Geometria Euclidiana
Introdução

Notas de Aula

Marcela Duarte Ferrari

mdsilva@uem.br

Wesley Vagner Ines Shirabayashi

wvishirabayashi@uem.br

13 de outubro de 2020

LISTA DE FIGURAS

SUMÁRIO

2

GEOMETRIA EUCLIDIANA

Neste capítulo vamos estudar os Postulados de Euclides e os Axiomas de Hilbert para a Geometria Euclidiana Plana, que são afirmações aceitas sem demonstrações e formam a base para teoria dessa geometria.

Sob a axiomática de Hilbert:

- Ponto;
- Reta;
- Plano;
- Espaço.

são conceitos primitivos que não são definidos e, sim aceitos, chamados de **Entes Geométricos** . Euclides definiu esses conceitos primitivos em sua obra "Os Elementos".

2.1 AXIOMÁTICA DE HILBERT

Hilbert criou, a partir do trabalho de Euclides, 5 grupos de axiomas:

- Axiomas de Incidência;
- Axiomas de Ordem;

- Axiomas de Congruência;
- Axiomas de Continuidade;
- Axioma das Paralelas.

2.1.1 *Axiomas de Incidência*

Esses axiomas estão associados a uma noção espacial de existência.

1-I **Axioma de Incidência:** Dados dois pontos distintos, existe uma única reta contendo-os.

Figura 1: 1-i. Axiomas de Incidência

1-II **Axioma de Distinção da Reta e do Ponto:** Qualquer reta contém pelo menos dois pontos distintos.

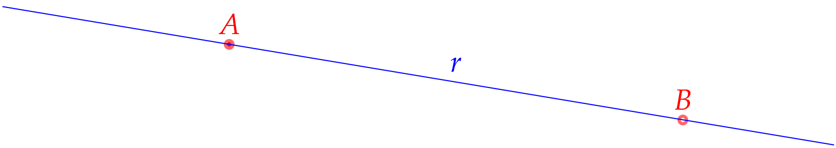


Figura 2: 1-ii. Axiomas de Incidência

1-III **Axioma de Distinção de Reta e Plano:** Existem pelo menos três pontos distintos com a propriedade de que nenhuma reta os contêm.

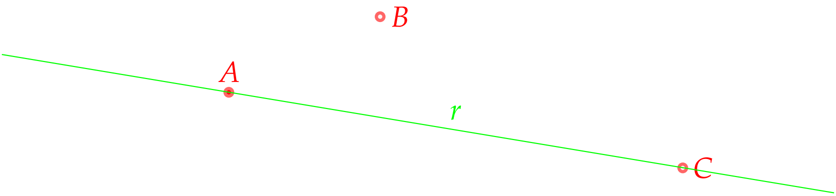


Figura 3: 1-iii. Axiomas de Incidência

O Axioma acima garante que "plano é mais do que uma reta". Também pode ser enunciado como

"Dado uma reta, existe pelo menos um ponto não pertencente a reta".

Uma geometria que satisfaz esse axiomas é chamada de **Geometria de Incidência.**

Exemplo 2.1.0.1 (O plano de 4 pontos.)**.** Seja

$$\Pi = \{A, B, C, D\}$$

e o conjunto de retas é

$$\{\{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, D\}, \{C, D\}\}.$$

Esse plano possui uma Geometria de Incidência.

Colocamos um novo postulado, chamado de Postulado da Régua, supondo-se que o plano Π está munido de uma **Função Distância**, isto é, uma função $d : \Pi \times \Pi \to \mathbb{R}$, tal que para todo par de pontos P e Q em Π, a função d satisfaz;

1. $d(P,Q) \geq 0$;
2. $d(P,Q) = 0$, se e somente se, $P = Q$;
3. $d(P,Q) = d(Q,P)$.

Veja a Definição de Distância.

postulado da régua Para cada reta r, existe uma função biunívoca $f : r \to \mathbb{R}$ tal que $d(P,Q) = |f(P) - f(Q)|$, para todos os pontos P e Q em Π.

Chamaremos as geometrias que satifazem a estes quatro postulados de **Geometria Métrica** .

Observamos que as geometrias métricas não admitem modelos onde o plano tem um número finito de pontos. Ademais, o postulado da régua permite que seja estabelecida uma ordem nos pontos de qualquer uma das retas e desta forma se pode definir as noções de segmento de reta, congruência de segmento, semi-reta, ângulo, triângulo, quadrilátero.

2.1.2 *Axiomas de Ordem*

Esses axiomas estão associados a uma noção de ordem

Os axiomas de incidência não garante que tem infinitos pontos na reta. No entanto, colocar axioma para garantir somente a existência de infinitos pontos não força a ser reta, pois pode haver “saltos” entre os pontos da reta. Para evitar esse fenômeno, precisaríamos garantir que se tenha pontos entre dois pontos quaisquer.

Alem disso, uma reta tem que continuar para ambos lados, o que requer que se existam pontos fora do segmento.

2-I Se um ponto B está entre os pontos A e C, então A, B e C são pontos distintos e B está entre C e A.

Figura 4: 2-i. Axioma de Ordem

2-II Dados dois pontos distintos B e D, existem pontos A, C e E tais que:

1. B está entre A e C.
2. C está entre B e D.
3. D está entre C e E.

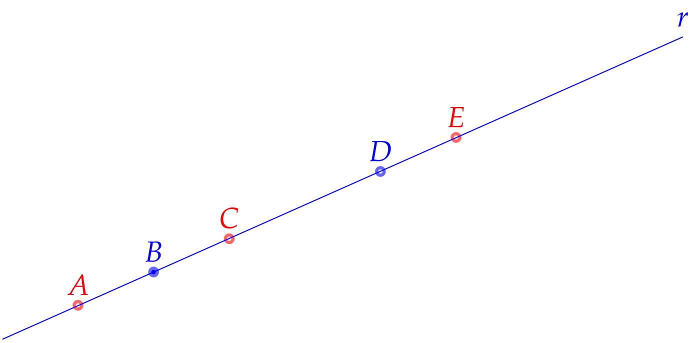


Figura 5: 2-ii. Axioma de Ordem

2-III Dados três pontos distintos de uma reta, apenas um deles localiza-se entre os outros dois.

