -4 \\ -1 & 3 & 4 \\ 1 & -2 & -3 \end{pmatrix}\begin{pmatrix} 2 & -2 & -4 \\ -1 & 3 & 4 \\ 1 & -2 & -3 \end{pmatrix} = \begin{pmatrix} 2 & -2 & -4 \\ -1 & 3 & 4 \\ 1 & -2 & -3 \end{pmatrix}$$ ◀

Definição α.36 (Transposta)**.** A *transposta* de uma matriz é a matriz onde o elemento na posição i, j é a_{ji}, ou seja, a matriz onde a i-ésima linha passa a ser a i-ésima coluna. Denota-se a transposta de A por A^T. ♦

Alguns textos podem também usar a notação A' para transposta.

Exemplo α.37. A transposta de

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 2 & 3 & 4 \end{pmatrix}$$

é

$$A^T = \begin{pmatrix} 0 & 2 \\ 0 & 3 \\ 1 & 4 \end{pmatrix}$$ ◀

Há alguns fatos evidentes a respeito da transposta:

- A transposta de um vetor coluna é um vetor linha e a de um vetor linha é um vetor coluna.

- A operação de transposição é bijetora.
- A função inversa da transposição é ela mesma: $(A^T)^T = A$.
- A transposição é distributiva sobre a soma de matrizes: $(A + B)^T = A^T + B^T$.
- $(cA)^T = c(A^T)$, para todo escalar c.

O efeito da transposição no produto de duas matrizes já não é imediatamente evidente. O Exercício 325 pede a demonstração do teorema a seguir.

Teorema α.38. *Para matrizes A e B tais que o produto AB seja definido, $(AB)^T = B^T A^T$.*

Definição α.39 (Inversão de matriz)**.** Seja A uma matriz quadrada. Se existe B tal que $AB = BA = \mathcal{I}$, então dizemos que A e B são *inversas* uma da outra. Denota-se a inversa de uma matriz M por M^{-1}. ♦

Exemplo α.40. Seja

$$A = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}.$$

Então

$$A^{-1} = \begin{pmatrix} 0 & 1 \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix},$$

porque

$$AA^{-1} = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \quad \blacktriangleleft$$

Para calcular a inversa de uma matriz A $n \times n$, pode-se escrever $AA^{-1} = \mathcal{I}$, tendo os elementos de A^{-1} como incógnitas. Isso resulta em um sistema linear com n^2 equações e n^2 variáveis.

Exemplo α.41. Neste exemplo mostramos como calcular a inversa da matriz apresentada no exemplo α.40.

$$\begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Naturalmente surge um sistema linear:

$$\begin{aligned} a + 2c &= 1 \\ b + 2d &= 0 \\ a + 0c &= 0 \\ b + 0d &= 1. \end{aligned}$$

A solução para este sistema é

$$\begin{aligned} a = 0, &\quad b = 1, \\ c = \frac{1}{2}, &\quad d = -\frac{1}{2}, \end{aligned}$$

portanto

$$A^{-1} = \begin{pmatrix} 0 & 1 \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix}. \quad \blacktriangleleft$$

Teorema α.42. *Se* A *e* B *são matrizes invertíveis* $n \times n$, AB *é invertível, e* $(AB)^{-1} = B^{-1}A^{-1}$.

Demonstração. Se A e B tem inversas A^{-1} e B^{-1}, então simplesmente verificamos que

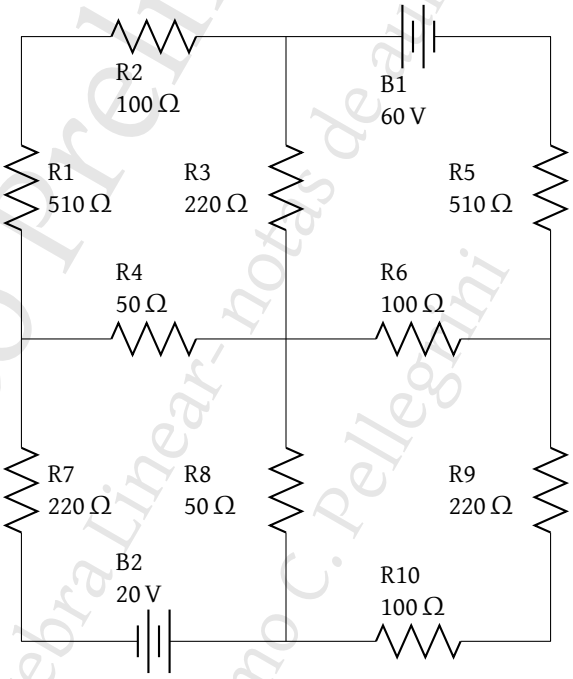
$$\begin{aligned}(AB)(B^{-1}A^{-1}) &= A(BB^{-1})A^{-1} \\ &= A\mathcal{I}A^{-1} \\ &= AA^{-1} \\ &= \mathcal{I}.\end{aligned}$$

■

α.3 Aplicações

α.3.1 Circuitos elétricos [sistemas lineares]

A lei de Kirchoff determina que em qualquer circuito fechado em um circuito elétrico, a soma diferenças de potencial é zero. Considere, por exemplo, o circuito a seguir.



Damos os nomes i_1, i_2, i_3 e i_4 às correntes em quatro ciclos:

i_1 :R1, R2, R3, R4
i_2 :R3, B1, R5, R6
i_3 :R7, R4, R8, B2
i_4 :R8, R6, R9, R10

Suponha que as correntes estão todas no sentido horário (se não estiverem, obteremos resultado negativo, nos indicando o sentido da corrente).

Para determinarmos as correntes, resolvemos o seguinte sistema:

$$\begin{cases} (510+100+220+50)i_1 - 220i_2 - 50i_3 & = 0 \\ -30 + (510+100+220)i_2 - 220i_1 - 100i_4 & = 0 \\ -20 + (220+50+50)i_3 - 50i_1 - 50i_4 & = 0 \\ (50+100+220+100)i_4 - 50i_3 - 100i_2 & = 0 \end{cases}$$

ou, simplificando,

$$\begin{cases} 880i_1 - 220i_2 - 50i_3 & = 0 \\ -220i_1 + 830i_2 - 100i_4 & = 60 \\ -50i_1 + 320i_3 - 50i_4 & = 20 \\ -100i_2 - 50i_3 + 470i_4 & = 0 \end{cases}.$$

Após resolver o sistema, obtemos:

$$\begin{aligned} i_1 &= 0.024428726007575 \\ i_2 &= 0.081759905888709 \\ i_3 &= 0.070201991822999 \\ i_4 &= 0.024864021659619 \end{aligned}$$

Como usamos Volts e Ohms no circuito, as correntes são todas em Ampère.

α.3.2 Balanceamento de equações químicas [sistemas lineares]

É possível produzir amônia a partir de nitrogênio e hidrogênio, como mostrado na equação a seguir.

$$N_2 + H_2 \to NH_3$$

No entanto, as proporções de nitrogênio, hidrogênio e amônia não estão representadas corretamente: à esquerda, temos uma molécula de cada gás, com dois átomos de nitrogênio e dois de hidrogênio. à direita, uma molécula de amônia, com *um* átomo de nitrogênio e *tres* de hidrogênio. Podemos *balancear* esta equação para que represente as quantidades corretas dos reagentes, multiplicamos a quantidade de moléculas de amônia por 2.

$$N_2 + H_2 \to 2NH_3$$

Agora a quantidade de nitrogênio está balanceada, mas há tres vezes mais hidrogênio à direita do que à esquerda. Multiplicamos a quantidade de H_2 por tres, e obtemos a equação balanceada:

$$N_2 + 3H_2 \to 2NH_3$$

Quando há muitos elementos a balancear, torna-se impossível realizar o trabalho usando apenas a intuição. Damos um exemplo ainda pequeno, mas um pouco mais interessante que o anterior, apenas para ilustrar o processo. Suponha que queiramos balancear equação a seguir, que representa a reação de redução onde hidróxido de sódio e ácido sulfúrico tornam-se sulfato de sódio e água:

$$NaOH + H_2SO_4 \to Na_2SO_4 + H_2O.$$

Denominamos as quantidades das moléculas de x_1, x_2, x_3 e x_4:

$$(x_1)NaOH + (x_2)H_2SO_4 \to (x_3)Na_2SO_4 + (x_4)H_2O.$$

Agora, sabemos que as quantidades de átomos de cada elemento não podem se alterar com a reação. Assim, a quantidade de átomos de Oxigenio no lado esquerdo (que é igual a $x_1 + 4x_2$) deve ser a mesma do lado direito (igual a $4x_3 + x_4$). Seguindo este raciocínio para cada um dos quatro elementos da reação, temos

$$\begin{cases} x_1 = 2x_3 & \text{Na} \\ x_1 + 4x_2 = 4x_3 + x_4 & \text{O} \\ x_1 + 2x_2 = 2x_4 & \text{N} \\ x_2 = x_3 & \text{S} \end{cases}$$

Este sistema tem infinitas soluções, da forma

$$\begin{aligned} x_1 &= x_4 \\ x_2 &= x_3 \\ x_1 &= 2x_2 \end{aligned}$$

Escolhemos $x_2 = 1$ e temos a equação balanceada:

$$2NaOH + H_2SO_4 \to Na_2SO_4 + 2H_2O$$

α.3.3 Cadeias de Markov [matrizes]

Suponha que um sistema qualquer possa ficar em um dentre n estados diferentes, que o sistema muda de estado periodicamente com determinadas probabilidades, e que a pobabilidade de mudança de um estado para o próximo só dependa do estado atual.

Exemplo α.43. Por exemplo, um paciente pode estar em n diferentes estágios de uma doença. Suponha que o paciente não esteja sendo tratado (porque não existe tratamento, ou porque não está disponível). Baseado em frequências de casos anteriores, um médico pode determinar a probabilidade do próximo estado do paciente, dado o estado atual. ◀

Exemplo α.44. Máquinas em operação em uma fábrica tem certa probabilidade de apresentar tres tipos de falha a cada dia. A presença de uma falha aumenta a probabilidade de ocorrer outro tipo de falha, portanto a probabilidade de que as outra falhas ocorram depende do estado atual. ◀

Quando o próximo estado de um sistema depende apenas do estado atual, dizemos que vale para ele a *propriedade de Markov*.

Definição α.45 (Cadeia de Markov)**.** Uma *cadeia de Markov*[1] é um processo que pode ser descrito por vários estados, com probabilidades de transição bem definidas entre os estados, para o qual vale a propriedade de Markov: a probabilidade de que o próximo estado seja s' depende somente do estado atual, s, e da probabilidade de transição de s para s'. ♦

[1] Esta definição é simplificada.

Usamos matrizes para representar as probabilidades de mudança de estado em uma cadeia de Markov: o sistema passará do estado i para o estado j com probabilidade p_{ij}.

Suponha que a matriz de probabilidade de mudança de estado seja

$$P = \begin{pmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{pmatrix}$$

Se calcularmos P^2 teremos, por exemplo, na posição p_{21},

$$p'_{21} = p_{23}p_{31} + p_{22}p_{21} + p_{21}p_{11},$$

que é a probabilidade de o sistema começar no estado 2 e terminar no estado 1 após dois estágios:

- $p_{23}p_{31}$, passando de 2 para 3 e de 3 para 1;
- $p_{22}p_{21}$, permanecendo em 2, e depois passando de 2 para 1;
- $p_{21}p_{11}$, passando de 2 para 1 e depois permanecendo em 1.

De maneira geral, a posição p_{ij} na matriz P^k dará a probabilidade de o sistema começad no estado i e mudar, após k estágios, para o estado j. Para calcular as probabilidades de mudança de estado após vários estágios, portanto, calculamos uma potência da matriz.

Por exemplo, suponha que as probabilidades sejam dadas por

$$P = \begin{pmatrix} 0.2 & 0.4 & 0.4 \\ 0.1 & 0.8 & 0.1 \\ 0.5 & 0.2 & 0.3 \end{pmatrix}$$

Então após a troca de estados temos

$$P^2 = \begin{pmatrix} 0.28 & 0.48 & 0.24 \\ 0.15 & 0.7 & 0.15 \\ 0.27 & 0.42 & 0.31 \end{pmatrix},$$

e na segunda troca de estados,

$$P^3 = \begin{pmatrix} 0.224 & 0.544 & 0.232 \\ 0.175 & 0.650 & 0.175 \\ 0.251 & 0.506 & 0.243 \end{pmatrix}$$

E a probabilidade do sistema mudar, depois de duas trocas de estado[2], do estado 3 para o estado 2 é 0.506.

Cadeias de Markov são normalmente abordadas em cursos versando sobre Probabilidade e Processos Estocásticos. O livro de Robert Ash [Ash08], por exemplo, é uma introdução à Probabilidade com um Capítulo sobre Cadeias de Markov.

[2]Na verdade pode-se calcular também o limite da potência P^k quando $k \to \infty$. Para esta matriz, obteremos

$$\lim_{k\to\infty} P^k = \begin{pmatrix} 0.2 & 0.6 & 0.2 \\ 0.2 & 0.6 & 0.2 \\ 0.2 & 0.6 & 0.2 \end{pmatrix}.$$

α.3.4 Sistemas de Votação [matrizes]

É muito conhecido o sistema de votação onde cada eleitor escolhe um candidato, e o candidato que obtiver mais votos é declarado o vencedor da eleição. Este, no entanto, não é o único sistema de votação, e são conhecidos diversos problemas com este sistema – um deles é a possibilidade de se eleger um candidato que não é a preferencia da maioria, e que com a mais alta rejeição dentro todos os candidatos. Isto fica mais claro com um exemplo.

Exemplo α.46. Há dez candidatos em uma eleição, $c_1, c_2, \ldots, c_{10}$, e mil eleitores, $e_1, e_2, \ldots, e_{1000}$.

Suponha que os votos tenham sido como na tabela a seguir.

candidato	votos	candidato	votos
c_1	280	c_6	50
c_2	110	c_7	55
c_3	90	c_8	85
c_4	100	c_9	90
c_5	70	c_{10}	70

Claramente, c_1 venceu a eleição de acordo com os critérios definidos (ele tem a maior quantidade absoluta de votos). No entanto, ele não é a preferencia da maioria, porque há 720 candidatos que não votaram nele, e é possível que dentre esses 720, a rejeição de c_1 seja altíssima. ◀

O Marquês de Condorcet desenvolveu um método alternativo de votação, que permite escolher o candidato com a menor rejeição dentro todos.

Cada eleitor, ao invés de escolher um candidato, determina uma *ordem de preferência* entre todos os candidatos. Assim, um voto poderia ser

$$(c_2, c_{10}, c_8, c_3, c_1, c_4, c_7, c_5, c_6, c_9),$$

representando a escolha "minha primeira opção é c_2; a segunda, c_{10}, ..., e minha última opção é c_9". Neste caso, contabilizamos nove vitória de c_2 (uma sobre cada um dos outros candidatos); oito vitórias de c_{10} (uma sobre cada um dos candidatos à sua direita no voto), e assim por diante.

Vence o candidato que tiver o maior número de vitórias sobre outros, quando considerados par-a-par.

Uma maneira simples de realizar a apuração de eleições deste tipo é representar os votos como matrizes: cada eleitod e_i envia, em sua cédula (supostamente eletrônica), uma matriz A_i. As matrizes A_i são quadradas, e suas linhas e colunas representam os candidatos. O eleitor marcará $+1$ na posição $A_{(i,j)}$ se preferir o candidato c_i ao candidato c_j, e 0 caso contrário. A matriz a seguir, por exemplo, é um voto para uma eleição com tres candidatos (a diagonal não importa, porque não comparamos um candidato com ele mesmo).

$$A_i = \begin{pmatrix} & 0 & +1 \\ +1 & & 0 \\ 0 & +1 & \end{pmatrix}$$

Na linha 1, vemos que o candidato prefere c_1 a c_3, mas prefere c_2 a c_1. A matriz, portanto, representa o voto

$$(c_2, c_1, c_3).$$

Para calcular o total de votos, simplesmente somamos as matrizes,

$$T = \sum_i A_i$$

A matriz T conterá, na posição $T_{(i,j)}$, a quantidade de eleitores que preferem c_i a c_j. Olhando para T, podemos comparar os candidatos dois a dois e declarar o vencedor. Por exemplo, se tivermos os votos

$$\begin{pmatrix} & +1 & 0 \\ 0 & & +1 \\ +1 & 0 & \end{pmatrix}, \quad \begin{pmatrix} & 0 & +1 \\ +1 & & 0 \\ 0 & +1 & \end{pmatrix}, \quad \begin{pmatrix} & 0 & +1 \\ +1 & & +1 \\ 0 & 0 & \end{pmatrix}, \quad \begin{pmatrix} & 0 & 0 \\ +1 & & +1 \\ +1 & 0 & \end{pmatrix}, \quad \begin{pmatrix} & 0 & +1 \\ +1 & & +1 \\ 0 & 0 & \end{pmatrix},$$

a soma das matrizes será

$$T = \begin{pmatrix} & +1 & +3 \\ +4 & & +4 \\ +2 & +1 & \end{pmatrix}$$

Agora, para cada par de candidatos c_i, c_j, verificamos se $T_{ij} > T_{ji}$. Se for, é porque i ganha de j. Assim, temos:

- $T_{12} < T_{21}$, por isso c_2 vence c_1
- $T_{13} > T_{31}$, por isso c_1 vence c_3
- $T_{23} > T_{32}$, por isso c_2 vence c_3

Temos então duas vitórias para c_2, uma para c_1 e nenhuma para c_3. O candidato c_2 é vencedor.

O sistema de votação de Condorcet também apresenta problemas: é possível que não seja possível declarar um vencedor, por exemplo. Apesar disso, é usado por diversos grupos de pessoas.

Uma grande quantidade de sistemas de votação são discutidos, por exemplo, nos livros de Kenneth Arrow[3] [ASS02; ASS10] e de Duncan Black [Bla58].

Exercícios

Ex. 319 — Resolva os sistemas lineares:

$$(a)\begin{cases} 3x_1 - 2x_2 + x_3 = 0 \\ x_1 + x_2 - 5x_3 = 1 \end{cases} \quad (b)\begin{cases} x_1 - x_2 = 4 \\ x_2 + x_3 = 8 \\ -x_1 + x_3 = 3 \end{cases} \quad (c)\begin{cases} 2x_1 - 3x_2 + x_3 - x_4 = 8 \\ x_1 + 2x_2 + x_4 = 9 \\ x_2 + x_3 = 0 \\ -3x_1 + 4x_2 - x_3 - 5x_4 = -7 \end{cases}$$

$$(d)\begin{cases} 2x_1 - x_2 - x_3 = 0 \\ x_1 + 3x_2 + 7x_3 = 1 \\ 6x_1 + 4x_2 + 12x_3 = 2 \end{cases} \quad (e)\begin{cases} 3x_1 + x_2 - x_3 = 1 \\ 2x_2 + 2x_3 = 2 \\ 3x_1 - 4x_2 - x_3 = 3 \end{cases} \quad (f)\begin{cases} -2x_1 + x_2 - x_3 = 1 \\ 5x_1 - 6x_2 + 3x_3 = -5 \\ 6x_1 - 10x_2 + 4x_3 = 7 \end{cases}$$

Ex. 320 — Seja

$$A = \begin{pmatrix} x & 2 & 1 \\ 0 & 0 & 0 \\ 2 & x & 1 \end{pmatrix},$$

com $x \in \mathbb{R}$. Determine B tal que AB seja triangular superior.

Ex. 321 — Dê exemplos de matrizes 2×2 idempotentes, diferentes da identidade e da matriz zero.

[3] Kenneth Arrow ganhou o prêmio Nobel por seu trabalho em sistemas de escolha.

Ex. 322 — Determine a real tal que

$$A = \begin{pmatrix} a & 3 & 3 \\ 2 & 2 & 0 \\ 3 & 3 & a \end{pmatrix}$$

tenha inversa.

Ex. 323 — Seja

$$A = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}.$$

Determine uma fórmula para a matriz A^n, para qualquer n natural.

Ex. 324 — Prove a parte que falta do Teorema α.31.

Ex. 325 — Prove o Teorema α.38.

Ex. 326 — Mostre como usar multiplicação de matrizes 2×2 para realizar soma de inteiros. Para isto, exiba uma família de matrizes 2×2 com a seguinte propriedade: há uma posição fixa nas matrizes que representa o número a ser somado. Se a matriz A contém x naquela posição e B contém y, então AB terá $x + y$ ali.

Ex. 327 — Se quisermos dobrar a corrente i_1 do circuito elétrico em nosso exemplo modificando apenas a bateria B2 por uma outra bateria B3, qual deveria ser a diferença de potencial entre os pólos de B3? Quais passariam a ser os valores das outras correntes (i_2, i_3, i_4)?

Ex. 328 — Se tomarmos um circuito elétrico qualquer formado por resistores e baterias apenas, e determinarmos uma equação descrevendo a corrente em cada ciclo fechado, como fizemos no exemplo neste Capítulo, é possível obter um sistema incompatível? Indeterminado? Explique porque sim ou porque não.

Ex. 329 — Balanceie:

a) $Fe + Cl_2 \to FeCl_3$

b) $KMnO_4 + HCl = KCl + MnCl_2 + H_2O + Cl_2$

c) $PhCH_3 + KMnO_4 + H_2SO_4 = PhCOOH + K_2SO_4 + MnSO_4 + H_2O$

Ex. 330 — Quando descrevemos o uso de matrizes no sistema de votação usando o critério de Condorcet, usamos entradas $+1$ para "prefere" e 0 para "não prefere". Se tivéssemos usado $+1$ e -1 – ou, de maneira mais geral, $+k$ e $-k$, para $k \in \mathbb{N}$, o sistema ainda funcionaria?