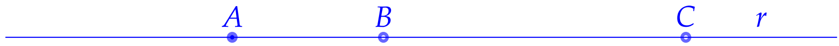


Figura 6: 2-iii. Axioma de Ordem

2-IV Sejam r uma reta e A, B, C três pontos distintos não pertencentes a r.

1. Se A e B estão do mesmo lado de r e B e C estão do mesmo lado de r, então A e C estão do mesmo lado de r;
2. Se A e B estão em lados opostos de r, e B e C estão em lados opostos de r, então A e C estão do mesmo lado de r.

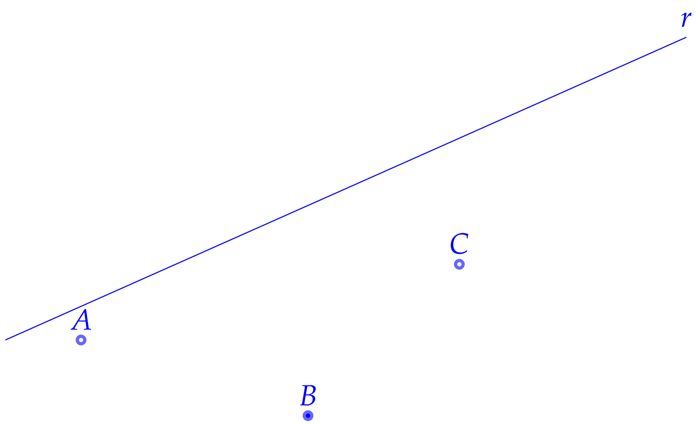


Figura 7: 2-iv.1 Axioma de Ordem

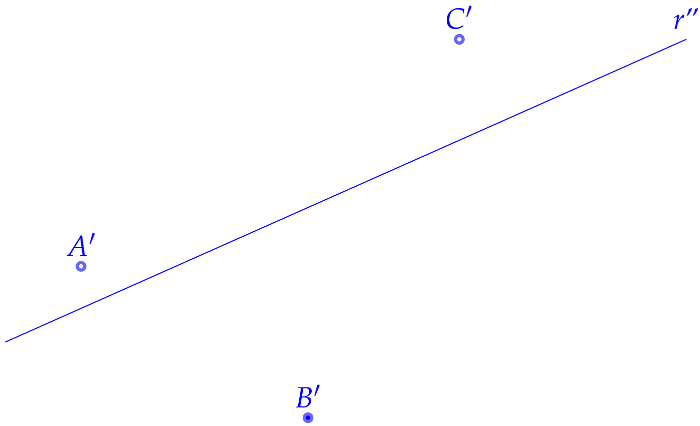


Figura 8: 2-iv.2 Axioma de Ordem

2.1.3 *Axiomas de Congruência*

Esses axiomas estão associados a uma noção de igualdade entre segmentos e ângulos.

3-I Se A e B são dois pontos distintos e A_0 é a origem da semi-reta s, então existe um único ponto B_0 distinto de A_0 em s tal que o segmento $\vec{AB}$ é congruente ao segmento $\vec{A_0B_0}$.

3-II Se o segmento $\vec{AB}$ é congruente ao segmento $\vec{CD}$ e ao segmento $\vec{EF}$, então o segmento $\vec{CD}$ é congruente ao segmento $\vec{EF}$.

Além disso, todo segmento é congruente a si mesmo.

3-III Sejam $\vec{AB}$ e $\vec{BC}$ segmentos em uma reta r com apenas B em comum. Além disso, seja, $\vec{A_0B_0}$ e $\vec{B_0C_0}$ segmentos em uma reta r_0 com apenas B_0 em comum. Se o segmento $\vec{AB}$ for congruente ao segmento $\vec{A_0B_0}$ e o

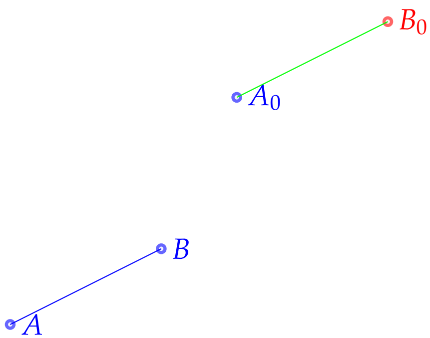


Figura 9: 3-i. Axioma de Congruência

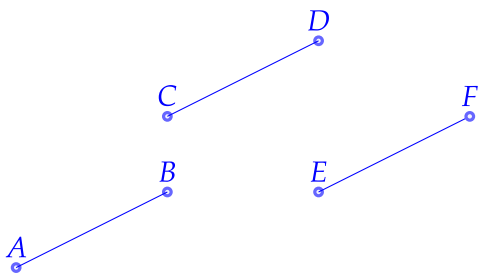


Figura 10: 3-ii. Axioma de Congruência

segmento $\vec{BC}$ for congruente ao segmento $\vec{B_0C_0}$, então o segmento $\vec{AC}$ é congruente ao segmento $\vec{A_0C_0}$.

3-IV Sejam um semiplano σ e um ângulo α. Tomemos uma semi-reta s com origem em B contida nessa reta que determina o semiplano σ. Então, existe apenas um ângulo β com lado em s contido no semiplano σ e congruente ao ângulo α.

3-V Se o ângulo α é congruente ao ângulo β e ao ângulo γ, então o ângulo β é congruente ao ângulo γ.

Além disso, todo ângulo é congruente a si mesmo.

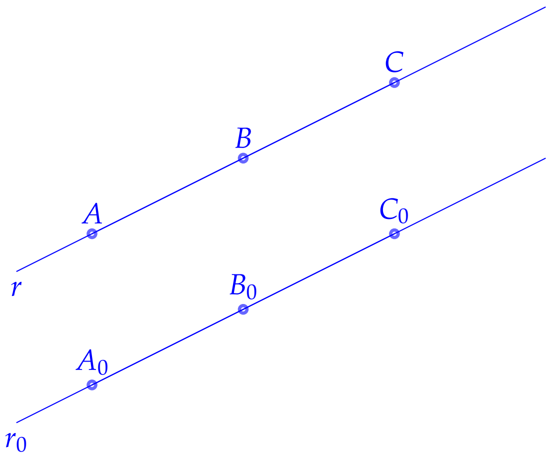


Figura 11: 3-iii. Axioma de Congruência

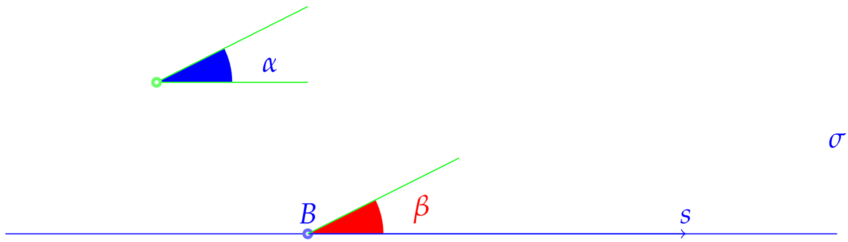


Figura 12: 3-iv. Axioma de Congruência

3 - VI Dados dois triângulos ABC e EFG, se $\vec{AB}$ é congruente a $\vec{EF}$, $\vec{AC}$ é congruente a $\vec{EG}$ e α é congruente β, entâo ABC é congruente a EFG.

(caso "Lado, Ângulo, Lado" de congruência)

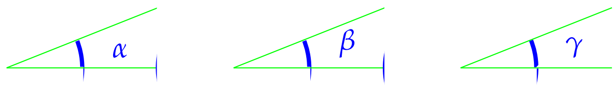


Figura 13: 3-v. Axioma de Congruência

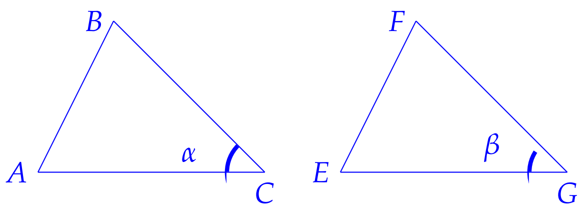


Figura 14: 3-vi. Axioma de Congruência

2.1.4 *Axiomas de Continuidade*

Esses axiomas são utilizados para medição de segmentos e ângulos

4-I - **Axioma de Arquimedes** - Sejam $\vec{AB}$ e $\vec{CD}$ dois segmentos. Então existe um número finito de pontos

$$A_1, A_2, A_3, \ldots, A_n$$

na reta r que passa por A e B tais que os segmentos

$$\vec{AA_1}, \vec{A_1A_2}, \vec{A_2A_3}, \ldots, \vec{A_{n-1}A_n}$$

possuem o mesmo comprimento de $\vec{CD}$ e o ponto B está entre A e A_n.

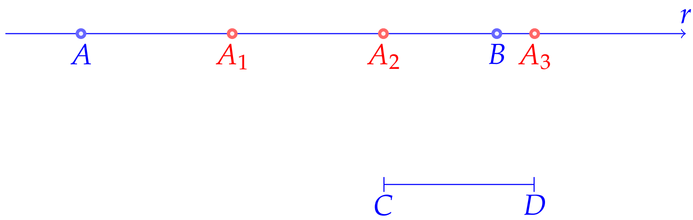


Figura 15: 4-i. Axioma de Arquimedes

4-II - **Axioma de Dedekind** Suponha que o conjunto de todos os pontos de uma reta r está na união dos conjuntos não vazios C_1 e C_2. Suponha ainda que nenhum ponto de C_1 está entre dois pontos de C_2 e vice-versa. Então "existe um único ponto $O \in r$ tal que O está entre P_1 e P_2 se, e somente se, $P_1 \in C_1$, $P_2 \in C_2$ e $O \neq P_1$ e $O \neq P_2$".

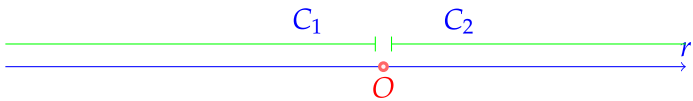


Figura 16: 4-ii. Axioma de Dedekind

Ou seja, se identificarmos r com a reta real temos

- Se $a \in I_1$ e $b \in I_2$ então $a < b$;
- $I_1 \cup I_2 = \mathbb{R}$ então I_1 possui um maior elemento ou I_2 possui um menor elemento.

2.1.5 *Axioma das Paralelas*

Quinto Postulado de Euclides:

Por um ponto fora de uma reta r pode-se traçar uma única reta paralela a r.

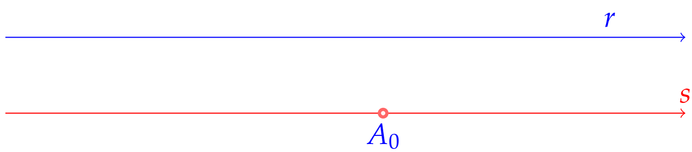


Figura 17: 5. Axioma das Paralelas

Formulação equivalente ao 5^o Postulado de Euclides de John Playfair (1748 - 1819), físico e matemático escocês.

Definição 2.1.1 (Geometria Plana)**.** Uma geometria plana é um conjunto Π, que chamamos de plano, cujos elementos são chamados de pontos e contendo certos subconjuntos chamados de retas, satisfazendo os Axiomas de Incidência, os Axiomas de Ordem, os Axiomas de Congruência, os Axiomas de Continuidade e o Axioma das Paralela.

2.2 EXERCÍCIOS

1. Encontre um modelo de Geometria de incidência com 7 pontos.
2. Explique o significado de cada um dos Axiomas de Incidência.
3. Defina o que é pontos serem colineares.
4. Mostre que, se três pontos forem não colineares, então são distintos.
5. Mostre que dois últimos axiomas pode ser substituido por
   (a) **Existência da Reta:** Existe pelo menos uma reta.
   (b) **Distinção da Reta:** Dada uma reta, existe pelo menos dois ponto pertencentes a reta e um ponto não pertencente a reta.
6. O conjunto que satisfaz os axiomas de incidência é denominado de **Plano de Incidência**. Mostre que o plano de incidência tem pelo menos três pontos e três retas.

   Dê exemplo do plano de incidência com exatamente três pontos e três retas.
7. Faça o desenho ilustrativo para cada um dos axiomas.

3

PRODUTO INTERNO

Conforme estudamos a Geometria Euclidiana no capítulo anterior, introduzimos a noção de Espaço Euclidiano elaborada pelos antigos gregos como uma abstração do nosso espaço físico. A grande inovação desse ideia era construir e provar toda a geometria partindo de algumas propriedades básicas, que são abstraídas do mundo físico e que não podemos comprovar matematicamente.