Apêndice β

Indução Finita

A técnica de demonstração por indução finita é usada algumas vezes no texto. Este Apêndice desenvolve brevemente esta ferramenta, ilustrando seu uso em alguns exemplos. Apenas a forma fraca de indução é abordada, porque somente ela é usada no texto. Mostramos também como usar indução em objetos não-numéricos, como matrizes.

β.1 Enunciado do Princípio da Indução Finita

Usamos indução finita para demonstrar fatos a respeito dos números naturais. Por exemplo,

- Todo número natural pode ser decomposto em fatores primos.
- Para todo número natural $n > 2$, $2n < 2^n$.
- Para todo número natural n, $\sum_i^n i = n(n+1)/2$

são todas *predicados* $P(n)$:

- $P(n) =$ "n pode ser decomposto em fatores primos"
- $P(n) =$ "$2n < 2^n$"
- $P(n) =$ "$\sum_i^n i = n(n+1)/2$"

Informalmente, o princípio da indução finita é frequentemente comparado a um dominó. Quando queremos provar que alguma afirmação é verdadeira para todo número natural, o princípio da indução finita consiste em

i) Provar que a afirmação é verdadeira para o primeiro número (zero, um, ou algum outro);

ii) Provar que, se a afirmação vale para um natural k, então ela deve valer para $k+1$.

Damos um exemplo trivial. Suponha que a afirmação que queiramos demonstrar é "para todo $n \geq 3$, $2n < 2^n$". Faremos a demonstração *por indução em* n.

Provamos primeiro que

$$2(3) < 2^3,$$

o que é óbvio. A este primeiro caso chamamos de *base de indução.*

Agora *presumimos que a afirmação vale para* k:

$$2k < 2^k$$

A este pressuposto chamamos *hipótese de indução.*

Finalmente, executamos o *passo de indução:* provamos que a afirmação também vale para $k+1$, usando nossa hipótese (de que vale para k):

$$\begin{aligned} 2^{k+1} &= 2(2^k) \\ &= 2^k + 2^k \\ &> 2 + 2^k && (2^k > 2, \text{ para } k > 3) \\ &> 2 + 2k && (2^k > 2k, \text{ pela hipótese!}) \\ &= 2(k+1). \end{aligned}$$

Assim, mostramos que se $2^k > 2k$, então $2^{k+1} > 2(k+1)$. Isto termina nossa demonstração.

Conceitualmente, a indução funciona porque demonstramos um primeiro caso (para $n = 3$) e depois provamos uma implicação que "amarra" todos os outros casos maiores que tres:

$$\begin{aligned} 2(3) &< 2^3 && \text{(base)} \\ 2(4) &< 2^4 && (\text{porque } 2(3) < 2^3 \to 2(4) < 2^4) \\ 2(5) &< 2^5 && (\text{porque } 2(4) < 2^4 \to 2(5) < 2^5) \\ &\vdots \\ 2(n) &< 2^n && (\text{porque } 2(n-1) < 2^{n-1} \to 2(n) < 2^n) \\ &\vdots \end{aligned}$$

Formalizamos agora o princípio da indução finita.

(Princípio da Indução Finita – "indução fraca"). Seja $p(n)$ um predicado a respeito de números naturais (ou seja, $n \in \mathbb{N}$ é argumento do predicado). Se

i) $p(n_0)$ é verdadeiro para algum $n_0 \in \mathbb{N}$;

ii) se para qualquer natural $k > n_0$, a veracidade de $p(k)$ implica na veracidade de $p(k+1)$;

então $p(n)$ é verdadeiro para todo natural $n \geq n_0$.

O item (i) é chamado de *base* de indução. Quando presumimos que $p(k)$ vale, esta é nossa *hipótese de indução.* Ao mostrarmos que $p(k)$ implica em $p(k+1)$, executamos o *passo de indução.* ◊

Há uma segunda forma do princípio da indução finita, mais conveniente em algumas situações. Pode ser eventualmente mais fácil provar que "se a proposição vale para *todo* número menor que n, então vale para n".

Por exemplo, se quisermos demonstrar que $F_n < 2^n$ (onde F_n é o n-ésimo númerode Fibonacci), observamos que F_n é definido usando não apenas F_{n-1}, mas F_{n-2} também. Assim, provamos a base com dois casos:

$$F_0 = 0 < 2^0$$
$$F_1 = 1 < 2^1$$

A hipótese de indução é "para *todo* $k < n$, $F_k < 2^k$". Para realizar o passo, usamos a hipótese para mostrar que $F_n < 2^n$:

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ &< 2^{n-1} + 2^{n-2} && \text{(pela hipótese, } F_{n-1} < 2^{n-1}, F_{n-2} < 2^{n-2}\text{)} \\ &< 2^{n-1} + 2^{n-1} \\ &= 2 \cdot 2^{n-1} \\ &= 2^n. \end{aligned}$$

E assim concluímos a demonstração.

(Princípio da Indução Finita – "indução forte"). Seja $p(n)$ um predicado a respeito de números naturais (ou seja, $n \in \mathbb{N}$ é argumento do predicado). Se

i) $p(n_0)$ é verdadeiro para algum $n_0 \in \mathbb{N}$;

ii) se para qualquer natural $k > n_0$, a veracidade de $p(1), p(2), \ldots, p(k)$ (todos!) implica na veracidade de $p(k+1)$;

então $p(n)$ é verdadeiro para todo natural $n \geq n_0$. ◊

Nas próximas seções damos alguns exemplos de demonstração por indução. A divisão das seções não implica que estas são as únicas áreas ou os únicos modos de usar indução.

β.2 Demonstrações de igualdades e desigualdades simples

Exemplo β.1. Demonstramos por indução a seguinte proposição:

$$2^n < n! \text{ para todo } n > 0.$$

i) **Base:** $2^1 > 1!$

ii) **Hipótese:** $2^k < k!$

iii) **Passo:** Queremos mostrar que, presumindo que se a hipótese de indução vale, temos $2^{k+1} < (k+1)!$. O passo é detalhado a seguir.

$$\begin{aligned} 2^k + 1 &= 2(2^k) \\ &< 2(k!) && \text{(usamos a hipótese de indução)} \\ &\leq (k+1)(k!) && (2 \leq k+1, \text{porque } k > 0) \\ &= (k+1)! \end{aligned}$$

Desta forma, demonstramos a proposição. ◀

Exemplo β.2. Provamos agora que todo número natural maior que um é divisível por algum primo, usando a segunda forma do princípio da indução finita.

i) **Base:** 2 é divisível por si mesmo, e 2 é primo, portanto a afirmação vale para 2

ii) **Hipótese:** "Todo número natural $k < n$ é divisível por algum primo".

iii) **Passo:** Agora consideramos o número n. Há duas possibilidades:

   a) Se n é primo, ele é divisível por si mesmo (um primo).

   b) Se n não é primo, então ele é divisível por dois outros números menores que ele. Mas estes dois outros números, pela hipótese de indução, são divisíveis por primos, e concluímos que n é divisível por algum primo. ◀

Exemplo β.3. Demonstramos a seguir que para qualquer $n > 0$,

$$2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 2.$$

i) **Base:** para $n = 1$, temos$2 = 2^2 - 2$.

ii) **Hipótese:** $2 + 2^2 + 2^3 + \cdots + 2^k = 2^{k+1} - 2$.

iii) **Passo:** Queremos mostrar que, presumindo que se a hipótese de indução vale, temos

$$2 + 2^2 + 2^3 + \cdots + 2^{k+1} = 2^{k+1+1} - 2.$$

O passo é detalhado a seguir.

$$\begin{aligned} 2 + 2^2 + \cdots + 2^k + 2^{k+1} &= \left(2 + 2^2 + \cdots + 2^k\right) + 2^{k+1} \\ &= \left(2^{k+1} - 2\right) + 2^{k+1} && \text{(usamos a hipótese de indução)} \\ &= 2(2^{k+1}) - 2 \\ &= 2^{k+2} - 2. \end{aligned}$$

Provamos assim a proposição. ◀

Exemplo β.4. Mostramos neste exemplo que $9^n - 2^n$ é divisível por 7 para todo inteiro positivo n.

i) **Base:** para $n = 1$, temos trivialmente $9 - 2 = 7$.

ii) **Hipótese:** $9^k - 2^k = 7q$ para algum q natural.

iii) **Passo:**

$$\begin{aligned} 9^{k+1} - 2^{k+1} &= 9(9^k - 2^k) + 2^k(9 - 2) \\ &= 9(9^k - 2^k) + 2^k(7) \\ &= 9(7q) + 2(7) \\ &= 7(9q + 2), \end{aligned}$$

e portanto 7 divide $9^{k+1} - 2^{k+1}$. Isto conclui a demonstração.

◀

Exemplo β.5. Neste exemplo usamos a segunda forma do princípio da indução para mostrar que notas de \$3, e \$7 são suficientes para compor qualquer quantia acima de \$12.

i) **Base:** mostramos inicialmente que podemos compor 12, 13 e 14 com estas notas.
Para $n = 12$, temos trivialmente $3 + 3 + 3 + 3 = 12$.
Para $n = 13$, temos $7 + 3 + 3 = 13$.
Para $n = 14$, temos $7 + 7 = 14$

ii) **Hipótese:** presumimos que todo valor $12 \leq k < n$ pode ser composto por notas de 3 e de 7.

iii) **Passo:** Queremos agora mostrar que $n \geq 15$ também pode ser composto por tais notas. Como $n-3 < n$ e $n \geq 15$, podemos compor $n - 3$ e adicionar uma nota de 3, terminando a demonstração. ◀

Exemplo β.6. Mostramos agora que se $\operatorname{sen}(x) \neq 0$, então para todo $n \in \mathbb{N}$,

$$(\cos x)(\cos 2x)(\cos 4x)\cdots(\cos 2^{n-1}x) = \frac{\sin 2^n x}{2^n \sin x}$$

i) **Base:** Para $n = 1$, temos

$$\cos x = \frac{\operatorname{sen}(2x)}{2\operatorname{sen}(x)},$$

que segue naturalmente de que $\operatorname{sen}(2x) = 2\operatorname{sen}(x)\cos(x)$.

ii) **Hipótese** Presumimos que a proposição vale para k, ou seja,

$$(\cos x)(\cos 2x)(\cos 4x)\cdots(\cos 2^{k-1}x) = \frac{\operatorname{sen} 2^k x}{2^k \operatorname{sen} x}.$$

iii) **Passo:** *Para chegar na forma válida para $k+1$ é interessante mudar um dos lados da equação da hipótese de forma que fique já como queiramos*, assim tomamos a hipótese e multiplicamos os dois lados por $\cos(2^k x)$:

$$(\cos x)(\cos 2x)(\cos 4x)\cdots(\cos 2^k x) = \frac{\operatorname{sen} 2^k x \cos(2^k x)}{2^k \operatorname{sen} x}.$$

O numerador da fração no lado direito é[1]

$$\operatorname{sen} 2^k x \cos(2^k x) = \frac{\operatorname{sen}(2^{k+1}x)}{2},$$

logo temos

$$\begin{aligned}(\cos x)(\cos 2x)(\cos 4x)\cdots(\cos 2^k x) &= \frac{\left(\frac{\operatorname{sen}(2^{k+1}x)}{2}\right)}{2^k \operatorname{sen}(x)} \\ &= \frac{\operatorname{sen}(2^{k+1}x)}{2^{k+1}\operatorname{sen}(x)},\end{aligned}$$

e terminamos a demonstração, porque esta é a forma da proposição para $k+1$. ◀

[1] $\operatorname{sen}(a)\cos(b) = \frac{1}{2}[\operatorname{sen}(a+b) + \operatorname{sen}(a-b)]$.

Exemplo β.7. A função β é definida como

$$\beta(a,b)=\int_0^1 x^{a-1}(1-x)^{b-1}\,dx.$$

para $a,b\in\mathbb{R}_+^*$.

Provamos agora que para um y real qualquer e n natural, $\beta(n,y)=(n!)/(y+1)(y+2)\cdots(y+n+1)$, ou seja,

$$\int_0^1 x^n(1-x)^y\,dx=\frac{n!}{(y+1)(y+2)\cdots(y+n+1)}.$$

Demonstramos por indução em n.

i) **Base:** para $n=0$,

$$\int_0^1 x^0(1-x)^y\,dx=\frac{1}{y+1}=\frac{0!}{y+0+1}$$

ii) **Hipótese:** presumimos que a igualdade vale para $n-1$:

$$\int_0^1 x^{n-1}(1-x)^y\,dx=\frac{(n-1)!}{(y+1)(y+2)\cdots(y+n)}.$$

iii) **Passo:** calculamos o valor para n. Integrando por partes e usando

$$\begin{aligned}u&=x^n\\ dv&=(1-x)^y\,dx\end{aligned}$$

chegamos a

$$\begin{aligned}\int_0^1 x^n(1-x)^y\,dx&=\frac{x^n(1-x)^{y+1}}{y+1}\bigg|_0^1+\frac{n}{y+1}\int_0^1 x^{n-1}(1-x)^{y+1}\,dx\\ &=0+\frac{n}{y+1}\int_0^1 x^{n-1}(1-x)^{y+1}\,dx\\ &=\frac{n}{y+1}\left(\frac{(n-1)!}{(y+1)(y+2)\cdots(y+n)}\right)\qquad\text{(pela hipótese de indução)}\\ &=\frac{n!}{(y+1)(y+2)\cdots(y+n+1)},\end{aligned}$$

o que conclui a demonstração. ◀

β.3 Indução dupla

Podemos também usar *indução dupla,* quando tivermos uma proposição $P(m,n)$ a ser demonstrada.

Exemplo β.8. Seja f uma função de dois argumentos inteiros, definida a seguir:

$$\begin{aligned} f(1,1) &= 2 \\ f(m+1,n) &= f(m,n) + 2(m+n) \\ f(m,n+1) &= f(m,n) + 2(m+n-1) \end{aligned}$$

Provaremos que para $m, n \geq 1$,

$$f(m,n) = (m+n)^2 - (m+n) - 2n + 2.$$

i) **Base:**

$$\begin{aligned} (1+1)^2 - (1+1) - 2(1) + 2 &= 2^2 - 2 - 2 + 2 \\ &= 2 \\ &= f(1,1) \end{aligned}$$

ii) **Passo (m):** Nossa hipótese é de que para qualquer n fixo,

$$f(m-1,n) = (m-1+n)^2 - (m-1+n) - 2n + 2.$$

Agora calculamos $f(m,n)$, usando a hipótese:

$$\begin{aligned} f(m,n) &= f([\mathbf{m-1}]+1, n) \\ &= f(\mathbf{m-1}, n) + 2(\mathbf{m-1}+n) \\ &= f(m-1,n) + 2m - 2 + 2n \\ &= \Big((m-1+n)^2 - (m-1+n) - 2n + 2\Big) + 2m - 2 + 2n \qquad \text{(hipótese de indução)} \\ &= (m-1+n)^2 - (m-1+n) + 2m \\ &= (m-1+n)^2 + m - n + 1 \\ &= (m^2 + n^2 + 2mn - 2n - 2m + 1) + m - n + 1 \\ &= (m+n)^2 - 2n - 2m + m + n + 2 \\ &= (m+n)^2 - (m+n) + 2. \end{aligned}$$

E demonstramos o passo para a variável m.

iii) **Passo (n):** Nosas hipótese é de que para qualquer m fixo,

$$f(m,n-1) = (m+n-1)^2 - (m+n-1) - 2(n-1) + 2.$$

calculamos $f(m,n)$, usando a hipótese.

$$\begin{aligned} f(m,n) &= f(m, [\mathbf{n-1}]+1) \\ &= f(m, [\mathbf{n-1}]) + 2(m + [\mathbf{n-1}] - 1) \\ &= f(m, [\mathbf{n-1}]) + 2m + 2n - 4 \\ &= \Big((m+n-1)^2 - (m+n-1) - 2(n-1) + 2\Big) + 2m + 2n - 4 \end{aligned}$$

(hipótese de indução)

$$
\begin{aligned}
&= (m+n-1)^2 - m - n + 1 - 2n - 2 + 2 + 2m + 2n - 4 \\
&= (m+n-1)^2 + m - n - 3 \\
&= (m^2 + n^2 + 2mn - 2n - 2m + 1) + m - n - 3 \\
&= m^2 + n^2 + 2mn - (n+m) - 2 \\
&= (m+n)^2 - (m+n) + 2.
\end{aligned}
$$

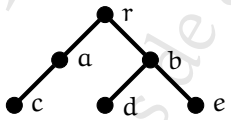
Desta forma, usando passos separados para m e n, mostramos a validade da fórmula. ◀

β.4 Indução em estruturas

Exemplo β.9. Definimos informalmente neste exemplo as árvores. Para uma definição mais formal veja no capítulo um o exemplo 1.41 (pág 20), e observe que uma árvore é um grafo onde não há ciclos e onde qualquer vértice á alcançavel por outros por arestas.

Uma árvore é um conjunto de vértices, que representamos graficamente como pontos, e um conjunto de arestas, que repersentamos graficamente como linhas ligando estes pontos.

A figura a seguir mostra uma árvore.



Os nós (vértivces) da árvore são a, b, c, d, e, r.

Uma árvore é chamada de *binária* se cada nó tem exatamente um ou tres vizinhos – como é o caso deste exemplo. Um nó que só tem um vizinho é chamado de *folha*. As folhas da árvore na figura são c, d, e.

Em uma árvore, normalmente marcamos um vértice "especial" e o chamamos de *raiz*.

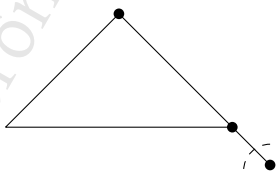
Provaremos que em qualquer árvore binária, $v = e + 1$, onde v é o número de vértices e e é o número de arestas.

i) **Base:** Um único vértice isolado é uma árvore binária. Temos $v = e + 1$, já que $v = 1$ e $e = 0$.

ii) **Hipótese:** Presumimos que a proposição vale para v, ou seja, uma árvore com v vértices tem $v = e+1$ vértices

iii) **Passo:** Tome uma árvore qualquer com $v' = v+1$ vértices. (Denotaremos os vértices e arestas desta nova árvore por v' e e').

Retiramos uma folha da árvore. Necessariamente, retiramos também uma aresta.



O resultado é uma árvore com v vértices, e portanto com $e = v - 1$ arestas. Ao recolocar o vértice e arestas removidos, temos $v' = v + 1$ vértices e $e' = v$ arestas. Logo,

$$v' = e' + 1.$$

Como este procedimento vale paar qualquer árvore com $v + 1$ vértices, a demonstração está concluída. ◀

β.5 Indução em Geometria

Exemplo β.10. Provaremos que o número de regiões definidas por n retas no plano, sendo que não há retas paralelas e não há mais de duas retas se interceptando no mesmo ponto, é

$$\frac{n^2 + n}{2} + 1.$$

i) **Base:** com nenhuma linha, temos uma única região, e

$$\frac{0^2 + 0}{2} + 1 = 1,$$

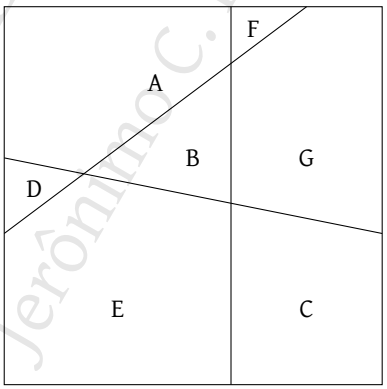
logo a proposição é válida para zero linhas.

ii) **Hipótese:** suponha que com n linhas dividimos o plano em no máximo

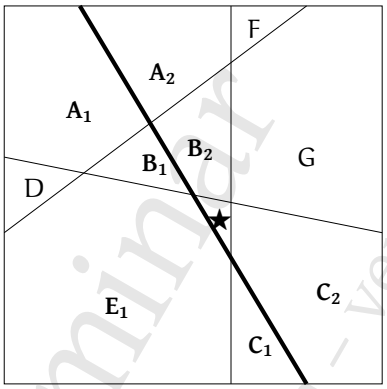
$$\frac{n^2 + n}{2} + 1$$

regiões.

ii) **Passo:** suponha que o plano tenha sido dividido por n linhas em $\frac{n^2+n}{2} + 1$ regiões. Ao adicionar a $n + 1$-ésima linha, ela deverá cruzar com todas as outras (senão haveria linhas paralelas), e estes cruzamentos são todos distintos (senão haveria pontos com mais de duas linhas se cruzando).



Estes novos cruzamentos dividem portanto a nova linha em $k+1$ segmentos, cada um destes segmentos em uma das $\frac{n^2+n}{2}+1$ regiões formadas anteriormente, como ilustra a figura a seguir para o caso[2] em que $k=3$ (a estrela marca a região E_2).



Cada um destes segmentos divide sua região em duas, e portanto adicionamos $k+1$ regiões. Temos portanto

$$\frac{n^2+n}{2}+1+(n+1)$$

regiões. Rearranjando a expressão, vemos que temos

$$\frac{(n+1)^2+(n+1)}{2}+1$$

regiões – que é a forma que queríamos para $n+1$. ◀

Exemplo β.11. Provaremos que o número de diagonais em um polígono convexo com n lados é

$$\frac{n(n-3)}{2},$$

quando $n \geq 3$.