Em 1637, Rene Descartes introduziu coordenadas cartesianas e mostrou que isto permite reduzir problemas geométricos a cálculos algébrico. Esta redução da geometria para a álgebra foi considerado uma grande mudança, onde foram trabalhados números racionais e números não racionais e, definidos em termos geométricos, como comprimento e distância.

Apesar da ampla utilização de abordagens de Descartes, que foi chamada de Geometria Analítica, a definição de espaço euclidiano permaneceu inalterada até o final do século 19.

A introdução abstrata de espaços vetoriais permitiu definir espaços euclidianos atráves de uma definição algébrica. Esta nova definição é equivalente à definição clássica em termos de axiomas geométricos, entretanto, essa definição algébrica é mais frequentemente usada para a introdução de espaços euclidianos.

3.1 DEFINIÇÕES PRELIMINARES

Definição 3.1.1 (Produto Interno)**.** Seja E um espaço vetorial. Uma aplicação

$$h : E \times E \to \mathbb{R}$$

que satisfaz as seguintes propriedades:

1. **Simetria:**

$$h(u, v) = h(v, u);\ \forall\ u, v \in E;$$

2. **Positividade:**

$$h(u, u) \geq 0;\ \forall\ u \in E,\ \text{com}\ h(u, u) = 0 \leftrightarrow u = 0_E$$

3. **Distributividade:**

$$h(u + w, v) = h(u, v) + h(w, v);\ \forall\ u,\ v,\ w \in E$$

4. **Homogeneidade:**

$$h(\lambda u, v) = \lambda h(u, v);\ \forall\ u, v \in E \text{ e } \lambda \in \mathbb{R}$$

define um produto interno no espaço euclidiano E, Utilizando as propriedades de simetria, distributividade e homogeneidade temos

- $h(u, v + w) = h(u, v) + h(u, w)$ para todos $u, v, w \in E$.
- $h(u, \lambda v) = \lambda h(u, v)$, para todos $u, v \in E$ e $\lambda \in \mathbb{R}$.

Assim, dizemos que o produto interno é uma aplicação bilinear, isto é, é uma aplicação linear nas duas variáveis.

Definição 3.1.2 (Espaço Euclidiano)**.** Um Espaço Euclidiano $\mathbb{E}^n$ é um espaço vetorial real de $n-$dimensional munido de um produto interno.

3.2 BASES ORIENTADAS

Vamos considerar nessas notas de aula os espaços euclidianos $n-$dimensionais, $\mathbb{E}^n$, com $n > 0$ um número inteiro positivo.

Sabemos que todo espaço vetorial de dimensão finita possui uma base também finita.

Uma **Base** de um espaço vetorial $\mathbb{E}^n$ é um subconjunto finito de vetores de $\mathbb{E}^n$, $B = \{b_1, \ldots, b_n\}$, linearmente independentes que geram todo espaço.

Observemos que toda base de um espaço vetorial real finito possui o mesmo número de elementos e existem infinitas bases.

Se consideramos a base de $\mathbb{E}^n$:

$$B_{\mathbb{E}^n} = \{e_1, e_2, \ldots, e_n\},$$

onde

$$e_i = (0, 0, \ldots, 0, \underbrace{1}_{i-\text{ésima posição}}, 0, \ldots, 0)$$

então dizemos que essa base é a **Base Canônica** de $\mathbb{E}^n$, onde

$$\mathbb{E}^n = [[B_{\mathbb{E}^n}]] = \left\{ u = u_1e_1 + \ldots + u_ne_n = \sum_{i=1}^{n} u_ie_i : \ u_i \in \mathbb{R} \right\}.$$

Observe que, para qualquer base $B = \{\}$, dizemos que $(u_1, \ldots, u_n)$ são as **coordenadas** do vetor u relativas à base B.

Além disso, o número n é unicamente determinado e chamado de dimensão onde escrevemos, $\dim(\mathbb{E}^n) = n$.

Uma **Base Orientada** é uma base formada por conjunto ordenado de elementos.

Além disso, se $B = \{b_1, b_2, b_3, \ldots, b_n\}$ é uma base orientada de $\mathbb{E}^n$, então $C = \{b_2, b_1, b_3, \ldots, b_n\}$ é outra base orientada de $\mathbb{E}^n$ diferente de B.

Se $B = \{b_1, b_2, \ldots, b_n\}$ e $C = \{c_1, c_2, \ldots, c_n\}$ são bases para $\mathbb{E}$, então, dada um vetor $u \in \mathbb{E}$, é possível escrever

$$\begin{aligned} v]_B &= \sum_{1 \leq i \leq n} u_i b_i \\ v]_C &= \sum_{1 \leq i \leq n} \mu_i c_i \end{aligned}$$

Como C é base podemos escrever os elementos de B nessa base,

$$\begin{cases} b_1 &= \alpha_{11} c_1 + \ldots + \alpha_{n1} c_n \\ &\vdots \\ b_n &= \alpha_{1n} c_1 + \ldots + \alpha_{nn} c_n \end{cases}$$

isto é, para todo $1 \leq i \leq n$,

$$b_i = \sum_{1 \leq j \leq n} \alpha_{ij} c_j.$$

Substituindo em $v]_B$ temos

$$\begin{aligned} v]_B &= u_1 \left(\alpha_{11} c_1 + \ldots + \alpha_{n1} c_n\right) \\ &+ \\ &\vdots \\ &+ u_n \left(\alpha_{1n} c_1 + \ldots + \alpha_{nn} c_n\right) \end{aligned}$$

logo

$$\begin{array}{rcl} v]_B & = & (u_1\alpha_{11} + \ldots + u_n\alpha_{1n})\, c_1 \\ & + & \\ & \vdots & \\ & + & (u_1\alpha_{1n} + \ldots + u_n\alpha_{nn})\, c_n \end{array}$$

portanto

$$\begin{array}{rcl} \mu_1 & = & u_1\alpha_{11} + \ldots + u_n\alpha_{1n} \\ & \vdots & \\ \mu_n & = & u_1\alpha_{1n} + \ldots + u_n\alpha_{nn} \end{array}$$

em termos matriciais, temos

$$\begin{bmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_n \end{bmatrix} = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & \vdots & \ldots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \ldots & \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix}$$

essa matriz é chamada de **Matriz de Mudança de Base** da base B para a base C. Ela será denotada por M_B^C

Observamos que a matriz mudança de base sempre possui determinante diferente de zero, dessa forma podemos definir:

Definição 3.2.1 (Orientação entre bases)**.** Dadas duas bases B e C de um espaço $\mathbb{E}^n$, dizemos que B e C possuem a mesma orientação se $\det(M_B^C) > 0$. Esta relação é denotada por $B \sim C$. Caso contrário, se $\det(M_C^B) < 0$ diz-se que B e C têm orientação contrária.

A relação de orientação entre bases é uma relação de equivalência.

3.3 PROPRIEDADES E DEFINIÇÕES AUXILIARES DO PRODUTO INTERNO

3.3.1 *Exemplos*

Exemplo 1

Em $\mathbb{E}^2$, sejam $u = (u_1, u_2)$, $v = (v_1, v_2)$ e h a aplicação definida em $\mathbb{E} \times \mathbb{E}$ e determinada por

$$h(u,v) = 2u_1v_1 + 3u_2v_2 \in \mathbb{R}.$$

então h satisfaz todos os itens da definição de Produto Interno e, portanto, h é um produto interno em $\mathbb{E}^2$.

Exemplo 2

Em $\mathbb{E}^2$, sejam $u = (u_1, u_2)$, $v = (v_1, v_2)$ e h a aplicação definida em $\mathbb{E} \times \mathbb{E}$ e determinada por

$$h(u,v) = 2u_1v_1 \in \mathbb{R}.$$

Então h não satisfaz a positividade, pois

$$h\left((0,1),(0,1)\right) = 0$$

mas $(0,1) \neq 0_{\mathbb{E}^2}$. Portanto, não é um produto interno em $\mathbb{E}^2$.

3.3.2 *Produto Interno Canônico*

Definição 3.3.1 (Produto Interno Canônico)**.** Em $\mathbb{E}^n$, $n > 0$ o produto interno canônico (ou usual) é definido por

$$\begin{array}{rcl} \langle\ ,\ \rangle : \mathbb{E}^n \times \mathbb{E}^n & \longrightarrow & \mathbb{R} \\ (u,v) & & u \cdot v \end{array}$$

Se $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n)$ são as coordenadas dos vetores u e v na base canônica então temos que

$$u \cdot v = u_1 v_1 + \ldots + u_n v_n = \sum_{i=1}^{n} u_i v_i.$$

3.4 MATRIZ DE UM PRODUTO INTERNO

Sejam $\mathbb{E}^3$ um espaço euclidiano e $B = \{b_1, b_2, b_3\}$ uma base ordenada de $\mathbb{E}^3$, os elementos

$$u = u_1 b_1 + u_2 b_2 + u_3 b_3 \quad \text{e} \quad v = v_1 b_1 + v_2 b_2 + v_3 b_3$$

vetores de $\mathbb{E}^3$ escritos em termos da base B, denotados matricialmente por

$$[u] = [u_1\ u_2\ u_3\ ] \quad \text{e} \quad [v] = [v_1\ v_2\ v_3]$$

e, um produto interno em $\mathbb{E}^2$

$$h : \mathbb{E}^3 \times \mathbb{E}^3 : (u, v) \longmapsto \langle u, v \rangle \in \mathbb{R}.$$

Nestas condições, existe uma matriz $PI \in M_3(\mathbb{R})$, onde $M_3(\mathbb{R})$ é o conjunto de todas as matrizes quadradas de ordem 3 com entradas reais, que depende da escolha da base B e é tal que

$$h\,(u, v) = [u]\, PI\, [v]^T$$

Demonstração. Observemos que

$$\begin{aligned}
h(u,v) &= h(u, v_1b_1 + v_2b_2 + v_3b_3) \\
&= v_1h(u,b_1) + v_2h(u,b_2) + v_3h(u,b_3) \\
&= v_1h(u_1b_1 + u_2b_2 + u_3b_3, b_1) \\
&\quad +v_2h(u_1b_1 + u_2b_2 + u_3b_3, b_2) \\
&\quad +v_3h(u_1b_1 + u_2b_2 + u_3b_3, b_3) \\
&= u_1h(b_1,b_1)v_1 + u_2h(b_2,b_1)v_1 + u_3h(b_3,b_1)v_1 \\
&\quad +u_1h(b_1,b_2)v_2 + u_2h(b_2,b_2)v_2 + u_3h(b_3,b_2)v_2 \\
&\quad +u_1h(b_1,b_3)v_3 + u_2h(b_2,b_3)v_3 + u_3h(b_3,b_3)v_3
\end{aligned}$$

Podemos considerar a matriz

$$PI = \begin{pmatrix} h(b_1,b_1) & h(b_1,b_2) & h(b_1,b_3) \\ h(b_2,b_1) & h(b_2,b_2) & h(b_2,b_3) \\ h(b_3,b_1) & h(b_3,b_2) & h(b_3,b_3) \end{pmatrix}$$

e, obtemos

$$h(u,v) = \begin{pmatrix} u_1 & u_2 & u_3 \end{pmatrix} \begin{pmatrix} h(b_1,b_1) & h(b_1,b_2) & h(b_1,b_3) \\ h(b_2,b_1) & h(b_2,b_2) & h(b_2,b_3) \\ h(b_3,b_1) & h(b_3,b_2) & h(b_3,b_3) \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}$$

□

Podemos ainda provar que essa matriz é única, a menos da base.

Exemplo 3.4.0.1. Consideramos a base de $\mathbb{E}^2$ dada por

$$C = \{(1,2),(2,-3)\}.$$

O produto interno definido por

$$h(u,v) = 2u_1v_1 + 3u_2v_2$$

foi definido, implicitamente, para vetores dados na base canônica

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

de $\mathbb{E}^2$. Logo

$$\begin{array}{lcr} h\left((1,2),(1,2)\right) & = & 14 \\ h\left((1,2),(2,-3)\right) & = & -14 \\ h\left((2,-3),(1,2)\right) & = & -14 \\ h\left((2,-3),(2,-3)\right) & = & 35 \end{array}$$

assim

$$PI_B = \begin{pmatrix} 14 & -14 \\ -14 & 35 \end{pmatrix}$$

para vetores escritos em termos desta base C, temos

$$h_B(u_B, v_B) \quad = \quad \begin{pmatrix} u_{B1} & u_{B2} \end{pmatrix}_B PI_B \begin{pmatrix} v_{B1} \\ v_{B2} \end{pmatrix}_B \quad ,$$

isto é,

$$\begin{aligned} h_B(u_B, v_B) &= \begin{pmatrix} u_{B1} & u_{B2} \end{pmatrix}_B \begin{pmatrix} 14 & -14 \\ -14 & 35 \end{pmatrix} \begin{pmatrix} v_{B1} \\ v_{B2} \end{pmatrix}_B \\ &= \begin{pmatrix} 14u_{B1} - 14u_{B2} & -14u_{B1} + 35u_{B2} \end{pmatrix}_B \begin{pmatrix} v_{B1} \\ v_{B2} \end{pmatrix}_B \\ &= 14u_{B1}v_{B1} - 14u_{B2}v_{B2} - 14u_{B1}v_{B1} + 35u_{B2}v_{B2} \,. \end{aligned}$$