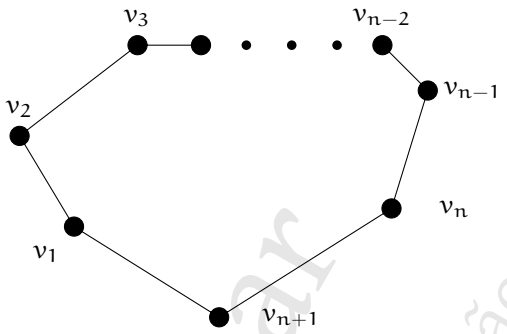
i) **Base:** Um triângulo tem tres lados e nenhuma diagonal. A fórmula está correta para triangulos, já que

$$\frac{n(n-3)}{2}=\frac{3(3-3)}{2}=\frac{0}{2}=0.$$

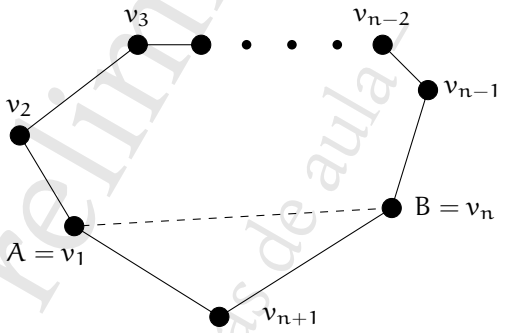
ii) **Hipótese:** Presumimos que todo polígono convexo com n lados tem $\frac{n(n-3)}{2}$ diagonais.

iii) **Passo:** Tome um polígono convexo qualquer con $n+1$ lados.

[2] A figura é ilustrativa, mas não é essencial para a demonstração, em especial porque trata somente do caso $k=3$, e o argumento neste momento é de *qualquer* k para $k+1$.

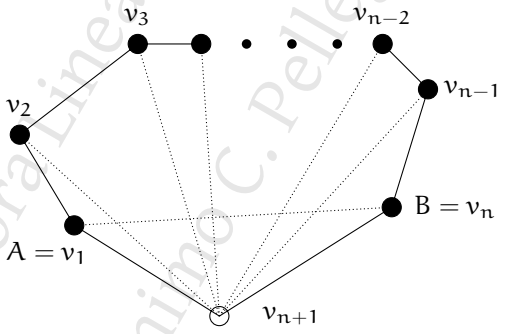


Escolha dois vértices A e B tais que, quando traçamos a diagonal AB, o polígono fica dividido em um triângulo e um outro polígono convexo com n lados.



O polígono original, de $n+1$ lados, tem todas as diagonais do polígono menor. Mas ele tem também:

- A diagonal AB, que transformamos em aresta;
- As $n-2$ diagonais que incidem no vértice que foi isolado por AB.



Assim, a quantidade de diagonais do polígono com $n+1$ lados é

$$\overbrace{\frac{n(n-3)}{2}}^{\text{valor para } n} + 1 + (n-2) = \frac{n(n-3)}{2} + n - 1$$

$$
\begin{aligned}
&= \frac{n(n-3)+2(n-1)}{2} \\
&= \frac{(n^2-3n)+(2n-2)}{2} \\
&= \frac{(n^2-n+2)}{2} \\
&= \frac{(n-1)(n+2)}{2} \\
&= \frac{(n-1)(3(n-1))}{2},
\end{aligned}
$$

exatamente a mesma fórmula, para $n+1$. ◀

β.6 Indução em número de operações com matriz

Exemplo β.12. Podemos usar indução finita também em demonstrações envolvendo matrizes. Mostraremos que

$$\begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}^n = \begin{pmatrix} n+1 & n \\ -n & -n+1 \end{pmatrix}$$

i) **Base:** Para $n = 1$, trivialmente,

$$\begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}^1 = \begin{pmatrix} 1+1 & 1 \\ -1 & -1+1 \end{pmatrix}.$$

ii) **Hipótese:**

$$\begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}^k = \begin{pmatrix} k+1 & k \\ -k & -k+1 \end{pmatrix}$$

iii) **Passo:** Queremos mostrar que, presumindo que a hipótese de indução vale, temos

$$\begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}^{k+1} = \begin{pmatrix} (k+1)+1 & (k+1) \\ -(k+1) & -(k+1)+1 \end{pmatrix} = \begin{pmatrix} k+2 & k+1 \\ -k-1 & -k \end{pmatrix}.$$

Detalhamos portanto o passo.

$$
\begin{aligned}
\begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}^{k+1} &= \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}^k \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} && (A^{k+1} = A^k A) \\
&= \begin{pmatrix} k+1 & k \\ -k & -k+1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} && \text{(usamos a hipótese de indução)} \\
&= \begin{pmatrix} k+2 & k+1 \\ -k-1 & -k \end{pmatrix}. && \text{(após multiplicar)}
\end{aligned}
$$

Demonstramos, portanto, a proposição.

Na verdade, poderíamos ter demonstrado para qualquer $n \geq 0$, porque para qualquer matriz A, $A^0 = \mathcal{I}$.

É vácil verificar também que o resultado vale para $n < 0$: basta multiplicar

$$\begin{pmatrix} n+1 & n \\ -n & -n+1 \end{pmatrix} \begin{pmatrix} -n+1 & -n \\ n & n+1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \qquad \blacktriangleleft$$

β.7 Indução em ordem de matriz quadrada

Exemplo β.13. Toda matriz quadrada A sem zeros na diagonal pode ser decomposta em BC, sendo B triangular inferior e C triangular superior.

Procedemos por indução na ordem da matriz.

i) **Base:** quando $n = 1$, temos $A = (a)$, e $A = (1)(a)$, trivialmente.

ii) **Hipótese:** Presumimos que qualquer matriz quadrada X de ordem $n - 1$ pode ser decomposta em YZ, com Y triangular inferior e Z triangular superior.

iii) **Passo:** Temos A de ordem n, que particionamos em blocos, separando a primeira linha e primeira coluna.

$$A = \begin{pmatrix} a_{11} & \mathbf{l}^T \\ \mathbf{c} & R \end{pmatrix},$$

onde $\mathbf{l}$ é um vetor linha com $n-1$ elementos; $\mathbf{c}$ é vetor coluna com $n-1$ elementos; e R é uma matriz quadrada de ordem $n-1$. Também supomos, *usando a hipótese de indução* que $R = MN$, com M triangular inferior e N triangular superior.

Observe que podemos dividir pode a_{11}, porque presumimos que A não tem zeros na diagonal.

A matriz $MN - \frac{\mathbf{c}\mathbf{l}^T}{a_{11}}$ também pode ser decomposta em X e Y triangulares, da mesma forma, portanto seja

$$XY = MN - \frac{1}{a_{11}}\mathbf{c}\mathbf{l}^T,$$

de forma que

$$MN = XY + \frac{1}{a_{11}}\mathbf{c}\mathbf{l}^T.$$

Sejam B e C definidas a seguir

$$B = \left(\begin{array}{c|c} a_{11} & \mathbf{0}^T \\ \hline \mathbf{c} & X \end{array}\right) \quad C = \left(\begin{array}{c|c} 1 & \frac{1}{a_{11}}\mathbf{l}^T \\ \hline \mathbf{0} & Y \end{array}\right),$$

Temos então

$$\begin{aligned} BC &= \left(\begin{array}{c|c} a_{11} & \mathbf{0}^T \\ \hline \mathbf{c} & X \end{array}\right) \left(\begin{array}{c|c} 1 & \frac{1}{a_{11}}\mathbf{l}^T \\ \hline \mathbf{0} & Y \end{array}\right) \\ &= \left(\begin{array}{c|c} a_{11}+0 & a_{11}\frac{1}{a_{11}}\mathbf{l}^T + \mathbf{0} \\ \hline \mathbf{c}+\mathbf{0} & XY + \frac{1}{a_{11}}\mathbf{c}\mathbf{l}^T \end{array}\right) \end{aligned}$$

$$= \left(\begin{array}{c|c} a_{11} & l^T \\ \hline c & MN \end{array}\right)$$
$$= A.$$

Assim, decompusemos A usando a decomposição de R, que era uma matriz de ordem $n-1$. ◀

β.8 Demonstração de corretude de algoritmos

É comum provar por indução que um algoritmo retorna o resultado correto.

Exemplo β.14. O seguinte algoritmo pode ser usado para elevar um número qualquer a uma potência natural:para calcular $\text{pot}(b,k)$,

- se $k = 0$ retorne 1
- se k é ímpar retorne $b \cdot \text{pot}(b, k-1)$
- se k é par, retorne $b^2 \cdot \text{pot}(b, k/2)$

A seguir demonstramos, por indução no expoente, que o algoritmo sempre calculará b^k.

- **Base:** para $k = 0$, o algoritmo corretamente retorna 1.
- **Hipótese:** presumimos que para todo $k < n$, $\text{pot}(b,k)$ retorna corretamente b^k.
- **Passo:** Quando o algoritmo é usado para calcular b^n, há duas possibilidades:

  i) n é ímpar:

$$\begin{aligned} \text{pot}(b,n) &= b\,\text{pot}(b,n-1) \\ &= bb^{n-1} && \text{(pela hipótese de indução)} \\ &= b^n \end{aligned}$$

  ii) n é par:

$$\begin{aligned} \text{pot}(b,n) &= b^2\,\text{pot}(b,n/2) \\ &= b^2 b^{n/2} && \text{(pela hipótese de indução)} \\ &= b^n \end{aligned}$$

E com isto demonstramos que o algoritmo está correto. ◀

Exemplo β.15. Queremos determinar se um número binomial $\binom{m}{n}$ é par ou ímpar; chamamos esta função de $f(m,n)$, tal que

$$f(m,n) = \begin{cases} 1 & \text{se } \binom{m}{n} \text{ é ímpar} \\ 0 & \text{se } \binom{m}{n} \text{ é par.} \end{cases}$$

Podemos calcular o número binomial e verificar o resto da divisão por dois. Para isto teríamos que computar

$$\begin{aligned}\binom{m}{n} &= \frac{m!}{n!(m-n)!}\\ &= \frac{1\cdot 2\cdot 3\cdots m}{n![1\cdot 2\cdot 3\cdots (m-n)]}\\ &= \frac{m(m-1)(m-2)\cdots(m-n+1)}{n!}\\ &= \frac{m(m-1)(m-2)\cdots(m-n+1)}{1\cdot 2\cdot 3\cdots n},\end{aligned}$$

realizando $m-n-1$ multiplicações no numerador, $n-2$ multiplicações no denominador (totalizando $m-3$ multiplicações), uma divisão para obter o valor de $\binom{m}{n}$ e mais uma divisão por dois para obter a paridade.

Há uma maneira mais eficiente de determinar a paridade de números binomiais, necessitando apenas de $4\lfloor \log_2 n\rfloor$ divisões[3] por 2, e nenhuma multiplicação.

Por exemplo, para $\binom{1000001}{2112}$ o primeiro método precisa de $1000001-3 = 999998$ multiplicações, e o método que dscreveremos a seguir usa apenas $4\lfloor \log_2 2112\rfloor = 44$ divisões.

Suponha $m, n \in \mathbb{N}$, e que a função $f(m,n)$, é computada de acordo com o seguinte algoritmo:

- se $n = 0$ retorne 1
- senão, se m é par e n ímpar, retorne 0
- senão, retorne $f(\lfloor m/2\rfloor, \lfloor n/2\rfloor)$

Damos dois exemplos de uso do algoritmo. Primeiro calculamos

$$\begin{aligned}f(991,12) &= f(495,6)\\ &= f(247,3)\\ &= f(123,1)\\ &= (61,0)\\ &= 1. \qquad (n=0)\end{aligned}$$

Realmente,

$$\binom{991}{12} = 1751905219023893762873161845,$$

ímpar.

Agora calculamos

$$\begin{aligned}f(791,33) &= f(395,16)\\ &= f(197,8)\\ &= f(98,4)\\ &= f(49,2)\end{aligned}$$

[3] Em computadores, a divisão por dois pode ser implementada de maneira mais rápida que outras divisões e multiplicações.

$$\begin{aligned} &= f(24,1) \\ &= 0 \qquad (m \text{ par, } n \text{ ímpar}) \end{aligned}$$

De fato,

$$\binom{791}{8} = 25538103034701028903784191930670086104508663600436238803720,$$

par.

Provaremos que este algoritmo calcula corretamente $f(m,n)$.

A demonstração *não* é em m ou em n, e sim na quantidade de repetições feitas pelo algoritmo. Presumiremos que o algoritmo calcula corretamente a paridade para todos binomiais $\binom{p}{q}$, com $p < m$ e $q < n$, e com isto provaremos que oa paridade de $\binom{m}{n}$ é calculada corretamente.

i) **Base:** quando $n = 0$, o algoritmo retorna um. Isto está claramente correto, já que

$$\binom{m}{0} = 1,$$

ímpar.

Ainda como parte da basae de indução, temos todos os casos em que m é par e n ímpar, e algoritmo retorna zero determinando que $\binom{m}{n}$ é par. Isto está correto, porque

$$n\binom{m}{n} = m\binom{m-1}{n-1}.$$

Como o lado direito é par, o esquerdo deve ser. Mas se k é ímpar, então $\binom{m}{n}$ é par!

ii) **Hipótese:** presumimos que $f(p,q)$ para retorna corretamente a paridade para $\binom{p}{q}$, para $p < m$, $q < n$.

iii) **Passo:** Como temos dois números naturais (m e n) envolvidos no passo, e estamos interessados na paridade do número binomial, faz sentido dividir a demonstração em quatro partes – uma para cada possível combinação de paridades de m e n:

I)	$f(2a, 2b)$,	ambos pares
II)	$f(2a+1, 2b)$	m ímpar, n par
III)	$f(2a, 2b+1)$	n par ,m ímpar
IV)	$f(2a+1, 2b+1)$	ambos ímpares

Estes casos correspondem a dois pares, um ímpar e um par, um par e um ímpar, e dois ímpares.

I) Neste caso temos m e n pares. Expandimos o coeficiente binomial $\binom{m}{n}$:

$$\begin{aligned} \binom{m}{n} &= \frac{m!}{n!(m-n)!} \\ &= \frac{1 \cdot 2 \cdot 3 \cdots m}{n![1 \cdot 2 \cdot 3 \cdots (m-n)]} \end{aligned}$$

$$
\begin{aligned}
&= \frac{m(m-1)(m-2)\cdots(m-n+1)}{n!} \\
&= \frac{m(m-1)(m-2)\cdots(m-n+1)}{1\cdot 2\cdot 3\cdots n} \\
&= \left(\frac{(m-1)(m-3)\cdots(m-n+1)}{1\cdot 3\cdot 5\cdots(n-1)}\right)\left(\frac{m(m-2)(m-4)\cdots(m-n+2)}{2\cdot 4\cdot 6\cdots(n)}\right) \\
&\qquad\qquad \text{(separamos fatores pares e ímpares)} \\
&= \left(\frac{(m-1)(m-3)\cdots(m-n+1)}{1\cdot 3\cdot 5\cdots(n-1)}\right)\left(\frac{m(m-2)(m-4)\cdots(m-n+2)}{2(1)\cdot 2(2)\cdot 2(3)\cdots 2(n/2)}\right) \\
&\qquad\qquad \text{(o denominador tem } n/2 \text{ fatores pares; fatoramos o 2)} \\
&= \left(\frac{(m-1)(m-3)\cdots(m-n+1)}{1\cdot 3\cdot 5\cdots(n-1)}\right)\left(\frac{m(m-2)(m-4)\cdots(m-n+2)}{2^{\frac{n}{2}}1\cdot 2\cdot 3\cdots n/2}\right) \\
&= \left(\frac{(m-1)(m-3)\cdots(m-n+1)}{1\cdot 3\cdot 5\cdots(n-1)}\right)\left(\frac{2^{\frac{m}{2}}\cdot 2(\frac{m}{2}-1)\cdot 2(\frac{m}{2}-2)\cdots 2(\frac{m-n}{2}+1)}{2^{\frac{n}{2}}1\cdot 2\cdot 3\cdots n/2}\right) \\
&\qquad\qquad \text{(o numerador tem } n/2 \text{ pares; fatoramos o 2)} \\
&= \left(\frac{(m-1)(m-3)\cdots(m-n+1)}{1\cdot 3\cdot 5\cdots(n-1)}\right)\left(\frac{2^{\frac{n}{2}}\cdot\frac{m}{2}\cdot(\frac{m}{2}-1)\cdot(\frac{m}{2}-2)\cdots(\frac{m-n}{2}+1)}{2^{\frac{n}{2}}1\cdot 2\cdot 3\cdots n/2}\right) \\
&= \left(\frac{(m-1)(m-3)\cdots(m-n+1)}{1\cdot 3\cdot 5\cdots(n-1)}\right)\frac{2^{\frac{n}{2}}}{2^{\frac{n}{2}}}\left(\frac{\frac{m}{2}(\frac{m}{2}-1)\cdot(\frac{m}{2}-2)\cdots(\frac{m-n}{2}+1)}{1\cdot 2\cdot 3\cdots n/2}\right) \\
&= \underbrace{\frac{(m-1)(m-3)\cdots(m-n+1)}{1\cdot 3\cdot 5\cdots(n-1)}}_{\text{ímpar}}\binom{m/2}{n/2}.
\end{aligned}
$$

Como multiplicação por ímpar não muda a paridade de um número, então

$$\binom{m}{n} \text{ tem a mesma paridade de } \binom{m/2}{n/2}.$$

Sendo ambos pares, temos

$$\begin{aligned} \lfloor m/2 \rfloor &= m/2 \\ \lfloor n/2 \rfloor &= n/2. \end{aligned}$$

Usamos a hipótese de indução, que nos diz que o algoritmo calcula corretamente $f(m/2, n/2)$, e concluimos esta parte da demonstração.

II) Temos m ímpar e n par. Usaremos a identidade

$$\binom{x}{y} = \binom{x}{x-y}.$$

nesta demonstração. Esta identidade implica que

$$(m-n)\binom{m}{n} = (m-n)\binom{m}{m-n}, \text{ e}$$

$$m\binom{m-1}{m-n-1} = m\binom{m-1}{n}.$$

Também podemos usar a identidade

$$(x-y)\binom{x}{x-y} = x\binom{x-1}{x-y-1}.$$

para concluir que

$$(m-n)\binom{m}{n} = m\binom{m-1}{n}.$$

Como $m-n$ e m são ambos ímpares,

$$\binom{m}{n} \text{ tem a mesma paridade de } \binom{m-1}{n}.$$

Aplicamos o caso (I) na expressão do lado direito, e temos que

$$\binom{m}{n} \text{ tem a mesma paridade de } \binom{\lfloor (m-1)/2 \rfloor}{\lfloor n/2 \rfloor}.$$

Como m é ímpar, $\lfloor (m-1)/2 \rfloor$ é o mesmo que $\lfloor m/2 \rfloor$, e *usamos a hipótese de indução, que nos diz que o algoritmo calcula corretamente* $f(m/2, n/2)$, para concluir que a paridade é calculada corretamente neste caso.

III) este caso é trivial, porque é nossa base de indução. O algoritmo nunca chegaria a calcular $f(\lfloor m/2 \rfloor, \lfloor n/2 \rfloor)$ nete caso, porque teria terminado antes e retornado 0.

IV) quando tanto m como n são ímpares, observamos que

$$n\binom{m}{n} = m\binom{m-1}{n-1}. \tag{β.1}$$

Como m e n são ímpares, e a multiplicação por ímpar não altera a paridade de um número, temos que a paridade de $\binom{m}{n}$ é a mesma que a de $\binom{m-1}{n-1}$.
Agora, como m e n são ímpares,

$$\begin{aligned} m-1 &= 2\lfloor m/2 \rfloor \\ n-1 &= 2\lfloor n/2 \rfloor, \end{aligned} \tag{β.2}$$

temos que

$$\begin{aligned}
\binom{m}{n} &\text{ tem a mesma paridade de } \binom{m-1}{n-1} && \text{(por β.1)} \\
\binom{m-1}{n-1} &\text{ tem a mesma paridade de } \binom{2\lfloor m/2 \rfloor}{2\lfloor n/2 \rfloor} && \text{(por β.2)} \\
\binom{2\lfloor m/2 \rfloor}{2\lfloor n/2 \rfloor} &\text{ tem a mesma paridade de } \binom{\lfloor m/2 \rfloor}{\lfloor n/2 \rfloor} && \text{(semelhante ao caso (I))}
\end{aligned}$$

Usamos novamente a hipótese de indução, ao presumir que o algoritmo calcula corretamente $f(\lfloor m/2 \rfloor, \lfloor n/2 \rfloor)$, para finalizar esta parte a damonstração.

Concluímos aqui a prova de corretude do algoritmo. ◀

β.9 Indução para trás, com base infinita

Uma outra forma de indução consiste em provar que o teorema é válido para uma quantidade infinita de números naturais (mas não para todos); e depois provar que se valepara n, vale para $n-1$.

Exemplo β.16. Provaremos que a média geométrica de n números positivos é sempre menor que a média aritmética.

A prova será feita da seguinte maneira:

Base (I): provaremos que o teorema vale para dois números;

Base (II): provaremos por indução que o teoerma vale para 2^k números;

Passo: provaremos *por indução para trás* que se o teorema vale para todo natural– ou seja, se vale para k, então vale para $k-1$.

Note que provaremos uma base infinita (que neste caso consiste nas potencias de dois):

e depois faremos indução "para trás".

Seja n um número natural *qualquer*. Certamente há uma potência de dois mairo que n (por exemplo, 2^n. Como a base nos garante que o teorema vale para 2^n, e o passo garante que vale para todo número menor que 2^n, vale para n.

i) **Base (I):** Para $n = 2$, partimos do enunciado do teorema para chegar a uma tautologia:

$$\begin{aligned}\left(\frac{x+y}{2}\right)^2 &\geq \sqrt{xy}\\ \frac{x^2+2xy+y^2}{4} &\geq xy\\ x^2+2xy+y^2 &\geq 4xy\\ x^2-2xy+y^2 &\geq 0\\ (x-y)^2 &\geq 0\end{aligned}$$

Como $(x-y)^2$ é ≥ 0 para quaisquer x e y, provamos o caso $n = 2$.

ii) **Base (II):**

$$\begin{aligned}\frac{a_1+a_2+\ldots+a_{2^{k+1}}}{2^{k+1}} &= \frac{1}{2}\left(\frac{a_1+a_2+\ldots+a_{2^k}}{2^k}+\frac{a_{2^k+1}+a_{2^k+2}+\ldots+a_{2^{k+1}}}{2^k}\right)\\ &\geq \frac{1}{2}\left(\sqrt[2^k]{a_1a_2\cdots a_{2^k}}+\sqrt[2^{k+1}]{a_{2^k+1}a_{2^k+2}\cdots a_{2^{k+1}}}\right)\\ &\qquad\qquad\text{(hipótese de indução)}\\ &\geq \sqrt[2^{k+1}]{a_1a_2\cdots a_{2^{k+1}}}\qquad\text{(segue do caso } n=2)\end{aligned}$$

iii) **Passo:** Supomos que a proposição vale para k variáveis, que denotamos $a_1, \ldots, a_{k-1}$. Adicionamos uma nova variável, igual à media das outras:

$$b = \frac{a_1 + a_2 + \cdots a_{k-1}}{k-1}.$$

Pela hipótese de indução, a proposição vale para $a_1, a_2, \ldots, a_k, b$:

$$\begin{aligned}
\frac{a_1 + a_2 + \cdots + a_{k-1} + \frac{a_1+a_2+\cdots+a_{k-1}}{k-1}}{k} &\geq \sqrt[k]{a_1 a_2 \cdots a_{k-1} \left(\frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1}\right)} \\
\frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1} &\geq \sqrt[k]{a_1 a_2 \cdots a_{k-1} \left(\frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1}\right)} \\
\left(\frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1}\right)^k &\geq a_1 a_2 \cdots a_{k-1} \left(\frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1}\right) \\
\left(\frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1}\right)^{k-1} &\geq a_1 a_2 \cdots a_{k-1} \\
\frac{a_1 + a_2 + \cdots + a_{k-1}}{k-1} &\geq \sqrt[k-1]{a_1 a_2 \cdots a_{k-1}},
\end{aligned}$$

que é a forma para $k-1$. ◀

★ β.10 Indução em $\mathbb{R}$

No início deste Capítulo, observamos que o princípio da indução finita é usado em demonstrações de validade de predicados sobre $\mathbb{N}$ – ou seja, para demonstrar fatos da forma "para todo natural n, $P(n)$ é verdade" É natural questionar se o princípio da indução pode ser adaptado para proposições $P(x)$, onde x pertence a $\mathbb{R}$. Nesta seção trataremos de proposições a respeito de intervalos reais (ou seja, as do tipo "para todo $x \in [a, b]$, $P(x)$".

O princípio da indução fraca exige que possamos estabelecer um "primeiro" x, e para cada x deve haver um "sucessor imediato". Esta é exatamente a estrutura dos naturais. Podemos também usar indução em racionais, usando passos diferentes para o numerador e o denominador. Mas para reais, precisamos do princípio da indução forte (ou indução completa).

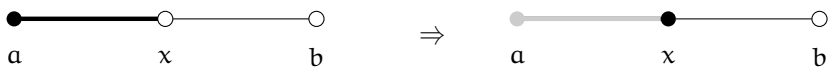
O princípio da indução forte, no entanto, não serve para demonstrações sobre reais – ao menos não como o descrevemos, porque como a discussão a seguir deverá tornar claro não bastam apeans "uma base e um passo".

Suponha que queiramos demonstrar que $P(x)$ vale para todo x em um intervalo $[a, b] \subset \mathbb{R}$.

i) Precisamos que a proposição valha para a – (isto é semelhante à base de indução finita);

ii) A validade da proposição em todo real menor que x, deve implicar na validade para x – ou seja, a validade em num intervalo *aberto em* x, $[a, x)$, implica[4] na validade para x.

[4] Na figura, a seta ⇒ é sinônimo de "implica em".



No entanto, Isto apenas não é suficiente. Suponha que tenhamos provado que $P(0)$ vale e que a validade *em um intervalo* implica na validade para x, ainda falta mostrar que a proposição vale para alguém à frente de x (de outra forma não teríamos a "validade no intervalo" a que se refere o item (ii). Assim, precisamos de mais um item:

iii) Se a proposição vale para um número real x, que não está no final de um intervalo fechado, então deve valer para mais números depois dele – mesmo que seja um intervalo ínfimo (na figura o intervalo é representado por δ).

O enunciado formal do princípio da indução em reais é dado a seguir.

(Princípio da Indução em $\mathbb{R}$). Seja $p(s)$ uma predicado a respeito de números reais (ou seja, $s \in \mathbb{R}$ é o argumento do predicado) e $a < b$ dois números reais. Se (i), (ii), (iii) a seguir valem:

i) $p(a)$ é verdadeiro;

ii) Para todo $x \in [a, b)$, se $p(x)$ vale, então existe algum δ tal que para todo $0 < k \leq \delta$, $p(x + k)$ vale;

iii) Para todo $x \in (a, b]$, se $p(k)$ vale para $k \in [a, x)$, então $p(x)$ é verdadeiro.

Então $p(s)$ é verdadeiro para todo $s \in [a, b]$. ◊

Exemplo β.17. Demonstramos agora o Teorema do Valor Intermediário: seja $f : [a, b] \to \mathbb{R}$ uma função contínua, e suponha, sem perda de generalidade, que $f(a) < f(b)$. Então para todo $f(a) < \nu < f(b)$, existe algum $x \in [a, b]$ tal que $f(x) = \nu$.

Suponha que $f(x) \neq \nu$ para todo $x \in [a, b]$.

Provaremos por indução em reais, que $f(x) < \nu$, para todo x no intervalo. Ou seja, nossa proposição $P(x)$ é "$f(x) < \nu$".

i) $f(a) < \nu$, porque é como definimos ν.

ii) Seja $x \in [a, b)$. Suponha que $P(x)$ vale, ou seja, $f(x) < \nu$. Como

   – f é contínua, e
   – x foi escolhido num intervalo aberto à direita, $[a, b)$,

   então deve haver algum δ tal que $f(x + \delta) < \nu$, ou seja, vale $P(x + \delta)$.

iii) Seja $x \in (a, b]$. Suponha que para *todo* $w \in [a, x]$, $P(w)$ vale – ou seja, $f(w) < \nu$. Como f é contínua, não podemos ter $f(x) > \nu$. Mas por hipótese, temos $f(x) \neq \nu$, logo só nos resta $f(x) < \nu$, ou seja, vale $P(x)$.

Assim, presumindo que $f(x) \neq \nu$ para todo $x \in [a, b]$, provamos que $f(x) < \nu$, para todo x no intervalo. Mas ν foi escolhido de forma que $\nu < f(b)$, e temos uma contradição. A única suposição que fizemos foi que $f(x) \neq \nu$ para todo $x \in [a, b]$, que agora nos vemos obrigados a negar – e a negação resulta exatamente no enunciado do Teorema. ◀

O princípio da indução em reais (ou indução no contínuo) é descrito em diversos trabalhos; uma redação bastante acessível é a de Dan Hathaway [Hat11].

O leitor poderá ler mais sobre as diferenças fundamentais entre reais e naturais (e sobre cardinalidade de conjuntos infinitos) na literatura de Teoria de Conjuntos, onde também encontrará o *princípio da indução transfinita*. Mencionamos os livros de Herbert Enderton [End77], de Derek Goldrei [Gol96] e, para uma introdução simples, o de Charles Pinter [Pin14].

Exercícios

Ex. 331 — Prove que $n! < n^n$ para todo $n > 1$.

Ex. 332 — Mostre que para qualquer inteiro positivo n,

$$\sum_{j=1} n(2j-1) = n^2.$$

Ex. 333 — Defina qual é o menor n para o qual as afirmações valem, e depois prove-as.

a) n divide $n^3 - n$

b) 13 divide $2^{4n+2} + 3^{n+2}$

c) 3^{n+1} divide $2^{3^n} + 1$

Ex. 334 — Prove que

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} + \cdots + (-1)^{n-1}\frac{1}{n}$$

é sempre positivo.

Ex. 335 — Prove que um número que tem exatamente 3^n dígitos, todos idênticos, é divisível por 3.

Ex. 336 — Mostre que $1 + 3 + 5 + \ldots + (2n-1) = n^2$, para todo inteiro $n > 0$.

Ex. 337 — Prove que para todo natural $n \geq 1$,

$$\sum_{j=1}^{n} \frac{1}{\sqrt{j}} \geq \sqrt{n}$$

Ex. 338 — Prove que

$$\sum_{n=1}^{n} \frac{1}{i^2 + i} = \frac{n}{n+1}.$$

Ex. 339 — Prove que

$$\sqrt{2+\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}} < 2.$$

Ex. 340 — Seja

$$f(0) = 2$$
$$f(n) = 2\sqrt{f(n-1)}$$

Prove que para qualquer $n \in \mathbb{N}$, $f(n) < 4$.

Ex. 341 — Prove que

$$\sqrt{1+\sqrt{1+\cdots+\sqrt{1}}}$$

é irracional se a quantidade de raízes aninhadas for finita e maior ou igual a dois.

Ex. 342 — Prove que há infinitos números cuja decomposição tem somente quadrados ou primos elevados a potências maiores (não tem primos isolados). (Por exemplo, $48200 = 2^3 5^2$).

Ex. 343 — Para quaisquer m, n inteiros com $m \neq 0$ e $m > n$, seja

$$g(m,n) = \begin{cases} m & \text{se } n = 0 \\ g(n,r) & \text{caso contrário (r é resto de } m \div n) \end{cases}$$

Prove que $g(m,n)$ é o maior natural que divide tanto m como n.

Ex. 344 — No Exercício β.15 mostramos um algoritmo que calcula a paridade de um número binomial $\binom{m}{n}$, e dissemos que o algoritmo usa $4\lfloor \log_2 n \rfloor$ divisões. Prove que esta é de fato a quantidade de divisões feitas.

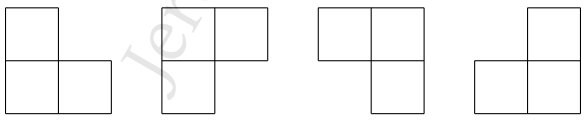
Ex. 345 — Prove que para $n \geq 2$, a expansão de $(1 + x + x^2)^n$ tem pelo menos um coeficiente par.

Ex. 346 — Prove que para $n \geq 3$, a soma dos ângulos interiores de um polígono convexo com n vértices é $\pi(n-2)$.

Ex. 347 — Prove que se dividirmos o plano usando retas como no Exemplo β.10, poderemos pintar as regiões formadas com apenas duas cores, sem que regiões adjacentes fiquem com a mesma cor.

Ex. 348 — Prove a fórmula de Euler: Se um poliedro tem V vértices, F faces e E arestas, então $V + F - E = 2$.

Ex. 349 — Um *tridominó* é uma peça que ocupa tres casas contíguas mas não na mesma linha ou coluna, em um tabuleiro. A seguir temos exemplos de um tridominó (rotacionado quatro vezes apenas para clarificar como ele poderá ser usado no tabuleiro).



a) Prove que um tabuleiro quadrado de lado com 2^n quadrados com um dos cantos removidos pode ser preenchido completamente por tridominós.

b) Após cobrir um tabuleiro de tamanho 2^n, quantos tridominós estarão rotacionados de cada forma (veja as quatro rotações na figura). Por exemplo, com $n = 4$, temos um , um e tres .

Obviamente, se rotacionarmos o tabuleiro a solução muda, mas continua sendo da forma $A + B + 3C$ – é esta a resposta pedida.

★ **Ex. 350 —** Prove que para todo $n \geq 2$,

$$\sqrt{2\sqrt{3\sqrt{4\cdots(n-1)\sqrt{n}}}} < 3.$$

Ex. 351 — Mostre, por indução, que a inversa da matriz diagonal A com valores $a_{11}, a_{22}, \ldots, a_{nn}$ é a matriz diagonal om valores $1/a_{11}, 1/a_{22}, \ldots, 1/a_{nn}$.

Ex. 352 — Prove que

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}^n = 2^{n-1} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

para todo natural $n \geq 1$.

Ex. 353 — Seja

$$A = \begin{pmatrix} 5 & -1 \\ 4 & 1 \end{pmatrix}$$

Prove que para $n \geq 1$,

$$A^n = 3^{n-1} \begin{pmatrix} 2n+3 & -1 \\ 4n & 3-2n \end{pmatrix}$$

Ex. 354 — Determine a forma fechada para A^n, onde A é uma matriz com uns na diagonal principal; um elemento igual a um acima da diagonal principal; e todos os outros elementos iguais a zero.

★ **Ex. 355 —** Determine a forma fechada para

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 1 & & 1 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & & \cdots & 1 \end{pmatrix}^n$$

(A matriz tem zeros abaixo da diagonal principal e uns na diagonal e acima dela).

Ex. 356 — Prove a corretude do algoritmo de Strassen. Sejam

$$A = \left(\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array}\right), B = \left(\begin{array}{c|c} B_{11} & B_{12} \\ \hline B_{21} & B_{22} \end{array}\right),$$

duas matrizes particionadas em quatro blocos cada uma (as partições de A e B são tais que permitem multiplicar AB por blocos).
Seja

$$C = \left(\begin{array}{c|c} C_{11} & C_{12} \\ \hline C_{21} & C_{22} \end{array}\right),$$

onde os quatro blocos de C são

$$\begin{aligned} C_{11} &= M_1 + M_2 - M_4 + M_6 \\ C_{12} &= M_4 + M_5 \\ C_{21} &= M_6 + M_7 \\ C_{22} &= M_2 - M_3 + M_5 - M_7, \end{aligned}$$

onde

$$\begin{aligned} M_1 &= (A_{12} - A_{22})(B_{21} + B_{22}) \\ M_2 &= (A_{11} + A_{22})(B_{11} + B_{22}) \\ M_3 &= (A_{11} - A_{21})(B_{11} + B_{22}) \\ M_4 &= (A_{11} + A_{12})B_{22} \\ M_5 &= A_{11}(B_{12} - B_{22}) \\ M_6 &= A_{22}(B_{21} - B_{11}) \\ M_7 &= (A_{21} + A_{22})B_{11} \end{aligned}$$

Prove que $C = AB$, ou seja, ao calcular as matrizes M_i e montar C da maneira descrita, teremos multiplicado A por B.

Ex. 357 — Seja

$$\begin{aligned} f(1) &= 1 \\ f(2) &= 5 \\ f(n+1) &= 2f(n-1) \end{aligned}$$

Conjecture uma fórmula para $f(n)$, presumindo que n sempre é natural, e prove por indução que sua fórmula está correta.

Ex. 358 — Seja $a_1, a_2, \ldots$ uma sequência de números reais tal que $a_{i+j} \leq a_i + a_j$ para quaisquer i e j. Prove que

$$a_n \leq a_1 + \frac{a_2}{2} + \frac{a_3}{3} + \cdots + \frac{a_n}{n}.$$

Ex. 359 — Seja F_n o n-ésimo número de Fibonacci:

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2} \end{aligned}$$

Prove que $F_n < 2^n$ para todo $n \geq 0$.

Ex. 360 — Demonstre (a) e (b) abaixo, usando indução.

a) Todo número natural pode ser decomposto em fatores primos.

★ b) Seja $\mathbb{Z}[x]$ a estrutura algébrica composta por polinômios com coeficientes inteiros e as operações de soma e multiplicação usuais sobre eles[5]. Assim como para números naturais, a divisão está definida em $\mathbb{Z}[x]$. Um polinômio em $\mathbb{Z}[x]$ com é *irredutível* se não pode ser escrito como produto de dois outros. Prove que todo polinômio p em $\mathbb{Z}[x]$ pode ser decomposto em polinômios em $\mathbb{Z}[x]$, irredutíveis e de grau menor ou igual que o de p.

★ **Ex. 361 —** Prove que $|\operatorname{sen}^n(x)| \leq 1 - \epsilon$, com $\epsilon > 0$, para todo $n \in \mathbb{N}$. (Aqui $\operatorname{sen}^n(x)$ é a repetição de n vezes a função seno, e não potencia). Determine ϵ, e prove que $\operatorname{sen}^n(x)$ pode ser exatamente igual tanto a $1 - \epsilon$ quanto a $-1 + \epsilon$.

Ex. 362 — Prove, por indução, a identidade de De Moivre: para todos os $x \in \mathbb{R}$, $n \in \mathbb{Z}$,

$$(\cos x + i \operatorname{sen} x)^n = \cos(nx) + i \operatorname{sen}(nx),$$

onde $i = \sqrt{-1}$.

Ex. 363 — Prove que a função Γ é uma generalização do fatorial. Ou seja, dada a função

$$\Gamma(x) = \int_0^\infty t^{x-1} e^{-t} dt$$

Prove que para todo n natural $\Gamma(n+1) = n!$, ou seja,

$$\int_0^\infty t^n e^{-t} dt = n!$$

Ex. 364 — Prove que para todo $n \geq 1$ natural,

$$\frac{d^n}{dx^n}\left(xe^{2x}\right) = 2^{n-1}(2x+n)e^{2x}.$$

Ex. 365 — Prove que

$$\int_0^\pi \operatorname{sen}^n x dx = \frac{n-1}{n} \int_0^\pi \operatorname{sen}^{n-2} x dx,$$

e em seguida calcule $\int_0^\pi \operatorname{sen}^8 x dx$.

[5] Esta estrutura é um *anel.*

Ex. 366 — Prove que a n-ésima derivada de x^n é $n!$.

Ex. 367 — Demontre a generalização da regra do produto para derivadas:

$$\begin{aligned}(f_1 f_2 f_3 \cdots f_n)' &= f_1' f_2 f_3 \cdots f_n \\ &+ f_1 f_2' f_3 \cdots f_n \\ &+ f_1 f_2 f_3' \cdots f_n \\ &\vdots \\ &+ f_1 f_2 f_3 \cdots f_n'\end{aligned}$$

Ex. 368 — Seja $f : [0,1] \to \mathbb{R}$ cotínua e infinitas vezes diferenciável em $(0,1)$. Denote por $f^{(n)}$ a n-ésima derivada de f, e seja $f^0 = f$. Prove que para todo $m \in \mathbb{N}$,

$$\frac{1}{n!}\int_0^1 x^n f(x)\,dx = \sum_{j=1}^{m} \frac{(-1)^{j-1} f^{(j-1)}(1)}{(n+j)!} + (-1)^m \int_0^1 \frac{x^{n+m} f^m(x)}{(n+m)!}\,dx$$

Ex. 369 — Prove que para todo $n \geq 2$,

$$\frac{1}{2}\int_{-\pi/2}^{\pi/2} \cos^{2n-1}(x)\,dx = \frac{(2n-2)(2n-4)(2n-6)\cdots}{(2n-1)(2n-3)(2n-5)\cdots}$$

★ **Ex. 370 —** Seja $f : [a,b] \to \mathbb{R}$ contínua, assumindo valores reais em a e b (ou seja, $f(a)$ e $f(b)$ são reais). Prove que f é limitada por cima e por baixo nesse intervalo.

★ **Ex. 371 —** Prove o teorema do valor médio usando indução em reais: Seja $f : [a,b] \to \mathbb{R}$ contínua, e diferenciável em (a,b). Então existe $c \in (a,b)$ tal que

$$f'(c) = \frac{f(b) - f(a)}{b-a}$$

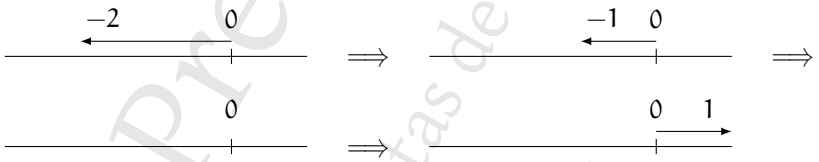
ou seja, existe algum ponto entre a e b onde a tangente é paralela à reta passando por a e b.

Apêndice γ

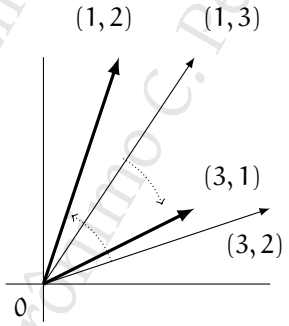
Orientação de Bases

Neste Apêndice damos uma definição geometrica mais rigorosa de orientação de base ordenada em $\mathbb{R}^n$.

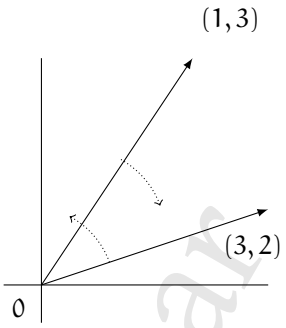
Começamos observando vetores em $\mathbb{R}$: não podemos transformar *continuamente* o vetor (-2) (que é uma base para $\mathbb{R}$) no vetor (1) sem que um dos vetores intermediários seja o vetor zero:



Passamos agora para $\mathbb{R}^2$, usando idéia análoga à que usamos para as bases de $\mathbb{R}$. Não podemos transformar a base $A = \{ (1,2)^T, (3,1)^T \}$ na base $B = \{ (3,2)^T, (1,3)^T \}$ sem que, no decorrer da transformação, tenhamos dois vetores colineares: temos que transformar $(1,2)^T$ em $(3,2)^T$ e $(3,1)^T$ em $(1,3)^T$. A figura a seguir ilustra a transformação. Os vetores em negrito ficam fixos, e os vetores em traçado leve são transformados.



Como os vetores em negrito, $(3,2)^T, (1,3)^T$ formam a base B e não seriam modificados, apresentamos a figura sem eles, mostrando que a transformação dos vetores de A:



Note que se duas bases ordenadas A e B tem a mesma orientação, e trocamos dois vetores de posição em A (ou em B), elas passam a ter orientação oposta, porque já não é mais possível transformar continuamente A em B sem passar por uma tupla que não é base. Isso é válido também para $\mathbb{R}^3$.