Definição 3.4.1 (Matriz Simétrica)**.** Uma matriz P de $M_n(\mathbb{R})$ é chamada de simétrica se $P = P^t$, isto é, H é igual a sua matriz tranposta.

Definição 3.4.2 (Matriz Positiva Definida)**.** Uma matriz P de $M_n(\mathbb{R})$ é chamada de positiva definida se, para todo vetor não-nulo $v \in \mathbb{E}$, temos

$$v]\ P\ v]^t > 0.$$

Lema 3.4.0.1. Sejam $\mathbb{E}^n$ um espaço euclidiano, $B = \{b_, \ldots, b_n\}$ uma base ordenada e $A \in M_n(\mathbb{R}$ uma matriz simétrica e positiva definida. A aplicação definida por

$$v]\ P\ v]^t > 0 \in \mathbb{R}$$

é um produto interno.

Lema 3.4.0.2. Sejam $\mathbb{E}^n$ um espaço euclidiano e h um produto interno desse espaço. Fixada uma base ordenada B, existe uma única matriz $PI \in M_n(\mathbb{R})$ tal que

$$v]\ P\ v]^t > 0 \in \mathbb{R}.$$

Nestas condições, PI é simétrica e positiva definida.

$$d(u, v) = ||u - v|| = \sqrt{\langle u - v, u - v\rangle}$$

onde

$$||u|| = \sqrt{\langle u, u\rangle}$$

4

MÉTRICA EUCLIDIANA

O espaço ueclidiano é o espaço métrico mais familiar. A métrica é uma generalização das quatro propriedades conhecidas da distância euclidiana.

A métrica euclidiana define a distância entre dois pontos como o comprimento do segmento de reta que os conecta.

4.1 O ESPAÇO TANGENTE

Definição 4.1.1 (Vetor)**.** Seja $\mathbb{E}^n$ um espaço vetorial. Um vetor v_A consiste de dois pontos, um que chamamos de parte vetorial v e outro de ponto de Aplicação A. Esse vetor é obtido ao se colocar a origem de v no ponto A e satisfaz as seguintes propriedades:

1. Os vetores u_A e v_B são iguais, se e somente se, possuem o mesmo ponto de aplicação $A = B$ e a mesma parte vetorial $u = v$;

2. Se $A \neq B$ e u v são vetores paralelos e não coincidentes;

3. A soma dos vetores a partir do ponto de aplicação é igual à soma dos vetores fixada no ponto de aplicação, isto é, $v_A + u_A = (u + v)_A$;

4. Se $\alpha \in \mathbb{R}$ então $\alpha u_A = (\alpha u)_A$.

Definição 4.1.2 (Espaço Tangente)**.** Sejam $A \in \mathbb{E}^n$ um ponto e $V \subseteq \mathbb{E}^n$ um (sub)espaço vetorial. O espaço tangente de V em A é definido como o conjunto de todos os vetores de V aplicados em A (ou seja, com sua origem transladada para o ponto A) e denotado por

$$T_A(V) = \{v_A : v \in V\}$$

Sejam $A \in \mathbb{E}^n$ um ponto e $V \subseteq \mathbb{E}^n$ um (sub)espaço vetorial. Consideramos

$$0_A = A,$$

$T_A(V)$ é um (sub)espaço vetorial.

A aplicação

$$\begin{array}{ccc} V & \longrightarrow & T_A(V) \\ v & \longmapsto & v_A \end{array}$$

é um isomorfismo entre espaços vetoriais.

Para A e V, valem as seguintes asserções:

- se $A = 0$ então
$$T_0(V) = V;$$
- Para todo $A \in \mathbb{E}^n$, temos
$$T_A(V) \subseteq \mathbb{E}^n$$

Definição 4.1.3 (Base Aplicada num Ponto)**.** Sejam V um (sub)espaço vetorial de E^n e $A \in \mathbb{E}^n$, por ser (sub)espaço vetorial de dimensão finita, admite base. Seja $B = \{b_1, b_2, \ldots, b_n\}$ uma base ordenada de V.

Uma base ordenada de $T_A(V)$ é definida como uma base de V aplicada em A, isto é, o conjunto de cada vetor b_i aplicado em A. A base de $T_A(V)$ é denotada por

$$B_A = \{b_{1A}, b_{2A}, \ldots, b_{nA}\}.$$

4.2 A MÉTRICA

Definição 4.2.1. O conjunto das matrizes quadradas, simétricas e positivas definidas será denotado por

$$\mathcal{M}_n(\mathbb{R}) = \left\{M \in M_n(\mathbb{R}) : \ M = M^t \text{ e } v]\ M\ v]^t > 0,\ \forall v \in \mathbb{E}^n \setminus \{0\}\right\}.$$

Observe que $\mathcal{M}_n(\mathbb{R}) \subseteq M_n(\mathbb{R})$.

A matriz de um produto interno não necessita ser constante. Pode variar em cada ponto A que define $T_A(\mathbb{E}^n)$.

Definição 4.2.2. Sejam $Y \subseteq \mathbb{E}^n$ e uma aplicação matricial

$$\begin{aligned} M : Y &\longrightarrow M_n(\mathbb{R}) \\ u &\longmapsto M(u) = \big(a_{ij}(u)\big) \end{aligned}$$

onde cada $u \in Y$ e cada $1 \leq i, j \leq n$ temos um funcional linear

$$\begin{aligned} a_{ij} : Y &\longrightarrow \mathbb{R} \\ u &\longmapsto a_{ij}(u) \end{aligned}$$

que é uma função diferenciável, chamada de função entrada de $M(u)$.