Formalizaremos este conceito da seguinte maneira. Uma base para $\mathbb{R}^n$ tem n vetores. Diremos que duas bases tem a mesma orientação quando houver n funções, $f_1, \ldots, f_n$, definidas em $[0, 1]$, tais que $\big(f_1(0), f_2(0), \ldots, f_n(0)\big) = A$ e $\big(f_1(1), f_2(1), \ldots, f_n(1)\big) = B$ – ou seja, o valor de f_i em zero é o i-ésimo vetor de A, e o valor de f_i em um é o i-ésimo vetor de B. Isso significa que podemos variar i de zero a um, transformando os vetores de A nos vetores de B. As restrições que impomos às funções são:

- Cada uma das f_i deve ser contínua.
- Para todo $t \in [0, 1]$, $\big(f_1(t), f_2(t), \ldots, f_n(t)\big)$ deve ser base ordenada (ou seja os vetores não podem ser LD).

Definição γ.1 (Bases com orientação concordante em $\mathbb{R}^n$)**.** Sejam A e B duas bases para $\mathbb{R}^n$. Dizemos que A e B tem a mesma *orientação* se A pode ser transformada em B *continuamente* e *sem tornar-se degenerada*, ou seja, existem n funções $f_1, f_2, \ldots, f_n$, todas definidas como $f_i : [0, 1] \to \mathbb{R}^n$, todas contínuas, sendo

$$\big(f_1(0), f_2(0), \ldots, f_n(0)\big) = A,$$
$$\big(f_1(1), f_2(1), \ldots, f_n(1)\big) = B,$$

e tais que para todo $t \in [0, 1]$ a tupla

$$\big(f_1(t), f_2(t), \ldots, f_n(t)\big)$$

é uma base ordenada para $\mathbb{R}^n$. ♦

Usualmente, define-se que a orientação de uma base B para $\mathbb{R}^n$ é *positiva* (ou ainda, que $O(B) = +1$) se ela concorda com a orientação da base canônica para $\mathbb{R}^n$. De outra forma, é *negativa* (ou que $O(B) = -1$).

Em $\mathbb{R}$, mudar o sinal da base muda sua orientação, porque não podemos transformar um vetor $(+x)$ em outro $(-x)$ continuamente sem passar pelo vetor zero.

Em $\mathbb{R}^n$, com $n \geq 2$, trocar a posição de dois vetores de uma base tem o efeito de mudar sua orientação, conforme o enunciado do teorema γ.2.

Teorema γ.2. *Seja A uma base para $\mathbb{R}^n$, com $n \geq 2$, e seja A' a base obtida de A trocando as posições de dois de seus vetores. Então A e A' não tem orientação concordante.*

Exercícios

Ex. 372 — Demonstre o Teorema $\gamma.2$.

★ **Ex. 373 —** Escolha um espaço de funções com dimensão finita (dois, por exemplo) e exiba duas bases com orientação concordante. Troque a posição de dois dos vetores da base e mostre que de fato as bases passam a ter orientações opostas. Tente não usar a representação das bases como matrizes.

Apêndice δ

Equações Diferenciais

Em alguns dos exemplos neste livro usamos equações diferenciais. Este Apêndice traz a definição de equação diferencial e conceitos básicos relacionados a elas. Não é uma introdução completa ao assunto – abordamos aqui somente o necessário para a compreensão do texto. Há excelentes livros abordando Equações Diferenciais Ordinárias – bons livros com exemplos de aplicação prática incluem o de Tennenbaum e Pollard [TP63] e o de George Simmons [Sim06]; dentre os livros mais compactos e sem excursões por aplicações e métodos numéricos temos o de Herbert Bear [Bea62], e o de Earl Coddington [Cod61]; em Português há os livros de Djairo Figueiredo e Aloisio Neves [FN14] e de Vinícius Cifú Lopes [Lop15]. Sobre Equações Diferenciais Parciais, mencionamos os livros de Walter Strauss [Str08], de Fritz John [Joh82] e de David Colton [Col88] e, para um ponto de vista bastante pragmático, o de Stanley Farlow [Far82]. Em Português, o livro de Djairo Figueiredo [Fig77] dá uma introdução às EDPs como aplicação de Séries de Fourier[1].

Começamos com um exemplo onde modelamos um fenômeno de crescimento com uma equação diferencial. Suponha que estejamos estudando uma cultura de bactérias. Se a quantidade de bactérias triplica em uma hora e a quantidade inicial de bactérias era x_0, quantas bactérias teremos na cultura após cinco horas?

A equação diferencial que descreve o crescimento das bactérias é

$$\frac{dx}{dt} = kx.$$

Esta equação nos diz exatamente que "a variação na quantidade x de bactérias ao longo do tempo é proporcional a x, com constante de proporcionalidade k". A equação nos informa uma relação entre a quantidade de bactérias e sua taxa de crescimento no tempo, mas não nos dá uma expressão da quantidade x de bactérias no tempo t. Nossa intenção é obter uma expressão de $x(t)$ que não envolva a derivada dx/dt.

Observando que temos dt em ambos os lados da equação, integramos os dois lados com relação a t,

$$\int \frac{1}{x}\frac{dx}{dt}dt = \int k dt.$$

Por substituição[2], temos

$$\int \frac{1}{x}dx = \int k dt.$$

[1] Damos uma breve introdução à série de Fourier no Capítulo 14 do presente livro; o livro citado, de Djairo Figueiredo, é mais extenso e detalhado.

[2] $\int f(g(t))g'(t)dt = \int f(u)du$, com $u = g(t)$. Neste caso, $g(t) = x(t)$, e $f(g(t)) = 1/x(t)$. Observe que $\frac{dx}{dt}$ *não* é uma

Disso já podemos concluir que $\log(x) = kt + c$, e portanto temos $x(t) = e^{kt+c}$. No entanto, não conhecemos k nem c – somente sabemos que *qualquer* função da forma $x(t) = e^{kt+c}$ é uma solução para a equação diferencial. No entanto, não queremos uma solução envolvendo *qualquer valor* para k. Queremos determiná-lo. Sabemos que a constante c será cancelada quando calcularmos a integral definida. A constante k nos será conhecida também quando usarmos a equação com as condições dadas.

Agora observamos:

i) A quantidade de bactérias triplica a cada hora;

ii) A quantidade inicial de bactérias era x_0;

iii) Queremos a quantidade de bactérias após 5 horas.

De (i), temos

$$\int_q^{3q} \frac{1}{x}dx = \int_0^1 k dt.$$

Integramos o lado esquerdo com x começando em um valor arbitrário q e terminando em $3q$, porque em uma hora a quantidade inicial triplicará. Mais adiante veremos que a variável q será cancelada em nossas contas.

Integramos o lado direito em t, que varia de zero a um (porque uma hora é o período em que observamos a quantidade triplicar). Temos então

$$\begin{aligned}
\int_1^{3q} \frac{1}{x}dx &= \int_0^1 k dt \\
\log x\big|_q^{3q} &= kt\big|_{t=0}^1 \\
\log \frac{3q}{q} &= kt\big|_{t=0}^1 \\
\log 3 &= k.
\end{aligned}$$

Já conhecemos a constante k. Agora, de (ii) e (iii), temos

$$\begin{aligned}
\int_{x_0}^{Q} \frac{1}{x}dx &= \int_0^5 k dt \\
\log x\big|_{x_0}^{Q} &= kt\big|_{t=0}^5 \\
\log(Q) - \log(x_0) &= 5\log 3 \\
\log \frac{Q}{x_0} &= \log(3^5) \\
Q &= 3^5 x_0.
\end{aligned}$$

fração, por isso não podemos "cancelar" dt. Poderíamos usar a definição de *diferencial*: $dy = y'dx$, e, *entendendo que* dt *na equação é um diferencial*, cancelá-lo. No entanto, a noção de diferencial ainda pressupõe a existência da derivada y' definida como limite. É possível, na verdade, construir o Cálculo sem definir a derivada como limite. Isso se faz usando Análise Não-Padrão, desenvolvida originalmente por Abraham Robinson [Rob66], mas que fica fora do escopo deste texto. A Análise é uma área da Matemática onde são estudadas as teorias que fundamentam o Cálculo Diferencial e Integral, convergência de séries, e outros tópicos, ali estudados em profundidade e com mais rigor do que em um curso de Cálculo. A Análise não-padrão reconstrói os fundamentos do Cálculo usando "infinitesimais". Uma abordagem de Cálculo baseada em Análise Não-Padrão é usada no livro de Howard Keisler [Kei12]; já o livro de Alain Robert [Rob11] contém um curso moderno de Análise Não-Padrão.

Assim, após 5 horas, teremos 3^5 vezes o valor inicial x_0.

O que fizemos neste exemplo foi determinar uma equação diferencial que descreve um fenômeno, e em seguida "*resolvê-la*" – ou seja, encontrar uma descrição da função incógnita que não dependa das suas derivadas.

δ.1 Equação Diferencial Ordinária

Definição δ.1 (Equação diferencial)**.** Uma *equação diferencial ordinária* é uma equação envolvendo uma função de uma variável e uma ou mais de suas derivadas. A *ordem* da equação é a maior ordem de derivada da função incógnita presente na equação. O *grau* da equação é o expoente da derivada de maior ordem. Dizemos que uma equação diferencial é linear se é de grau um. ♦

Exemplo δ.2. A seguir temos exemplos de várias equações diferenciais ordinárias.

$$\frac{d}{dx}f(x) + 2f(x) - 3 = 0$$
$$y'' - y = 0$$
$$(\dot{x})^2 + x^2 - x = 0$$

A primeira equação é linear e de primeira ordem. A segunda é linear de segunda ordem. A terceira é de primeira ordem e segundo grau. ◄

Exemplo δ.3. A *equação logística* é uma equação diferencial ordinária normalmente usada na modelagem de crescimento de populações. A população no instante t é $P(t)$; a taxa de crescimento é r (também é chamada de parâmetro Malthusiano), e K é a densidade populacional máxima:

$$\frac{dP}{dt} = rP\left(1 - \frac{P}{K}\right).$$

Esta é uma equação diferencial ordinária linear e de primeira ordem. ◄

Exemplo δ.4. A lei segunda lei de Newton, $F = ma$, é na verdade uma equação diferencial ordinária. Newton a formulou tendo em mente a massa da Lua e a força gravitacional entre Terra e Lua:

$$g = m\frac{d^2x}{dt^2}$$

Esta equação é linear e de segunda ordem. ◄

Definição δ.5 (Solução de equação diferencial)**.** Uma *solução específica* para uma equação diferencial envolvendo derivadas de uma função desconhecida f é uma função que pode ser usada no lugar de f satisfazendo a equação. A *solução geral* para uma EDO é uma descrição de *todas* as soluções específicas para aquela equação. ♦

Exemplo δ.6. Para quaisquer a e b, a função

$$y = \frac{x^3}{6} + ax + b$$

é solução da equação diferencial

$$y'' - x = 0,$$

porque

$$\begin{aligned} y'' - x &= \left(\frac{x^3}{6} + ax + b\right)'' - x \\ &= \left(\frac{x^2}{2} + a\right)' - x \\ &= x - x \\ &= 0. \end{aligned}$$

Assim,

$$y = \frac{x^3}{6} + ax + b, \quad a, b \in \mathbb{R}$$

é a solução geral, enquanto

$$\begin{aligned} y &= \frac{x^3}{6} \\ y &= \frac{x^3}{6} + x \\ y &= \frac{x^3}{6} + x + 1 \\ y &= \frac{x^3}{6} + -3x + \sqrt{2} \\ y &= \frac{x^3}{6} + \pi x - 1 \\ &\vdots \end{aligned}$$

são solções específicas para a equação. ◀

No exemplo δ.6, o conjunto de soluções para a equação pode ser definido por duas constantes, logo temos uma quantidade infinita mas *enumerável* de soluções.

δ.2 Separação de variáveis

Nesta seção apresentamos um método básico para solução de algumas equações diferenciais ordinárias. Este método servirá apenas para poucas situações simples, e é incluído aqui apenas como ilustração. Métodos apropriados a equações diferenciais de outros tipos são encontrados nos livros já citados no início deste Capítulo.

Quando é possível reorganizar as variáveis de forma que cada uma fique de um lado da equação, podemos usar o método de *separação de variáveis*.

Teorema δ.7. *Sejam* f *e* g *funções contínuas,* $F' = f$, $G' = g$, *e* y *é solução de*

$$g(y)\frac{dy}{dx} = f(x), \tag{δ.1}$$

então existe uma constante c *tal que*

$$G(y(x)) = F(x) + c. \tag{δ.2}$$

Além disso, qualquer função y *que satisfaça δ.2 para algum* c *é solução de δ.1.*

Demonstração. Temos

$$\begin{aligned} g(y)\frac{dy}{dx} &= f(x) \\ \int g(y)\frac{dy}{dx}dx &= \int f(x)dx && \text{(integre ambos os lados em } x\text{)} \\ \int g(y)dy &= \int f(x)dx && \text{(substituição/regra da cadeia)} \\ G(y) &= F(x) + c. && \blacksquare \end{aligned}$$

$$\frac{dy}{dx}dx = dy.$$

Exemplo δ.8. A equação

$$y' - x^2 = x^2 y$$

pode ser reescrita como

$$\begin{aligned} y' &= x^2(y+1) \\ \frac{1}{y+1}\frac{dy}{dx} &= x^2 \end{aligned}$$

Temos portanto

$$\begin{aligned} \int \frac{1}{y+1}dy &= \int x^2 dx \\ \log(y+1) &= \frac{x^3}{3} + c \\ y + 1 &= \exp(x^3/3 + c) \\ y &= \exp(x^3/3 + c) - 1, \end{aligned}$$

que é solução para a equação diferencial da qual partimos. ◀

Exemplo δ.9. A equação

$$\frac{y'}{\operatorname{sen}(x)} = \frac{x}{y}$$

pode ser reescrita como

$$yy' = x\operatorname{sen}(x).$$

Integramos ambos os lados,

$$\begin{aligned} \int y\,dy &= \int x\operatorname{sen}(x)dx \\ \frac{y^2}{2} &= \operatorname{sen}(x) - x\cos(x) + c \\ y &= \pm\sqrt{2(\operatorname{sen}(x) - x\cos(x) + c)}. \end{aligned}$$ ◀

δ.3 Problemas de valor inicial e de contorno

Muitas vezes não temos interesse em ober *todas* as soluções para uma equação diferencial, e nem mesmo *uma solução específica qualquer*, mas sim uma solução que satisfaça certas condições. Em um *problema de valor inicial* temos, além de uma equação diferencial descrevendo uma função $f(x)$, temos o valor da função em um ponto, por exemplo $f(z) = v$, e procuramos uma solução F que satisfaça $F(z) = v$. Se tivermos valores de f em vários pontos, temos um *problema de valores de contorno* (ou problema *com condições de contorno*). O que fizemos no início do Capítulo foi resolver um problema de valores de contorno: sabíamos que o crescimento de bactérias em uma cultura era descrito por

$$\frac{dx}{dt} = kt,$$

e tínhamos também um valor x_0 e o valor $x_1 = 3x_0$.

Exemplo δ.10. O problema

$$\begin{aligned} y'' + 2y' - 3x &= 0, \\ y(\pi) &= 2, \\ y'(\pi) &= -1 \end{aligned}$$

é um problema de valor inicial, porque além da equação diferencial, temos a descrição dos valores de y e y' em um ponto. ◀

Exemplo δ.11. O problema

$$\begin{aligned} y' + y - 2x &= 0, \\ y(0) &= 5, \\ y(1) &= -5 \end{aligned}$$

é um problema de valores de contorno, porque além da equação diferencial, temos a descrição dos valores de y e y em dois pontos. ◀

δ.4 Equação Diferencial Parcial

Definição δ.12 (Equação diferencial parcial)**.** Uma *equação diferencial parcial* é uma equação envolvendo uma função de várias variáveis e uma ou mais de suas derivadas parciais. ♦

Exemplo δ.13. A seguir temos exemplos de equações diferenciais parciais. Ao descrever as derivadas, pode-se usar u_{xxx} como sinônimo de $\frac{\partial^3 u}{\partial x^3}$.

$$\begin{aligned} \frac{\partial^2}{x^2} + \frac{\partial^2}{y^2} &= 0 \\ u_t - t^3 u_{xxx} &= 0 \\ \frac{\partial^2 f(x,y)}{\partial x^2} + xy - \frac{\partial f(x,y)}{\partial x} - \frac{\partial f(x,y)}{\partial y} &= 0 \end{aligned}$$ ◀

Observamos que o conjunto de soluções para uma EDP é bastante diferente daquele para uma EDO. Por exemplo, considere a EDP a seguir:

$$\frac{\partial u}{\partial x} = 0.$$

A solução geral desta equação é

$$u(x, y) = f(y),$$

onde $f : \mathbb{R} \to \mathbb{R}$ pode ser *qualquer função real de uma variável* – e daí notamos que embora as soluções para uma EDP sejam um conjunto infinito, com as de uma EDO, este conjunto não é enumerável (porque o conjunto de funções reais não é enumerável).

δ.5 Aplicações

A quantidade de aplicações possíveis de equações diferenciais é imensa, e seria ingênuo resumí-las em uma pequena seção de um livro. Podemos, no entanto, selecionar alguns poucos exemplos.

δ.5.1 Química nuclear: decaimento radioativo [EDO de primeira ordem]

Sabemos, a partir de estudos experimentais, que a velocidade de desintegração de qualquer material radioativo é proporcional à quantidade daquele material. Ou seja, quanto mais material radioativo, mais rápido ele se desintegra.

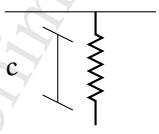
A *velocidade* de desintegração é a derivada da quantidade em relação ao tempo, dM/dt. Como ela é proporcional à quantidade, chegamos à equação diferencial do decaimento radioativo:

$$\frac{dM}{dt} = kM,$$

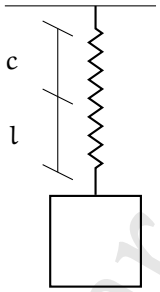
com $k < 0$. Esta é uma equação diferencial *linear* e *de primeira ordem.*

δ.5.2 Mecânica: oscilador harmônico [EDO de segunda ordem]

Suponha que uma mola de compimento c está fixada abaixo de uma superfície, sem nenhuma força atuando sobre ela.



Prendemos na outra extremidade da mola um objeto com masa m. Como a mola é elástica, o objeto (e consequentemente a extremidade da mola) será deslocado para baixo, por uma distância l. Nesta posição o sistema estará em equilíbrio, e não haverá movimento.



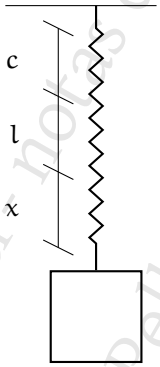
Haverá duas forças atuando sobre o objeto (ou, equivalentemente, sobre a extremidade de baixo da mola):

- a força gravitacional, na direção para baixo, com intensidade mg;
- a força da mola, que tentará retornar o sistema ao ponto de equilíbrio. A *Lei de Hooke* determina que esta força é proporcional à distância do ponto atual ao ponto de equilíbrio, logo sua intensidade é kl. Para cada mola existe um valor de k, chamado de *constante elástica* da mola.

Assim, temos

$$mg = kl.$$

Agora puxamos o objeto mais para baixo, forçando-o a descrever uma distância adicional x.



Agora as duas forças atuando são a força gravitacional, que continua a mesma, e a força da mola para tentar retornar ao ponto de equilíbrio, que passa a ser

$$k(l + x).$$

Usamos agora a segunda lei de Newton, $\vec{F} = m\vec{a}$: a força resultante em um sistema ($\vec{F}$) será igual à massa do sistema multiplicada por sua aceleração ($m\vec{a}$). Como já conhecemos a orientação da força, deixamos de lado a notação de vetor e usamos somente a magnitude de a e g:

$$ma = mg - k(l + x)$$
$$m\frac{d^2x}{dt^2} = (mg - kl) - kx$$

$$m\frac{d^2x}{dt^2} = -kx \qquad (mg = kl)$$

Temos finalmente

$$\frac{d^2x}{dt^2} + \frac{k}{m}x = 0,$$

que é a equação diferencial que descreve o movimento de uma mola.

Esta é uma equação diferencial *linear* e *de ordem dois*.

A solução para esta equação é dada por

$$x = \alpha\cos\left(\sqrt{\frac{k}{m}}t + \delta\right)$$

ou

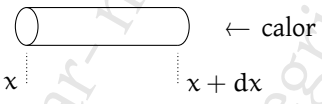
$$x = \alpha\,\mathrm{sen}\left(\sqrt{\frac{k}{m}}t + \delta\right).$$

δ.5.3 Termodinâmica: propagação de calor [EDP]

Grosso modo, o calor pode ser tranferido de três maneiras: em fluidos, a transferência se dá principalmente por *convecção* (o próprio fluido se move, levando calor); outra forma de transferencia é *condução*, sem que haja movimento da substancia; finalmente, o calor pode ser transferido por *radiação*.

Nesta seção analisaremos a condução de calor, chegando a uma equação diferencial parcial.

Trataremos aqui somente do caso emuma dimensão: temos uma barra como a ilustrada na figura a seguir, e aplicamos calor em uma das suas extremidades.



Sabemos que a quantidade de energia necessária para aumentar em du a temperatura de um corpo com massa m é proporcional a m, mas a constante de proporcionalidade depende do material de que o corpo é constituído. Podemos dizer, portanto que essa quantidade é $sm\,du$, onde m é a massa do corpo; s é uma constante que depende do corpo (chamamos de *calor específico*; e du é o valor do aumento na temperatura (note que já usamos notação de diferencial).

A energia flui por uma superfície a uma taxa proporcional à área (que denotamos por A) e ao gradiente da temperatura, ou seja, $kA(\partial u/\partial x)$. À constante k damos o nome de *condutividade térmica*.

O gradiente da temperatura no extremo da direita é

$$\frac{\partial u}{\partial x}(x + dx, t).$$

Assim, a energia passa pelo extremo da direita a uma taxa de

$$kA\frac{\partial u}{\partial x}(x + dx, t).$$

Em um intervalo de tempo infinitesimal, uma certa quantidade de calor entra na barra pelo lado direito, e outra quantidade sai pelo lado esquerdo. A quantidade total de calor que entra na barra é, portanto,

$$\underbrace{kA\frac{\partial u}{\partial x}(x+dx,t)}_{\text{entra à direita}} - \underbrace{kA\frac{\partial u}{\partial x}(x,t)}_{\text{sai à esquerda}}.$$

Suponha que a densidade da barra é D. Então a massa é $DA\,dx$, portanto a quantidade de energia necessária para aquecer a barra em $\frac{\partial u}{\partial x}(x+dx,t)$ é

$$s\,m\,du = s\,DA\,dx\,\frac{\partial u}{\partial x}(x+dx,t)$$

Esta deve ser a mesma quantidade de energia que entrou na barra no intervalo de tempo dt:

$$sDA\,dx\frac{\partial u}{\partial t}(x,t)\,dt = kA\left[kA\frac{\partial u}{\partial x}(x+dx,t) - kA\frac{\partial u}{\partial x}(x,t)\right]dt$$

ou seja,

$$sDA\frac{\partial u}{\partial t}(x,t) = kA\left[kA\frac{\partial^2 u}{\partial x^2}(x+dx,t) - kA\frac{\partial^2 u}{\partial x^2}(x,t)\right]$$

Quando $dx,\, dt \to 0$, temos

$$sDA\frac{\partial u}{\partial t}(x,t) = kA\frac{\partial^2 u}{\partial x^2}(x,t)$$
$$\frac{\partial u}{\partial t}(x,t) = \left(\frac{k}{sD}\right)\frac{\partial^2 u}{\partial x^2}(x,t)$$

Denotamos por $\alpha = k/sD$, e chamamos α de *difusividade térmica*. Chegamos assun à equação do calor em uma dimensão:

$$\frac{\partial u}{\partial t} = \alpha\frac{\partial^2 u}{\partial x^2}$$

Apresentamos a equação do calor para três dimensões[3], sem incluir sua derivação:

$$\frac{\partial u}{\partial t} = \alpha\Big(\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial^2 u}{\partial z^2}\Big).$$

Exercícios

Ex. 374 — Algumas das funções à esquerda são soluções para as equações à direita. Identifique-as.

[3] Uma forma alternativa de escrever a equação do calor é,

$$\frac{\partial u}{\partial t} = \alpha\nabla^2 u$$

se denotarmos o Laplaciano por ∇^2. O Laplaciano é dado pela divergencia do gradiente, $\nabla^2 f = \nabla\nabla f$, ou seja, $\nabla^2 f = \sum_{i=1}^{n}\frac{\partial^2 f}{\partial x_i^2}$.

(a) $y(x) = ae^x + x^2 + 2x + 2$
(b) $y(x) = a\,\mathrm{sen}(x) + b\cos(x)$
(c) $y(x) = x^2 + e^x$
(d) $y(x) = \cos(x^2)$
(e) $y(x) = -\log(x) + ax + b$
(f) $y(x) = \pm\sqrt{x+a}$
(g) $y(x) = ax^2 - b$

$$y' - \cos(x) = 0 \quad (i)$$
$$y'' + e^x = 0 \quad (ii)$$
$$e^{y'} - y'' + x = 0 \quad (iii)$$
$$xy'' - \frac{1}{x} = 0 \quad (iv)$$
$$xy'' - y = 0 \quad (v)$$
$$y'' + y = 0 \quad (vi)$$
$$\frac{1}{y} - y' = 0 \quad (vii)$$
$$y' - y + x^2 = 0 \quad (viii)$$

Ex. 375 — Determine soluções para as equações diferenciais dadas.

(i) $y' - \dfrac{x}{y} = 0$
(ii) $y'' + y\cos(x) = 0$
(iii) $\dfrac{x-1}{y+1}\dfrac{dx}{dy} - x^2\cos(y) = 0$
(iv) $y - 2y' = 0$
(v) $\dfrac{y''}{x} - \dfrac{e^x}{\cos(y)} = 0$

Ex. 376 — O isótopo Pluônio-241 (^{241}Pu) tem meia-vida de 14 anos (ou seja, a massa radioativa desse isótopo cai pela metade em 14 anos, unicamente por emissão radioativa[4]). Determine a constante de proporcionalidade para a equação de decaimento deste isótopo, ou seja, determine o valor de a na equação $dM/dt = aM$.

Ex. 377 — Considere equações diferenciais da forma

$$P(x,y)dx + Q(x,y)dy = 0,$$

onde P e Q são homogêneos da mesma ordem n, e tanto dx como dy são diferenciais. Prove que substituir

$$y \to ux$$
$$dy \to u\,dx + x\,du$$

resulta em uma equação com variáveis separáveis.

[4] mais especificamente, por decaimento β^-: seu núcleo muda, tornando-se um núcleo de Amerício (o número atômico aumenta), ao mesmo tempo em que emite um elétron e um elétron antineutrino – o tratamento em detalhes do assunto é feito no livro de Walter Loveland, David Morrisey e Glenn Seaborg [LM06]; uma explicação extremamente simplificada de decaimento β pode também ser obtida no livro de Harry Lipkin [J L12].

Apêndice ε

Alfabeto Grego

Uma vez que letras gregas são abundantes na Matemática, incluímos neste apêndice o alfabeto grego, com a pronúnica de cada letra.

maiúscula	minúscula	pronúncia
Α	α	alfa
Β	β	beta
Γ	γ	gama
Δ	δ	delta
Ε	ϵ, ε	épsilon
Ζ	ζ	zeta
Η	η	eta
Θ	θ, ϑ	teta
Ι	ι	iota
Κ	κ, ϰ	capa
Λ	λ	lambda
Μ	μ	mi
Ν	ν	ni
Ξ	ξ	csi
Ο	ο	ômicron
Π	π, ϖ	pi
Ρ	ρ, ϱ	rô
Σ	σ, ς	sigma
Τ	τ	tau
Υ	υ	úpsilon
Φ	ϕ, φ	fi
Χ	χ	qui
Ψ	ψ	psi
Ω	ω	ômega

Apêndice ζ

Dicas e Respostas

Resp. (Ex. 3) — Seja $(G, \cdot)$ um grupo, e sejam 1 e $1'$ dois neutros. Então

$$1x = x = x1,$$
$$1'x = x = x1'.$$

Agora, seja $x = (1')$. Então $1(1') = (1') = (1')1$. Mas pela segunda igualdade, $1'(1) = (1) = (1)1'$. Temos então $1 = 1'$.

Resp. (Ex. 5) — Não. A matriz $A = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ não é zero, porque não vale $B + A = B$ para todo B; por outro lado, A não tem inverso multiplicativo, porque contém um elemento zero.

Resp. (Ex. 7) — Não. (i) tanto $\vee$ como $\wedge$ são associativas; (ii) $\wedge$ é distributiva sobre $\vee$: $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$; (iii) o neutro para $\vee$ é 0, e para $\wedge$ é 1; (iv) no entanto, não há inverso para $\vee$ e 1: $\nexists a : \ 1 \vee a = 0$.
Poderíamos tentar trocar $\vee$ com $\wedge$, mas então perderíamos a propriedade (ii).

Resp. (Ex. 10) — $x = 0, y = 1, z = 0$.

Resp. (Ex. 12) — (vi) Não, porque não é verdade que $\forall \mathbf{v} \ \exists - \mathbf{v}$. As outras propriedades, no entanto, valem. (vii) Como se trata de subconjunto do conjunto de todas as funções, não é necessário demonstrar as propriedades de espaço vetorial: mostre apenas que a soma e multiplicação por escalar resultam em outra função com período π, e observe que $f(x) = 0$ é periódica com qualquer período (inclusive π).

Resp. (Ex. 15) — Há diversos exemplos. Um deles é $y' + y \ln(x) = 0$, com soluções da forma $y = ce^{x - x\ln(x)}$.

Resp. (Ex. 16) — (i) A função zero está bno subespaço: se $a = b = 0$, então $a + b = 0$. (ii) A soma de duas soluções desta forma é outra também desta forma: se $(a + b) = (\alpha + \beta) = 0$, e $(a + \alpha)e^x - (b + \beta)e^{-x}$ é solução, temos $(a + \alpha) + (b + \beta) = (a + b) + (\alpha + \beta) = 0$. (iii) A multiplicação por escalar também é fechada: Se $(a + b) = 0$, e $c(ae^x - be^{-x})$ é solução, então $ca + cb = c(a + b) = c0 = 0$.

Resp. (Ex. 25) — Muito claramente, para cada linha i,

$$\begin{aligned} &k(a_{i1}x_1 + a_{i2}x_1 + \cdots + a_{in}x_n) \\ =\, &k(0) = 0. \end{aligned}$$

Resp. (Ex. 26) — $\mathbf{v} + \mathbf{w}$ é solução para (ii):

$$\begin{aligned} A(\mathbf{v} + \mathbf{w}) &= A\mathbf{v} + A\mathbf{w} \\ &= \mathbf{0} + \mathbf{b} \\ &= \mathbf{b} \end{aligned}$$

Resp. (Ex. 27) — O vetor zero não é solução para sistemas não homogêneos.

Resp. (Ex. 29) — Como o conjunto só contém matrizes diagonais, a soma e multiplicação de matrizes podem ser usadas. Para matrizes quaisquer, isso já não funcionaria.

Resp. (Ex. 32) — Pode-se mostrar mais do que pede o exercício: que todo subespaço de $\mathbb{R}^2$ diferente do espaço trivial e diferente do $\mathbb{R}^2$ é uma reta. Os subespaços de $\mathbb{R}^2$ são:

i) o espaço trivial $\{\mathbf{0}\}$;

ii) espaços maiores que o trivial, mas não iguais a $\mathbb{R}^2$;

iii) o próprio $\mathbb{R}^2$.

Somente o caso (ii) é relevante. Suponha então que um vetor (x, y) pertença a um subespaço $X \subset \mathbb{R}^2$. Então todos os múltiplis desse vetor também pertencem a X, e portanto temos uma reta em X. Agora mostramos que não pode haver ninguém mais além dessa reta. Suponha que haja um em X um vetor (a, b) que não pertença à reta dos múltiplos de (x, y). Somando múltiplos de (x, y) e (a, b) podemos escrever qualquer vetor de $\mathbb{R}^2$, e portanto, se houvesse tal vetor (a, b) em X, teríamos $X = \mathbb{R}^2$.

Resp. (Ex. 33) — (i) sim, (ii) não.

Resp. (Ex. 37) — Não, porque há funções que não são pares nem ímpares, portanto $\mathcal{F}(\mathbb{R})$ não é soma dos dois conjuntos dados.

Resp. (Ex. 38) — (i) Não, porque a multiplicação de uma matriz por um escalar negativo muda o sinal de todos os elementos. (ii) Não, porque o segundo conjunto não contém a matriz zero, e também porque a soma de matrizes não preserva singularidade.

Resp. (Ex. 44) — Não: a base deve ser L.I., e portanto não pode conter o vetor zero; a multiplicação de vetor da base por escalar não pode resultar em outro vetor da base; e a soma de dois vetores da base não pode resultar em outro vetor também na base. A base *não pode* ser subespaço!

Resp. (Ex. 45) — Sim, de outra forma teríamos um vetor $(\ldots, k, \ldots)$ na base, com $k \neq 0$, e todo vetor da base também pertence ao espaço vetorial.

Resp. (Ex. 48) — (i) Infinito. (ii) Dimensão um. O espaço das sequências constantes é gerado por somente uma sequência constante diferente de zero.

Resp. (Ex. 52) — Suponha que em um espaço V não seja possível encontrar k vetores LI. Que se pode concluir a respeito de sua dimensão?

Resp. (Ex. 55) — Escrevemos a fórmula genérica,

$$F = m^a v^b r^c$$

e, sabendo que as dimensões são as mesmas dos dois lados, calculamos

$$[F] = \left[m^a v^b r^c\right]$$
$$MLT^{-2} = (M)^a \, (LT^{-1})^b \, L^c$$

e chegamos a

$$\begin{cases} a & = 1 \\ b + c & = 1 \\ -b & = -2 \end{cases}$$

o que nos dá $a = 1, b = 2, c = -1$, e a fórmula é

$$F = \frac{mv^2}{r}.$$

Resp. (Ex. 56) — O isomorfismo é dado por

$$f(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Resp. (Ex. 71) — Depende! Se permitirmos a rotação usando qualquer ângulo, a transformação certamente levará a pontos fora de $\mathbb{A}^2$, já que envolveria seno e cosseno de números algébricos – seria então uma transformação de $\mathbb{A}^2$ em $\mathbb{R}^2$, e não um operador em $\mathbb{A}^2$. Para continuar em $\mathbb{A}^2$ a rotação teria que ser restrita apenas a ângulos transcendentais.

Resp. (Ex. 80) — Como mencionado no exemplo 3.41, o kernel desta transformação é o conjunto de todas as funções constantes, e portanto não contém apenas a função $f(x) = 0$. A derivada, portanto, não é injetora.

Resp. (Ex. 82) — Usamos o isomorfismo entre o espaço de dimensão n e $\mathbb{R}^n$. O operador é

$$f\left[(x_1, x_2, \ldots, x_n)^T\right] = (0, x_1, x_2, \ldots, x_{n-1}).$$

O posto de f é $n-1$. O posto de f^k é $n-k$, para $1 \leq k \leq n$.

Resp. (Ex. 85) — AB também terá uma linha com zeros. O mesmo acontece com *colunas* de B: se B tem uma coluna com zeros, AB também terá.

Resp. (Ex. 86) — Trivial: uma matriz diagonal é triangular superior e inferior, por isso sua inversa deve ser também.

Resp. (Ex. 91) — (Dica) Observe que $AA^{-1} = \mathcal{I}$; suponha que A é triangular *inferior*, e observe que $\mathcal{I}$ é triangular *superior*, e que portanto ao multiplicar A por A^{-1}, os elementos abaixo da diagonal devem ser zero.

Resp. (Ex. 94) — Primeiro observamos que operações elementares em linhas ou em colunas não mudam a quantidade de linhas (ou de colunas) L.I. em uma matriz.
Seja A uma matriz. Realizamos operações elementares *em linhas* até obter a forma escalonada reduzida por linhas de A, que denotamos A'. Esta matriz A' é triangular superior, e sua diagonal contém apenas zeros e uns.
Agora realizamos operações elementares *em colunas* até obter a forma escalonada reduzida por colunas de A', que denotaremos por A''. As operações em colunas não mudam a parte abaixo da diagonal, que continha zeros – mas também transforma a parte superior de forma que contenha zeros. A matriz A'' é agora triangular inferior, também.
A'' é triangular inferior e superior – ou seja, é diagonal. Além disso, os elementos da diagonal são uns e zeros. A quantidade de linhas L.I. e a quantidade de colunas L.I. é claramente a mesma (e é igual à quantidade de uns na diagonal).

Resp. (Ex. 96) —

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

$$D = \begin{pmatrix} 1 & 0 & 0 \\ -2/x & 1 & 0 \\ 3/x & -3/2 & 1 \end{pmatrix} \begin{pmatrix} x & x & x^2 \\ 0 & 4 & 3x \\ 0 & 0 & \frac{5x}{2} \end{pmatrix}$$

Resp. (Ex. 97) — Decomponha $A = LU$. Queremos portanto $X = (LU)^{-1}B$, ou seja, $LUX = B$. Usamos a mesma idéia da Seção 4.8.1 para obter as colunas de X individualmente.

Resp. (Ex. 100) — Use indução em k e o Teorema α.42.

Resp. (Ex. 107) — Seja $\mathcal{S}$ o espaço de matrizes simétricas e $\mathcal{A}$ o espaço das matrizes anti-simétricas. Defina uma transfomração $T : \mathcal{S} \to \mathcal{A}$ com $T(M) = DM - MD$. Mostre que o núcleo de T é o espaço das matrizes diagonais, e que portanto T tem posto

$$\frac{n(n+1)}{2} - n = \frac{n(n-1)}{2}.$$

Assim, T é sobrejetora, e para cada $A \in \mathcal{A}$, existe uma simétrica S tal que $A = T(S) = DS - SD$.

Resp. (Ex. 109) — O método multiplica a matriz (que denotaremos por A) por diversas matrizes elementares até chegar à identidade, portanto $E_k E_{k-1} \dots E_1 A = \mathcal{I}$. Mas

$$\begin{aligned} E_k E_{k-1} \dots E_1 A &= \mathcal{I} \\ E_k E_{k-1} \dots E_1 &= A^{-1} \qquad \text{(multiplique à direita por } A^{-1}\text{)} \\ E_k E_{k-1} \dots E_1 \mathcal{I} &= A^{-1}. \end{aligned}$$

Mas a última linha acima descreve exatamente a sequência de operações que o método também aplica na identidade, e portanto a matriz à direita é de fato A^{-1}.

Resp. (Ex. 110) — A matriz com uns na diagonal secundária,

$$\begin{pmatrix} 0 & \cdots & & 0 & 1 \\ \vdots & & & 1 & 0 \\ & & \iddots & & \\ 0 & 1 & & & \vdots \\ 1 & 0 & & \cdots & 0 \end{pmatrix}$$

Resp. (Ex. 115) — Faça a multiplicação por blocos: para a primeira matriz,

$$\left(\begin{array}{c|c} R & \mathbf{0} \\ \hline \mathbf{0}^T & 1 \end{array}\right) \begin{pmatrix} \mathbf{v} \\ \hline z \end{pmatrix} = \begin{pmatrix} R\mathbf{v} \\ \hline z \end{pmatrix},$$

onde $\mathbf{v} - (x, y)^\top$.
Para a segunda, faça o mesmo, mas permutando linhas e colunas antes.

Resp. (Ex. 119) — É importante definir claramente o que precisa ser provado: (i) Que $A = [\mathrm{id}]_{B\to D}$, ou seja, que ao aplicarmos A na base B, *obtemos uma outra base para o mesmo espaço vetorial* – para isto basta mostrar que a aplicação re A na base B resulta na mesma quantidade de vetores LI. (ii) Que $A = [\mathrm{id}]_{E\to B}$. Para isto basta observar que $AE = B$, e portanto $E = A^{-1}B$. Mostre que E também é uma base, ou seja, que A^{-1} aplicada em B resulta em n vetores LI.

Resp. (Ex. 122) —

$$(a)\ \mathbf{x} = \begin{pmatrix} (-9i-3)/10 \\ (2i+9)/20 \\ (i+2)/20 \end{pmatrix}$$

$$(b)\ \mathbf{x} = \begin{pmatrix} (i-1)/10 \\ (4-i)/20 \\ 1/20 \end{pmatrix}$$

$$(c)\ \mathbf{x} = \begin{pmatrix} (1-4i)/5 \\ (3+7i)/20 \\ (3i+5)/20 \end{pmatrix}$$

Resp. (Ex. 123) — Na última matriz, observe que se subtraírmos o dobro da primeira linha à terceira obtemos

$$\begin{pmatrix} 2 & 3 & 7 & -1 & 0 \\ 22 & 12 & 3/2 & 15 & -2 \\ 47 & 0 & 0 & 0 & 0 \\ 10 & 3 & 3/2 & 34 & -2 \\ -91 & 16 & 0 & 0 & 0 \end{pmatrix}$$

Se subtraírmos ainda a segunda linha da quarta, teremos

$$\begin{pmatrix} 2 & 3 & 7 & -1 & 0 \\ 22 & 12 & 3/2 & 15 & -2 \\ 47 & 0 & 0 & 0 & 0 \\ -12 & -9 & 0 & 19 & 0 \\ -91 & 16 & 0 & 0 & 0 \end{pmatrix}$$

Permute linhas e colunas para obter uma matriz triangular.

Resp. (Ex. 125) — (Dica) a fórmula divide o determinante (volume de um paralelepípedo) por 2 e também por 3.

Resp. (Ex. 128) — Sejam α e β duas bases. Então

$$\begin{aligned}
[A]_\alpha &= [\mathrm{id}]_{\beta,\alpha}\,[A]_\beta\,[\mathrm{id}]_{\alpha,\beta} \\
\det[A]_\alpha &= \det\left([\mathrm{id}]_{\beta,\alpha}\,[A]_\beta\,[\mathrm{id}]_{\alpha,\beta}\right) \\
&= \det\left([\mathrm{id}]_{\beta,\alpha}\,[A]_\beta\,[\mathrm{id}]^{-1}_{\beta,\alpha}\right) && ([\mathrm{id}]_{\alpha,\beta} = [\mathrm{id}]^{-1}_{\beta,\alpha}) \\
&= \det\left([\mathrm{id}]_{\beta,\alpha}\right)\,\det\left([A]_\beta\right)\,\det\left([\mathrm{id}]^{-1}_{\beta,\alpha}\right) \\
&= k\det\left([A]_\beta\right)k^{-1} && (k = \det[\mathrm{id}]_{\beta,\alpha}) \\
&= \det[A]_\beta .
\end{aligned}$$

Resp. (Ex. 131) — $\det A' = +d$ se k for par, ou $-d$ se k for ímpar.

Resp. (Ex. 133) — (i) Mostre que $\det(E) = \det(E^T)$. (iv) A é produto de matrizes elementares?

Resp. (Ex. 138) — Esta função usa módulo, e $|x|$ não é linear. Assim, a função não é multilinear nas colunas da matriz.

Resp. (Ex. 139) — Compare o posto da transformação com o da matriz.

Resp. (Ex. 140) — (a) Uma das maneiras é mostrar que $B_nC_n = P_n$. Outra é escalonar P_n. (b) Use a expansão de Laplace na primeira linha ou coluna. (c) Na demonstração de (b), foi usada a expansão de laplace numa linha com uns. Se ao invés de uns tivermos uma constante c ao longo de uma linha de uma matriz qualquer, a expansão de Laplace nos dará

$$\det(M + K) = (\det M)(c + k)/c$$

Resp. (Ex. 143) — Comece construíndo uma matriz com blocos

$$\begin{pmatrix} \mathcal{I}_n & -A \\ B & \mathcal{I}_k \end{pmatrix}$$

e use decomposição LU em blocos.