Se houver um aberto conexo $X \subseteq Y$ tal que a restrição

$$M_{|X} \in \mathcal{M}_n(\mathbb{R}),$$

diz-se que $M = M(u)$ é uma métrica diferenciável em cada ponto $u \in X$.

Deste ponto em diante quando se falar de uma métrica é entendido que u pertence ao conjunto tal que

$$M(u) \in \mathcal{M}_n(\mathbb{R}).$$

Uma métrica $M = M(u_A)$ se aplica a $T_A(\mathbb{E}^n)$ para estabelecer um produto interno neste espaço tangente.

Para isso temos a seguinte definição:

Definição 4.2.3. Seja $M = M(u_A)$ uma métrica diferenciável de $T_A(\mathbb{E}^n)$, essa matriz define um produto interno dado por

$$\begin{array}{rcl} T_A(\mathbb{E}^n) \times T_A(\mathbb{E}^n) & \longrightarrow & \mathbb{R} \\ (w_A, v_A) & \longmapsto & \langle w_A, v_A \rangle = w_A] \; M(u_A) \; v_A]^t \in \mathbb{R} \end{array}$$

Esta aplicação será chamada de produto interno sobre $T_A(\mathbb{E}^n)$ segundo $M(u_A)$.

5

AÇÕES DE GRUPOS

Mostraremos diferentes aspectos de ações de grupos em geometria. Para isto, vamos nos restringir a dois tipos especiais de geometria, a geometria afim e a geometria projetiva.

5.1 GRUPOS E HOMOMORFISMOS

Definição 5.1.1 (Grupo)**.** Um grupo é um par $(G, \cdot)$ onde G é um conjunto não vazio e

$$\begin{array}{rcl} \cdot : G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & ab \end{array}$$

é uma função, denominada Operação do Grupo, satisfazendo as seguintes propriedades:

1. **(Associatividade):** Para todos os elementos $a, b, c \in G$ temos
$$(ab)c = a(bc).$$

2. **(Elemento Neutro):** Existe um elemento $e_G \in G$ tal que para todo $a \in G$ tenhamos
$$ae_G = e_G a = a.$$

3. **(Elemento Inverso):** A todo elemento $a \in G$ associa-se um elemento a^{-1} tal que

$$aa^{-1} = a^{-1}a = e_G.$$

Lema 5.1.0.1. 1. Existe um único elemento neutro em um grupo.

2. Existe um ùnico elemento inverso para cada elemento $a \in G$.

Definição 5.1.2 (Grupo Abeliano)**.** Um grupo $(G, \cdot)$ è dito ser abeliano, ou comutativo se para todos os elementos $a, b \in G$ temos

$$ab = ba,$$

ou seja, a operação do grupo satisfaz a propriedade da comutatividade

Lema 5.1.0.2. Se $H \subseteq G$ é subgrupo do grupo G, então o elemento neutro de H, e_H é igual ao elemento neutro de G, e_G, isto é $e_H = e_G$. Para qualquer $a \in H$, seu inverso com relação a H é o mesmo inverso com relação a G.

Lema 5.1.0.3. Uma condição necessária e suficiente para que um conjunto não vazio H , $H \subseteq G$ seja subgrupo de G é que para quaisquer $a, b \in H$, tivermos que

$$ab^{-1} \in H.$$

Lema 5.1.0.4. Um subgrupo de um grupo abeliano também é abeliano.

Definição 5.1.3 (Subgrupo)**.** Um subconjunto não vazio H de um grupo G é um Subgrupo de G se H é um grupo com a mesma operação de G.

5.1.1 *Exemplos*

1. O conjunto dos Números Inteiros com a operação de adição usual, $(\mathbb{Z}, +)$, é um grupo abeliano.

2. Seja $n \in \mathbb{Z}$ um número inteiro positivo. O conjunto das classes de congruência módulo n, denotado por $\mathbb{Z}_n$, com a adição usual de módulos é um grupo abeliano finito com n elementos.

3. O conjunto dos Números Reais com a operação de adição, $(\mathbb{R}, +)$ é um grupo abeliano e $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ são subgrupos de $(\mathbb{R}, +)$.

4. O conjunto dos Números Complexos não nulos com a operação de multiplicacção, $(\mathbb{C}^*, \cdot)$ é um grupo abeliano. Os conjuntos $(\mathbb{R}^*, \cdot)$ e $(\mathbb{Z}^*, \cdot)$ sâo subgrupos abelianos de $(\mathbb{C}^* \cdot)$.

5. O subconjunto dos números complexos de módulo unitário,
$$U(1) = \{z \in \mathbb{C} : \ |z| = 1\}$$
é um subgrupo de $(\mathbb{C}^*, \cdot)$. Geometricamente, este conjunto corresponde a circunferência no plano complexo de raio 1 e centro na origem.

   Se $z = a + bi$, então
$$|z| = \sqrt{z\bar{z}} = \sqrt{(a+bi)(a-bi)} = \sqrt{a^2 + b^2}.$$
   Se $|z| = 1$, então $z^{-1} = a - bi$ e $|z^{-1}| = |z| = 1$. Além disto, se $z, w \in U(1)$, então
$$|zw^{-1}| = |z||w^{-1}| = |z||w| = 1.$$
   Portanto $zw^{-1} \in U(1)$, mostrando que $U(1)$ é subgrupo de $(\mathbb{C}^*, \cdot)$.

6. Seja X um conjunto qualquer então o conjunto

$$Bij(X) = \{f : X \to X : \ f \text{ é bijeção}\}$$

é um grupo com a operação de composição de funções.

Note que, em geral, o grupo $Bij(X)$ não é abeliano.

7. Seja $I_n = \{1, \ldots, n\}$, o conjunto dos n primeiros inteiros positivos, uma permutação em I_n é uma bijeção $\pi : I_n \to I_n$. O conjunto

$$S_n = \{\pi : I_n \to I_n : \ \pi \text{ é permutação}\}$$

com a operação de composição é um grupo, chamado de **Grupo de Permutação**, denotado por S_n.