Resp. (Ex. 145) — $\mathbb{Z}_2$, porque todo elemento é seu próprio inverso aditivo, e portanto $a + b = a - b$.

Resp. (Ex. 146) — As de ordem ímpar. Observe que $A^T = -A$. Calcule o determinante em ambos os lados, obtendo $\det(A^T) = \det(-A)$. Assim, $\det(A^T) = (-1^n)\det(A)$. Quando n é ímpar, necessariamente $\det(A) = 0$.

Resp. (Ex. 148) — $a = 17/2$.

Resp. (Ex. 150) — (i), (ii): São LI em qualquer intervalo real. O Wronskiano é e^x, que sempre é diferente de zero. (iii) Pelo teste do Wronskiano, são LI em qualquer intervalo contendo $x = 1$. Além disso, para que as funções fossem LD deveria haver uma constante k tal que $k(x^x) = e^x$. Mas isso significaria que

$$k = \frac{e^x}{x^x},$$

e portanto k não seria constante, e sim uma função de x estritamente decrescente em x, e sempre diferente de zero. (Isso reforça que o teste do Wronskiano identifica que funções são LI apenas em alguns e em alguns intervalos, mas não necessariamente todos).

Resp. (Ex. 153) — O determinante é

$$\begin{aligned}&(1 \wedge 1 \wedge 1) \oplus (1 \wedge 1 \wedge 1) \oplus (0 \wedge 0 \wedge 0)\\ \oplus&(0 \wedge 1 \wedge 1) \oplus (1 \wedge 0 \wedge 0) \oplus (1 \wedge 0 \wedge 1)\\ =&1 \oplus 1 = 0\end{aligned}$$

Resp. (Ex. 154) — Argumente usando a fórmula de Leibniz.

Resp. (Ex. 155) — O determinante de A^{-1} é $1/\det(A)$, portanto para que a matriz tenha inversa com entradas inteiras, seu determinate deve ter inverso inteiro – o que significa que deve ser $+1$ ou -1.

Resp. (Ex. 156) — A matriz A dos coeficientes e as matrizes A_i são

$$A = \begin{pmatrix}1 & 1 & 1\\ 1 & 1 & 0\\ 0 & 1 & 1\end{pmatrix}, \quad A_1 = \begin{pmatrix}0 & 1 & 1\\ 1 & 1 & 0\\ 1 & 1 & 1\end{pmatrix}, \quad A_2 = \begin{pmatrix}1 & 0 & 1\\ 1 & 1 & 0\\ 0 & 1 & 1\end{pmatrix}, \quad A_3 = \begin{pmatrix}1 & 1 & 0\\ 1 & 1 & 1\\ 0 & 1 & 1\end{pmatrix},$$

Os determinantes são:

$$\det(A) = 1, \det(A_1) = 1, \det(A_2) = 0, \det(A_3) = 1$$

O vetor $\mathbf{b}$ é

$$\begin{pmatrix}0\\ 1\\ 1\end{pmatrix}$$

Finalmente, obtemos

$$\begin{aligned}x_1 =& \frac{\det(A_1)}{\det A} = 1 \wedge 1^{-1} = 1 \wedge 1 = 1,\\ x_2 =& \frac{\det(A_2)}{\det(A)} = 0 \wedge 1^{-1} = 0 \wedge 1 = 0,\end{aligned}$$

$$x_3 = \frac{\det(A_3)}{\det(A)} = 1 \wedge 1^{-1} = 1 \wedge 1 = 1.$$

Pode-se substituir os x_i no sistema para verificar a validade da solução.

$$\begin{aligned} x_1 \oplus x_2 \oplus x_3 &= 1 \oplus 0 \oplus 1 = 0 \\ x_1 \oplus x_2 &= 1 \oplus 0 = 1 \\ x_2 \oplus x_3 &= 0 \oplus 1 = 1 \end{aligned}$$

Resp. (Ex. 157) — Se

$$f(a + bi) = A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

então

$$\det A = \det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2 - [b(-b)] = a^2 + b^2,$$

que é o quadrado da norma (valor absoluto) do número complexo dado.

Resp. (Ex. 158) — Somente 1, -1 e 0, de outra forma haveria uma submatriz quadrada de ordem um com determinante diferente de ± 1 e diferente de zero.

Resp. (Ex. 159) — A parte fixa das soluções é inteira. A outra parte não.

Resp. (Ex. 160) — $\mathbb{Z}_2^n$, e de maneira geral, espaços sobre o corpo $\mathbb{Z}_2$. Se agregarmos os vetores para formar uma matriz e calcularmos seu determinante, ele será necessariamente $+1$ ou 0, que são os únicos escalares neste espaço (lembre-se que $\mathbb{Z}_2 = \{0, 1\}$). Assim, quando o determinante é zero, há vetores linearmente dependentes, e não temos uma base. Quando temos de fato uma base, o determinante será sempre um.

Resp. (Ex. 161) — Trivialmente, não! Basta considerar $T(\mathbf{v} = \mathbf{0})$. De maneira mais geral, multiplicação por escalar é uma transformação linear, e se multiplicarmos uma matriz inteira por um escalar c, teremos multiplicado seu determinante (e consequentemente seu volume) por c^n.

Resp. (Ex. 162) — a_n é a sequência de Fibonacci, deslocada em uma posição: $a_n = F_{n+1}$. Faça a demonstração por indução na ordem da matriz, usando a expansão de Laplace na primeira coluna, por exemplo, para mostrar que $\det A_n = \det A_{n-1} + \det A_{n-2}$.

Resp. (Ex. 164) — (ii) e (vi), sim. Ou outros, não. Em (i), os elementos não tem inverso; em (iii), as matrizes singulares não tem inverso; em (iv), a matriz com determinante 3, por exemplo, não tem inversa, porque o determinante teria que ser $1/3$; em (v) também, a matriz com determinante 2 não tem inversa.

Resp. (Ex. 165) — Tente por indução, usando a expansão de Laplace.

Resp. (Ex. 169) — Um contraexemplo:

$$A = \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix} B = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

Tanto A como B tem polinômio característico $x^2 - 4x + 4$, mas não são similares.

Resp. (Ex. 170) — Verifique primeiro para matrizes triangulares. Depois, mostre que se o Teorema vale para uma matriz M, vale para matrizes obtidas a partir de M com operações elementares.

Resp. (Ex. 173) —

$$\det(R - \lambda\mathcal{I}) = \det \begin{pmatrix} \cos\theta - \lambda & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta - \lambda \end{pmatrix} = (\cos\theta - \lambda)^2 + \operatorname{sen}^2\theta,$$

e os autovalores seriam os λ tais que

$$\begin{aligned} \cos^2\theta - 2\lambda\cos\theta + \lambda^2 + \operatorname{sen}^2\theta &= 0 \\ 1 - 2\lambda\cos\theta + \lambda^2 &= 0. \qquad (\cos^2\theta + \operatorname{sen}^2\theta = 1) \end{aligned}$$

Usando a fórmula de Bhaskara com

$$\begin{aligned} a &= 1 \\ b &= -2\cos\theta \\ c &= 1 \end{aligned}$$

temos

$$\begin{aligned} \lambda &= \frac{2\cos\theta \pm \sqrt{(-2\cos\theta)^2 - 4}}{2} \\ &= \frac{2\cos\theta \pm \sqrt{4(-\cos^2\theta - 1)}}{2} \\ &= \frac{2\cos\theta \pm 2\sqrt{\cos^2\theta - 1}}{2} \\ &= \cos\theta \pm 2\sqrt{\cos^2\theta - 1} \end{aligned}$$

Como $\cos^2\theta \leq 1$, o valor dentro da raiz será negativo, exceto quando $\theta = k\pi$, com $k \in \mathbb{Z}$.

Resp. (Ex. 175) — Nenhum.

Resp. (Ex. 177) —

$$\begin{pmatrix} 1 & 4 \\ 9 & 1 \end{pmatrix}$$

Resp. (Ex. 180) — (a) Autovalor 1 com multiplicidade dois. Autovetor $(0,1)^T$. (b) $\lambda_1 = 1, \lambda_2 = 0$. Autovetores $(0,1,1)^T$ e $(0,1,0)^T$.

Resp. (Ex. 182) — Resolvendo $AB = BA$, obtemos $x = 2, y = 4$.

Resp. (Ex. 183) — (a) $\lambda_1 = i + 1, \lambda_2 = 0$. Autovetores $(1,-1)^T$ e $(1,i)^T$. (b) $\lambda_1 = 2 + \sqrt{2}, \lambda_2 = 1$. Autovetores $(1, -\frac{\sqrt{2}+2}{2})^T$ e $(1,0)^T$.

Resp. (Ex. 184) —

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

$$-x^3 + x^2 - 2x + 2,$$

autovalores $1, -i\sqrt{2}, i\sqrt{2}$. Autovetores:

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -i\sqrt{2} \\ -2 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -i\sqrt{2} \\ -2 \end{pmatrix}.$$

Resp. (Ex. 190) — (Dica) Escreva a matriz como

$$\begin{pmatrix} p & (1-p) \\ q & (1-q) \end{pmatrix},$$

E observe que o traço da matriz é a soma de seus autovalores.

Resp. (Ex. 191) — Sobre $\mathbb{C}$ não, porque $\mathcal{I}$ é hermitiana, mas $i\mathcal{I}$ não é. Sobre $\mathbb{R}$, sim.

Resp. (Ex. 192) — (Dica) A e A^T tem os mesmos autovalores. Quem é $A^T\mathbf{e}$, e como isso leva à validade do teorema?

Resp. (Ex. 208) — Possivelmente o exemplo mais simples é $e(x) = f(x) = x$, $g(x) = h(x) = -x$.

Resp. (Ex. 216) — Aquela é a base canônica rotacionada no sentido anti-horário por um ângulo igual a $\pi/4$, como pode-se facilmente verificar.

Resp. (Ex. 221) — O operador de projeção deve levar $\mathbf{v} = \mathbf{u} + \mathbf{w}$ em $\mathbf{u}$. O polinômio x^5 é igual à soma

$$x^5 + 0,$$

por isso uma projeção em $\mathbb{R}_3[x]$ teria que levar x^5 em zero. A derivada sexta é uma projeção de $\mathbb{R}_5[x]$ em $\mathbb{R}_3[x]$, mas neste contexto ela é igual à função zero.

Resp. (Ex. 231) — Este produto interno dá a *paridade* da quantidade total de arestas comuns nos dois grafos (será zero quando for par e um quando for ímpar). Dois grafos serão ortogonais quando tiverem número par de arestas em comum.

Resp. (Ex. 238) — Defina $B = A^T A$ (ou $A^H A$, se quiser demonstrar para complexos). Verifique que a diagonal de B contém os quadrados das normas das colunas de A. Verifique então os casos em que A é ou não é positiva e invertível.

Resp. (Ex. 239) — Considere o cone convexo gerado pelas colunas de A; pense em como descrever um vetor qualquer em $\mathbb{R}^2$ usando as colunas de A (como são os coeficientes?) Depois, trate dois casos: $\mathbf{b}$ pertence ao cone gerado por A; e $\mathbf{b}$ não pertence ao cone. No segundo caso, você pode argumentar que há algu vetor formando ângulo menor que $\pi/4$ com o cone definido por A.

Resp. (Ex. 241) — As matrizes com linhas e colunas *ortogonais*, mas não *ortonormais*.

Resp. (Ex. 248) — A decomposição QR *não* é única, mas aqui há uma possibilidade.

$$Q_A = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \quad R_A = \begin{pmatrix} -2 & 00 \\ & -1 \end{pmatrix}$$

$$Q_B = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{3} & -1/\sqrt{6} \\ 0 & 1/\sqrt{3} & 2/\sqrt{6} \\ 1/\sqrt{2} & -1/\sqrt{3} & 1/\sqrt{6} \end{pmatrix}, \quad R_B = \begin{pmatrix} \sqrt{2} & \sqrt{2} & 1/\sqrt{2} \\ 0 & \sqrt{3} & 0 \\ 0 & 0 & \sqrt{6}/2 \end{pmatrix}$$

Resp. (Ex. 249) —

$$A^+ = \frac{1}{50}\begin{pmatrix} 1 & 3 \\ 1 & 3 \end{pmatrix}, \quad B^+ = \frac{1}{5}\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}, \quad C^+ = \begin{pmatrix} 1/10 & -1/5 & 0 \\ -1/3 & 5/6 & 1/6 \\ 3/10 & -3/5 & 0 \end{pmatrix}$$

Resp. (Ex. 252) — $A^+ = A^T(AA^T)^{-1}$.

Resp. (Ex. 253) — (i) A pseudoinversa de A é

$$A^+ = \frac{1}{15}\begin{pmatrix} 2 & -1 \\ 4 & -2 \\ 2 & -1 \end{pmatrix}$$

Resp. (Ex. 257) —

$$A:\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad B:\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad C:\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad D:\begin{pmatrix} 2 & 1 & 0 & \dots & 0 \\ 0 & 2 & 0 & & \\ 0 & 0 & \ddots & & \\ \vdots & 0 & \ddots & 2 & 1 \\ 0 & 0 & & 0 & 2 \end{pmatrix}$$

Resp. (Ex. 258) — Basta usar a definição de exponencial de matriz.

Resp. (Ex. 260) — Os autovalores de N são todos zero, portanto $\det N = 0$. O determinante de $\mathcal{I} + N$ é, portanto, 1, o que significa que $\mathcal{I} + N$ não é singular.

Resp. (Ex. 263) — Em $\mathbb{R}$ somente duas, $+x$ e $-x$. Em $\mathbb{R}^n$, com $n \geq 2$, infinitas.

Resp. (Ex. 264) — Sim, aqueles em que o corpo subjacente é discreto e finito. Por exemplo, $\mathbb{Z}_2^n$ ou o espaço de ciclos em um grafo.

Resp. (Ex. 266) — (Dica) Os vetores devem necessariamente ser LD e irracionais.

Resp. (Ex. 269) — A base $\left(\begin{smallmatrix} 2 & 1 \\ 0 & -2 \end{smallmatrix}\right)$ é menor.

Resp. (Ex. 273) — Se $\mathbf{x}^T A\mathbf{x} > 0$ e $\mathbf{x}^T B\mathbf{x} > 0$, então

$$\begin{aligned} \mathbf{x}^T(A+B)\mathbf{x} &= (\mathbf{x}^T A + \mathbf{x}^T B)\mathbf{x} \\ &= \mathbf{x}^T A\mathbf{x} + \mathbf{x}^T B\mathbf{x} \\ &> 0. \end{aligned}$$

De maneira semelhante, se $k \in \mathbb{R}^+$,

$$\mathbf{x}^T(kA)\mathbf{x} = k\mathbf{x}^T A\mathbf{x} > 0$$

Resp. (Ex. 274) — A demonstração do Teorema 12.20 pode ser adaptada:

$$\begin{aligned}
\det B &= \det A \det(DD) \\
(\det B)^2 &= (\det A \det(DD))^2 \\
(\det B)^2 &= (\det A)^2 \left(\frac{1}{\prod \sqrt{a_{ii}}}\right)^4 \\
(\det B)^2 &= \frac{(\det A)^2}{\prod {a_{ii}}^2} \\
\prod {a_{ii}}^2 (\det B)^2 &= (\det A)^2
\end{aligned}$$

Como $0 < \det B \leq 1$, temos

$$\left(\prod a_{ii}\right)^2 \geq (\det A)^2$$

e consequentemente,

$$\begin{aligned}
\left|\prod a_{ii}\right| &\geq |\det A| \\
\prod a_{ii} &\geq |\det A| \qquad \text{(porque os } a_{ii} \text{ são positivos)}
\end{aligned}$$

Resp. (Ex. 275) — (Rascunho, somente $\Rightarrow$) Por indução no número de dimensões: a base é o elipsóide em $\mathbb{R}^3$. Para o passo, seja Q a forma quadrática em $\mathbb{R}^n$. Se fixarmos uma das coordenadas x_i da figura geométrica definida por Q, estamos projetando uma forma quadrática em $\mathbb{R}^{n-1}$, que também é semidefinida positiva (explique porque!). Assim, *as coordenadas* x_j, *com* $j \neq i$, *são limitadas.* Agora fixamos x_k, com $k \neq i$, e repetimos o argumento para mostrar que os valores de x_i também são limitados.

Resp. (Ex. 278) — Uma forma com $\mathrm{In}(A) = (1, 0, 1)$ é $ax^2 = k$, que no plano define duas retas paralelas, dadas por $x = \pm\sqrt{k}$. A equação só é satisfeita nessas duas retas. É importante notar que esta equação *não* descreve uma parábola!
Já uma forma com $\mathrm{In}(B) = (1, 0, 2)$ é, também $ax^2 = k$, mas em $\mathbb{R}^3$, e portanto só é satisfeita quando $x = \pm\sqrt{k}$ – definindo dois planos paralelos.

Resp. (Ex. 282) — Não:

$$\nabla^2 f(a, b) = \begin{pmatrix} e^a & \\ & \frac{1}{b^2} \end{pmatrix}$$

e

$$\mathbf{x}^T \nabla^2 f(a, b)\mathbf{x} = e^a x_1^2 - \frac{x_2^2}{b^2}.$$

Com $x_1 = 0$, temos $-\frac{x_2^2}{b^2}$ negativo para todos x_2 e b.
Ou ainda, geometricamente, se fixarmos a temos a função $\log(b)$, que não é convexa.
No entanto, $g(a, b) = e^a - \log(b)$ é convexa, porque é soma de duas funções convexas. Ou ainda, porque

$$\mathbf{x}^T \nabla^2 g(a, b)\mathbf{x} = e^a x_1^2 + \frac{x_2^2}{b^2}$$

é sempre positivo.

Resp. (Ex. 284) — $x_2 > 0$.

Resp. (Ex. 286) — $x_1x_1 \oplus x_1x_3 \oplus x_2x_3$.

Resp. (Ex. 287) — É igual à quantidade de matrizes triangulares superiores com valores 0 ou 1. Há

$$\left\lceil \frac{n^2}{2} \right\rceil - \left\lfloor \frac{n}{2} \right\rfloor$$

valores possíveis, portanto a quantidade é

$$2^{\left(\left\lceil \frac{n^2}{2} \right\rceil - \left\lfloor \frac{n}{2} \right\rfloor\right)}$$

se incluirmos a forma $f(x) = 0$.
A notação $\lceil x \rceil$ significa "arredondamento para cima" (menor inteiro maior ou igual a x), e $\lfloor x \rfloor$ significa"arredondamento para baixo" (maior inteiro menor ou igual a x).

Resp. (Ex. 294) — Sim! Primeiro: é composição de $g[(x, y)^T] = (0, 0)$, linear, com a translação $h[(a, b)^T] = (a + 1, b + 1)$, uma translação.
Para uma demonstração algébrica, veja que

$$\begin{aligned} af[(p, q)^T] + bf[(x, y)^T] &= a(1, 1)^T + b(1, 1)^T \\ &= (a + b)(1, 1)^T \\ &= (a + b)f[\star] \\ &= af[\star] + bf[\star] \\ &= af[(p, q)^T] + bf[(x, y)^T], \end{aligned}$$

onde $\star$ significa "todo e qualquer argumento".

Resp. (Ex. 303) — $a_n = 0$ para funções ímpares; $b_n = 0$ para funções pares.

Resp. (Ex. 303) — Para $f(x)$,

$$\frac{8}{\pi} \sum_{i=1}^{\infty} \frac{n \operatorname{sen}(2nx)}{4n^2 - 1}$$

Resp. (Ex. 304) — (Dica) Use a fórmula de Euler, $e^{ix} = \cos(x) + i \operatorname{sen}(x)$.

Resp. (Ex. 307) — O teorema é demonstrado facilmente, já que a transformada de Fourier é uma integral definida.

Resp. (Ex. 308) — (a) $\mathbf{F}(\phi) = i\sqrt{-i}e^{-i\pi\phi^2}$.
(b) $(\sqrt{\pi/2})\ \left[\operatorname{sen}(\pi^2\phi^2) + \cos(\pi^2\phi^2)\right]$

Resp. (Ex. 309) — (ii) Observe que com $t = 0$ a série é telescópica.

Resp. (Ex. 311) — Por exemplo, $e^{2\pi i n x/L}$, com $n = 0, \pm1, \pm2, \ldots$

Resp. (Ex. 317) — Você pode argumentar observando que se V é isomorfo a $\mathbb{R}^n$, e seus vetores podem ser representados como colunas de n elementos, então o espaço dual é o espaço de todas as *linhas* de n elementos.

Resp. (Ex. 319) — (a) indeterminado: $x_1 = (9x_3+2)/5$, e $x_2 = (16x_3+3)/5$. (b) x_1 $= \frac{9}{2}$, x_2 $= \frac{1}{2}$, x_3 $= \frac{15}{2}$. (c) x_1 $= \frac{331}{49}$, x_2 $= \frac{80}{49}$, x_3 $= -\frac{80}{49}$, x_4 $= -\frac{50}{49}$. (d) há uma linha redundante ($l_3 = 2[l_1 + l_2]$). O resultado é indeterminado: $x_1 = (4x_3-1)/7$, $x_2 = (-15x_3-2)/7$. (e) $x_1 = 14/15$, $x_2 = -2/5$, $x_3 = 7/5$. (f) inconsistente.

Resp. (Ex. 321) — Exemplos:

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} -2 & 6 \\ -1 & 3 \end{pmatrix}.$$

Resp. (Ex. 322) — $a \neq 0$, $a \neq 3$.

Resp. (Ex. 325) — Primeiro apresentamos um argumento intuitivo: o elemento i, j de AB é construído somando uma um os produtos dos elementos da linha i de A com a coluna j de B. Como na transposta a i-éima linha torna-se a i-ésima coluna, temos o mesmo que se usarmos da i-ésima *linha* de B^T com a j-ésima *coluna* de A^T. Isso só é possível se trocarmos a ordem das matrizes, porque $A_{m\times p}$ transposta é $A^T_{p\times n}$, e $B_{p\times n}$ transposta é $B_{n\times p}$ – As seguintes matrizes são compatíveis para multiplicação:

$$A_{m\times p} \text{ e } B_{p\times n}$$
$$B^T_{n\times p} \text{ e } A^T_{p\times m}.$$

Desenvolvemos uma demonstração algébrica a seguir.
O elemento na linha l e coluna c de XY (para quaisquer matrizes X e Y compatíveis para esta operação) é

$$(XY)_{lc} = \sum_{k=1}^{p} X_{lk}Y_{kc}. \qquad (\alpha.1)$$

Agora seja A uma matriz $m \times p$ e B uma matriz $p \times n$. Então

$$\begin{aligned}
(B^T A^T)_{ij} &= \sum_{k=1}^{p} (B^T)_{ik}(A^T)_{kj} && \text{(por } (\alpha.1)\text{)} \\
&= \sum_{k=1}^{p} B_{ki}A_{jk} && \text{(na transposta trocamos os índices)} \\
&= \sum_{k=1}^{p} A_{jk}B_{ki} && \text{(comutatividade de produto de reais)} \\
&= (AB)_{ji} && \text{(por } (\alpha.1)\text{)} \\
&= (AB)^T_{ij}.
\end{aligned}$$

Resp. (Ex. 326) — As matrizes devem ser da forma

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

Quando multiplicamos duas matrizes, obtemos a soma dos elementos na posição $1, 2$:

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$$

Resp. (Ex. 329) — (a) $2Fe + 3Cl_2 \to 2FeCl_3$
(b) $2KMnO_4 + 16HCl = 2KCl + 2MnCl_2 + 8H_2O + 5Cl_2$
(c) $5PhCH_3 + 6KMnO_4 + 9H_2SO_4 = 5PhCOOH + 3K_2SO_4 + 6MnSO_4 + 14H_2O$

Resp. (Ex. 340) — Por indução em n.
Base: Com $n = 0$, temos $2 < 4$.
Hipótese: Presumimos que

$$f(n) < 4.$$

Passo: Será fácil se partirmos da hipótese:

$$\begin{aligned}
f(n) &< 4 \\
2\sqrt{f(n)} &< 2\sqrt{4} && \text{(aplicamos } f() \text{ p/obter } f(n+1)\text{)} \\
f(n+1) &< 4.
\end{aligned}$$

E o passo está feito, concluíndo a demonstração.

Resp. (Ex. 350) — É mais fácil não tentar diretamente induzir em n.

Resp. (Ex. 351) — Divida a matriz de ordem $n+1$ em blocos, isolando o $n+1$-ésimo elemento da diagonal.

Resp. (Ex. 354) — A^n é igual a A exceto pelo elemento não-zero fora da diagonal, que era um e passa a ser n.

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 0 & n & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Resp. (Ex. 361) — Desenhe o círculo unitário e calcule $\operatorname{sen}(x)$, $\operatorname{sen}^2(x)$ e $\operatorname{sen}^3(x)$ para algum x. Daí sai uma idéia que pode ser usada no passo de indução.

Resp. (Ex. 363) — Base: para $n = 0$,

$$\int_0^\infty t^0 e^{-t}\,dt = -e^{-t}|_0^\infty = 0 + 1 = 0!$$

Presumimos por hipótese que a igualdade é válida para k,

$$\int_0^\infty t^k e^{-t}\,dt = k!$$

E calculamos a integral para $k+1$:

$$\begin{aligned} \int_0^\infty t^{k+1} e^{-t}\,dt &= x^{k+1}(-e^{-x})|_0^\infty + \int_0^\infty e^{-x}(k+1)x^k\,dx && \text{(por partes)} \\ &= 0 + (k+1)\int_0^\infty e^{-t}t^k\,dt \\ &= (k+1)k! && \text{(usando a hipótese de indução)} \\ &= (k+1)! \end{aligned}$$

Resp. (Ex. 369) — Integre

$$\frac{1}{2}\int_{-\pi/2}^{\pi/2} \cos^{2n+1}(x)\,dx$$

por partes, usando

$$\begin{aligned} u &= \cos^{2n-1}(x), \\ dv &= \cos^2(x)\,dx. \end{aligned}$$

Resp. (Ex. 371) — Cuidado com as extremidades do intervalo! Prove para um ponto interno, e depois faça passos para a frente e para trás.

Resp. (Ex. 372) — (Rascunho de prova) Primeiro mostre que o teorema vale para bases de $\mathbb{R}^2$. Depois, suponha que $\mathbf{b}_i$ e $\mathbf{b}_j$, com $i < j$, pertencem a uma base B de $\mathbb{R}^n$. O subespaço gerado por estes dois vetores é $\mathbb{R}^2$. Se os trocarmos de posição, continuarão gerando $\mathbb{R}^2$, mas terão orientação oposta. Ou seja, não podemos transformar continuamente $(\mathbf{b}_i, \mathbf{b}_j)^T$ em $(\mathbf{b}_j, \mathbf{b}_i)^T$ sem passar por algum par que não seja base, como na definição $\gamma.1$. Daqui em diante, argumentar que $(\ldots, \mathbf{b}_i, \mathbf{b}_j, \ldots)^T$ e $(\ldots, \mathbf{b}_j, \mathbf{b}_i, \ldots)^T$ tem orientações opostas é fácil.

Resp. (Ex. 373) — Tente com as funções $f(x) = 1$, constante, e $g(x) = x$.

Resp. (Ex. 374) — (a — viii) (b — vi) (e — iv) (f — vii) (g — v)

Resp. (Ex. 375) — (i) $y^2 - x^2 = c$ (ii) $y = ae^{-\operatorname{sen}(x)}$ (iii) $x^{-1} + \log(x) - y\operatorname{sen}(y) - \operatorname{sen}(y) - \cos(y)$ (iv) $a\sqrt{e^x}$ (v) $y = -\arccos[(x-1)e^x - e^x]$

Ficha Técnica

Este texto foi produzido inteiramente em LaTeX em sistema Debian GNU/Linux. Os diagramas foram criados sem editor gráfico, usando diretamente os pacotes TikZ e Asymptote, exceto pela figura do conjunto de Mandelbrot na página 80, que foi produzida pelo programa Fraqtive. O ambiente Emacs foi usado para edição do texto LaTeX, e os sistemas Octave e Maxima foram usados na preparação dos exemplos.

Bibliografia

[Apo69] Tom M. Apostol. *Calculus*. 2ª ed. Vol. 2. Wiley, 1969. ISBN: 978-0471000075.

[Apo74] Tom Mike Apostol. *Mathematical Analysis*. 2ª ed. Pearson, 1974. ISBN: 978-0201002881.

[Art88] Emil Artin. *Geometric Algebra*. Wiley, 1988. ISBN: 0-471-60839-4.

[Ash08] Robert B. Ash. *Basic Probability Theory*. Dover, 2008. ISBN: 978-0-486-46628-6.

[ASS02] Kenneth J. Arrow, A. K. Sen e Kotaro Suzumura. *Handbook of Social Choice and Welfare*. Vol. 1. North Holland, 2002. ISBN: 978-0444829146.

[ASS10] Kenneth J. Arrow, A. K. Sen e Kotaro Suzumura. *Handbook of Social Choice and Welfare*. Vol. 2. North Holland, 2010. ISBN: 978-0444508942.

[Bar09] Gregory V. Bard. *Algebraic Cryptanalysis*. Springer, 2009. ISBN: 978-0387887562.

[BC11] James Brown e Ruel Churchill. *Fourier Series and Boundary Value Problems*. McGraw-Hill, 2011. ISBN: 978-0078035975.

[Bea62] H. S. Bear. *Differential Equations: a concise course*. Dover, 1990 (orig. 1962). ISBN: 0-486-40678-4.

[Bis93] David M. Bishop. *Group Theory and Chemistry*. Dover, 1993. ISBN: 0-486-67355-3.

[BJS90] M. S. Bazaraa, J. J. Jarvis e H. D. Sherali. *Linear Programming and Network Flows*. John Wiley & Sons, 1990.

[Bla58] Duncan Black. *Theory Committees and Elections*. Cambridge University Press, 1958. ISBN: 978-0521141208.

[BM08] J. A Bondy e U. S. R Murty. *Graph theory*. Springer, 2008. ISBN: 978-1846289699.

[Bol+86] José Luiz Boldrini et al. *Álgebra Lienar*. 3ª ed. Harbra, 1986.

[Bre08] Pierre Bremaud. *Markov Chains: Gibbs Fields, Monte Carlo Simulation, and Queues*. Springer, 2008. ISBN: 978-0387985091.

[Bro95] Robert S. Brodkey. *The Phenomena of Fluid Motions*. Dover, 1995. ISBN: 978-0486686059.

[BT97] Dimitris Bertimas e John N Tsitsiklis. *Introduction to linear Optimization*. Athena Scientific, 1997.

[CDS80] Dragos M. Cvetković, Michael Doob e Horst Sachs. *Spectra of Graphs: theory and applications*. Academic Press, 1980. ISBN: 0-12-195150-2.

[Çin13] Erhan Çinlar. *Introduction to Stochastic Processes*. Dover, 2013. ISBN: 978-0486497976.

[Cod61] Earl A. Coddington. *An Introduction to Ordinary Differential Equations*. Dover, 1989 (orig. 1961). ISBN: 978-0-486-65942-8.

[Col88] Dadid Colton. *Partial Differencial Equations: an introdution*. Dover, 1988. ISBN: 978-0-486-43834-4.

[Cor97] J. F. Cornwell. *Group Theory in Physics: and introduction*. Academic Press, 1997. ISBN: 0-12-189800-8.

[Cox08] H. S. M. Coxeter. *Projective Geometry*. 2ª ed. Springer, 2008. ISBN: 978-0387406237.

[DAB01] Sumner P. Davis, Mark C. Abrams e James W. Brault. *Fourier Transform Spectrometry*. Academic Press, 2001. ISBN: 978-0120425105.

[Dav89] Harry F. Davis. *Fourier Series and Orthogonal Functions*. Dover, 1989. ISBN: 978-0486659732.

[DFM07] Leo Dorst, Daniel Fontijne e Stephen Mann. *Geometric algebra for computer science: an object-oriented approach to geometry*. Elsevier/Morgan Kaufmann, 2007. ISBN: 978-0-12-369465-2.

[DH76] Whitfield Diffie e Martin Hellman. "New Directions in Cryptography". Em: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654.

[Dyk00] P. P. G. Dyke. *An Introduction to Laplace Transforms and Fourier Series*. Springer, 2000. ISBN: 978-1852330156.

[Dym07] Harry Dym. *Linear Algebra in Action*. AMS, 2007. ISBN: 978-0-8218-3813-6.

[End77] Herbert B. Enderton. *Elements of Set Theory*. Academic Press, 1977. ISBN: 978-0122384400.

[Est11] Ernesto Estrada. *The Structure of Complex Networks: Theory and Applications*. Oxford University Press, 2011. ISBN: 978-0199591756.

[Far82] Stanlry J. Farlow. *Partial Differential Equations for Scientists and Engineers*. Dover, 1982. ISBN: 0-486-67620-X.

[Fig77] Djairo Guedes de Figueiredo. *Análise de Fourier e Equações Diferenciais Parciais*. IMPA, 1977.

[FN14] Djairo Guedes de Figueiredo e Aloisio Freiria Neves. *Equações Diferenciais Aplicadas*. IMPA, 2014. ISBN: 978-85-244-0282-1.

[Fra07] Neide Bertoldi Franco. *Cálculo Numérico*. Pearson Prentice Hall, 2007. ISBN: 85-7605-087-0.

[Gal01] Jean Gallier. *Geometric Methods and Applications for Computer Science and Engineering*. Springer, 2001. ISBN: 0-387-95044-3.

[Gal12] Steven D. Galbraith. *Matehmatics of Public Key Cryptography*. Cambridge, 2012. ISBN: 978-1-107-01392-6.

[GGH97] Oded Goldreich, Shafi Goldwasser e Shai Halevi. "Public-key cryptosystems from lattice reduction problems". Em: *Lecture Notes in Computer Science* 1294 (1997).

[GH07] Peter R. Griffiths e James A de Haseth. *Fourier Transform Infrared Spectrometry*. 2ª ed. Wiley-Interscience, 2007. ISBN: 978-0-471-19404-0.

[Gib11] J. C. Gibbings. *Dimensional Analysis*. Springer, 2011. ISBN: 978-1-84996-316-9.

[Gol04] Jonathan S. Golan. *The Linear Algebra a Beginning Graduate Student Ought to Know*. Kluwer, 2004. ISBN: 1-4020-1824-X.

[Gol96] Derek C. Goldrei. *Classic Set Theory: for guided independent study*. Chapman & Hall, 1996. ISBN: 978-0412606106.

[GV08] Jonas Gomes e Luiz Velho. *Fundamentos da Computação Gráfica*. IMPA, 2008. ISBN: 978-85-244-0200-5.

[Ham89] Morton Hamermesh. *Group Theory and its application to physical problems*. Dover, 1989. ISBN: 978-0486661810.

[Har61] J. P. Den Hartog. *Mechanics*. Dover, 1961. ISBN: 978-0486607542.

[Hat11] Dan Hathaway. "Using Continuity Induction". Em: *College Mathematics Journal* 42.3 (2011), pp. 229–231.

[HC10] Shlomo Havlin e Reuven Cohen. *Complex Networks: Structure, Robustness and Function*. Cambridge University Press, 2010. ISBN: 978-0-521-84156-6.

[Hef13] Jim Hefferon. *Linear Algebra*. Disponível em `http://joshua.smcvt.edu/linearalgebra/`. Edição do autor, 2013.

[HPS08] Jeffrey Hoffstein, Jill Pipher e Joseph Silverman. *An Introduction to Mathematical Cryptography*. Springer, 2008. ISBN: 978-0-387-77993-5.

[HV08] Abramo Hefez e Maria Lúcia T. Villela. *Códigos Corretores de Erros*. IMPA, 2008. ISBN: 978-85-244-0169-5.

[J L12] harry J. Lipkin. *Beta Decay for Pedestrians*. Dover, 2012. ISBN: 978-0486438191.

[Jac04] Dunham Jackson. *Fourier Series and Orthogonal Polynomials*. Dover, 2004. ISBN: 978-0486438085.

[Joh82] Fritz John. *Patial Differential Equations*. 4ª ed. Springer, 1982. ISBN: 0-387-90609-6.

[Jol02] I.T. Jolliffe. *Principal Component Analysis*. 2ª ed. Springer, 2002. ISBN: 0-387-95442-2.

[Joy08] David Joyner. *Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and Other Mathematical Toys*. Johns Hopkins University, 2008. ISBN: 978-0801890130.

[Kei12] H. Jerome Keisler. *Elementary Calculus: An Infinitesimal Approach*. 3ª ed. Disponível livremente em `http://www.math.wisc.edu/~keisler/calc.html`. Dover, 2012.

[KH04] Jin Ho Kwak e Sungpyo Hong. *Linear Algebra*. 2ª ed. Birkhäuser, 2004. ISBN: 978-0-8176-4294-5.

[KL08] Jonathan Katz e Yehuda Lindell. *Introduction to Modern Cryptography*. Chapmen & Hall/CRC, 2008. ISBN: 978-1-58488-551-1.

[Kle13] Andreas Klein. *Stream Ciphers*. Springer, 2013. ISBN: 978-1-4471-5078-7.

[KM89] A. Kostrikin e Y. Manin. *Linear Algebra and Geometry*. CRC Press, 1989. ISBN: 978-2881246838.

[Lax07] Peter Lax. *Linear Algebra and its applications*. Wiley, 2007. ISBN: 978-0-471-75156-4.

[Lim11] Elon Lages Lima. *Álgebra Linear*. IMPA, 2011. ISBN: 978-85-244-0089-6.

[LM06] Walter Loveland e David J. Morrissey. *Modern Nuclear Chemistry*. Wiley, 2006. ISBN: 978-0-471-11532-8.

[Lop15] Vinícius Cifú Lopes. *Equações Diferenciais Ordinárias na Graduação*. Ciência Moderna, 2015.

[LY10] David G. Luenberger e Yinyu Ye. *Linear and Nonlinear Programming*. Springer, 2010. ISBN: 978-1441945044.

[Mac11] Alan Macdonald. *Linear and Geometric Algebra*. CreateSpace, 2011. ISBN: 9781453854938.

[MG07] Jiri Matousek e Bernd Gärtner. *Understanding and Using Linear Programming*. Springer, 2007. ISBN: 978-3-540-30697-9.

[MG12] Daniele Micciancio e Shafi Goldwasser. *Complexity of Lattice Problems: A Cryptographic Perspective*. Springer, 2012. ISBN: 978-1461352938.

[Mie11] Piet van Mieghem. *Graph Spectra for complex networks*. Cambridge University Press, 2011. ISBN: 978-0-521-19458-7.

[Mon02] Luiz Henrique Alves Monteiro. *Sistemas Dinâmicos*. 2ª ed. Editora Livraria da Física, 2002. ISBN: 85-88325-08-X.

[NW06] Jorge Nocedal e Stephen Wright. *Numerical Optimization*. Springer, 2006. ISBN: 978-0387303031.

[Pag+99] Lawrence Page et al. *The PageRank Citation Ranking: Bringing Order to the Web.* Technical Report 1999-66. Previous number = SIDL-WP-1999-0120. Stanford InfoLab, nov. de 1999. URL: http://ilpubs.stanford.edu:8090/422/.

[Pin14] Charles Pinter. *A Book of Set Theory*. Dover, 2014. ISBN: 978-0486497082.

[PW12] María Cristina Pereyra e Lesley A. Ward. *Harmonic Analysis: From Fourier to Wavelets*. AMS, 2012. ISBN: 978-0821875667.

[RN88] Josph Lee Rogers e W. Alan Nicewander. "Thirteen Ways to Look at the Correlation Coefficient". Em: 42.1 (1988), pp. 59–66.

[Rob11] Alain Robert. *Nonstandard analysis*. Dover, 2011. ISBN: 978-0486432793.

[Rob66] Abraham Robinson. *Non-standard analysis*. Princeton University Press, 1996 (orig. 1966). ISBN: 0-691-04490-2.

[Rom10] Steven Roman. *Advanced Linear Algebra*. Springer, 2010. ISBN: 978-1441924988.

[Roy04] A. E. Roy. *Orbital Motion*. Institute of Physics Publishing / CRC Press, 2004. ISBN: 978-0750310154.

[Rud76] Walter Rudin. *Principles of Mathematical Analysis*. 3ª ed. McGraw-Hill, 1976. ISBN: 978-0070542358.

[Sad08] Lorenzo A. Sadun. *Applied Linear Algebra*. 2ª ed. AMS, 2008. ISBN: 978-0-8218-4441-0.

[SAM09] Peter Shirley, Michael Ashikhmin e Steve Marschner. *Fundamentals of Computer Graphics*. 3ª ed. A K Peters/CRC Press, 2009. ISBN: 978-1568814698.

[Sch96] Dieter Schwarzenbach. *Crystallography*. John Wiley & Sons, 1996. ISBN: 0-471-95598-1.

[Sch99] A. Schrijver. *Theory of Linear and Integer Programming*. Wiley, 1999. ISBN: 978-0471982326.

[Sha04] Ruslan Sharipov. *Course of linear algebra and multidimensional geometry*. Disponível em http://arxiv.org/abs/math/0405323. Edição do autor, 2004. ISBN: 5-7477-0099-5.

[Shi77] Georgi E. Shilov. *Linear Algebra*. Dover, 1977. ISBN: 978-0486635187.

[Sim06] George Finlay Simmons. *Differential Equations with applications and historical notes*. McGraw-Hill, 2006. ISBN: 978-0071254373.

[Sin81] David Singmaster. *Notes on Rubik's 'Magic Cube'*. Enslow, 1981. ISBN: 978-0894900433.

[SL88] Pierre Samuel e Silvio Levy. *Projective Geometry*. Springer, 1988. ISBN: 978-0387967523.

[SR09] Igor R. Shafarevich e Alexey O. Remizov. *Linear Algebra and Geometry*. Springer, 2009. ISBN: 978-3-642-30993-9.

[SS10] Nevill Gonzalez Szwacki e Teresa Szwacka. *Basic Elements of Crystallography*. Pan Stanford Publishing, 2010. ISBN: 13-978-981-4241-59-5.

[Sti06] Douglas R. Stinson. *Cryptography: theory and practice*. 3ª ed. Chapman & Hall/CRC, 2006. ISBN: 1-58488-508-4.

[Str08] Walter A. Strauss. *Partial Differential Equations: an introduction*. Wiley, 2008. ISBN: 978-0470-05456-7.

[Tee98] Donald Teets. "Planetary Orbits: Change of Basis in $\mathbb{R}^3$". Em: *Teaching Mathematics and its Applications* 17.2 (1998).

[Tei12] Ralph Costa Teixeira. *Álgebra Linear: exercícios e soluções*. IMPA, 2012. ISBN: 978-85-244-0284-5.

[Tol76] Georgi P. Tolstov. *Fourier Series*. Dover, 1976. ISBN: 978-0486633176.

[TP63] Morris Tenenbaum e Harry Pollard. *Ordinary Differential Equations: an elementary textbook for students of Mathematics, Engineering and the Sciences*. Dover, 1985 (orig. 1963). ISBN: 978-0-486-64940-5.

[Val97] David A. Vallado. *Fundamentals of Astrodynamics and Applications*. McGraw-Hill, 1997. ISBN: 0-07-066834-5.

[Zyg03] A. Zygmund. *Trigonometric Series*. 3ª ed. Cambridge, 2003. ISBN: 978-0521890533.

Índice Remissivo