Um elemento do grupo de permutações pode sre escrito da seguinte maneira

$$\tau = \begin{pmatrix} 1 & 2 & \ldots & n \\ \tau(1) & \tau(2) & \ldots & \tau(n) \end{pmatrix}.$$

O Espaço Vetorial $GL(V)$

Seja V um espaço vetorial real. Seja $GL(V)$ o conjunto de todas as transformações lineares invertíveis de V em V. Certamente, este é um subconjunto do grupo de bijeções $Bij(V)$, então temos que $GL(V)$ é um subespaço vetorial de $Bij(V)$.

No caso em que o espaço vetorial V é de dimensão finita, $\dim(V) = n$, podemos identificar as transformações lineares de V em V com matrizes quadradas de ordem $n \times n$. Para isto, basta tomarmos uma base $B = b_1, \ldots, b_n$ e definirmos, para uma dada transformação linear $T : V \to V$, a matriz

$$T]_B = (t_{ij}) \in M_N(\mathbb{R})$$

onde $M_n(\mathbb{R})$ é o conjunto de todas as matrizes quadradas de ordem n e tal que

$$T(b_j) = \sum_{i=1}^{n} t_{ij} b_i.$$

A condição de que $T \in GL(V)$ equivale, em termos matriciais, a condição $\det(T]_B) \neq 0$. Geometricamente, esse determinante pode ser interpretado como o volume (com sinal) do paralelepípedo n dimensional determinado pelos vetores $T(b_1), \ldots, T(b_n)$. Dizermos que a transformação linear $T : V \to V$ é inversível, em dimensão finita, é equivalente a dizermos que o volume do paralelogramo determinado por estes vetores é não nulo.

Exemplo 5.1.0.1. Definamos $GL(n, \mathbb{R})$ como o conjunto das matrizes $n \times n$ de determinante não nulo, este conjunto corresponde ao grupo $GL(V)$ no caso em que $\dim(V) = n$, portanto, também é um grupo. Para verificar que $GL(n, \mathbb{R})$ é um grupo, sejam $A, B \in GL(n, \mathbb{R})$, então

$$\det(AB) = \det(A)\det(B) \neq 0,$$

logo $AB \in GL(V)$.

Com estas observações, podemos concluir que $GL(n, \mathbb{R})$ é um grupo.

Lema 5.1.0.5. Se $A, b \in M_n(\mathbb{R})$ então

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

O Grupo Ortogonal $O(V)$

Considere o espaço vetorial V seja de dimensão finita e munido com um produto interno

$$\begin{aligned} h : V \times V &\longrightarrow \mathbb{R} \\ (u, v) &\longmapsto h(u, v) \end{aligned}$$

O conjunto das transformações lineares que preserva o produto interno, isto é, que preserva as transformações denominadas **Transformações Ortogonais** é denotado por $O(V)$.

Um elemento de $O(V)$ é uma transformação linear T tal que

$$h(Tu, Tv) = h(u, v).$$

O conjunto $O(V)$ é um grupo. Observe que

1. $Id_V \in O(V)$.

2. Dada a tranformação linear $T : V \to V$, definimos a adjunta da transformação linear T como a transformação linear $T^* : V \to V$ tal que

   $$h(Tu, v) = h(u, T^*v), \ \forall u, v \in V.$$

   Se $T \in O(V)$ então, dados quaisquer $u, v \in V$ temos

   $$h(u, v) = h(Tu, Tv) = h(u, T^*Tv)$$

   portanto

   $$h(u, (v - T^*Tv)) = 0, \ \forall u \in V,$$

   o que implica que $T^*Tv = v$ para todo $v \in V$, ou seja, $T^*T = Id_V$. Analogamente, temos $TT^* = Id_V$. Portanto $T^* = T^{-1}$.

Assim podemos concluir que $O(V)$ é um grupo, chamado de **Grupo Ortogonal**

Observemos que

1. A adjunta de uma transformação linear, se existir, é única.

2. Considere uma base ortonormal $B = \{e_1, \ldots, e_n\}$ de V com produto interno euclidiano e uma tranformação linear $T : V \to V$ uma transformação linear. A matriz de T^* nessa base é a transposta da matriz de T, isto é,
$$T]_B^* = T]_B^t = \left(a_{ji}\right)_{ij}.$$

3. Temos que
$$(T]_B S]_B)^* = S]_B^* T]_B^*$$
o que acarreta
$$(T]_B S]_B)^t = S]_B^t T]_B^t.$$

4. Mostre que a matriz de uma transformação ortogonal T satisfaz
$$T]_B^t = T]_B^{-1}.$$

Com a mesma associação que a cada transformação linear associamos uma única matriz dessa transformação, as transformações ortogonais estarão associadas a matrizes que satisfazem a mesma propriedade da Proposição acima, 5.1.1, isto é, A é uma matriz

$$(T]_B S]_B)^* = S]_B^* T]_B^*$$

Estas matrizes são chamadas **Matrizes Ortogonais**. O conjunto das matrizes ortogonais de ordem $n \times n$, denotado por $O(n)$, também será um grupo, de fato será subgrupo de $GL(n, \mathbb{R})$, também chamado de **Grupo Ortogonal**.

O determinante de uma matriz ortogonal só pode assumir os valores 1 e -1.

A intersecção de dois subgrupos de um grupo G é um subgrupo de G.

Corolário 5.1.0.1. O conjunto das matrizes ortogonais de determinante igual a 1, denotado por $SO(n)$ e definido por

$$SO(n) = SL(n, \mathbb{R}) \cap O(n)$$

também é um grupo, denominado **Grupo Ortogonal Especial**, pois trata-se da intersecção de dois subgrupos de $GL(n, \mathbb{R})$.

5.1.2 *Homomorfismos*

Definição 5.1.4 (Homomorfismo)**.** Dados dois grupos G e H, uma função $\varphi : G \to H$ é um Homomorfismo de Grupos se

$$\varphi(ab) = \varphi(a)\varphi(b),$$

para todos os elementos $a, b \in G$.

Se o homomorfismo é bijetivo, dizemos que ele é um Isomorfismo.

Quando existe um isomorfismo entre os grupos G e H, denotaremos $G \equiv H$ e diremos que G e H são isomorfos.

Lema 5.1.0.6. Se $\varphi : G \to H$ é um homomorfismo de grupos, então

1. $\varphi(e_G) = e_H$.

2. Para qualquer $a \in G$, temos que $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

Se $\varphi : G \to H$ é um homomorfismo de grupos e $K \subseteq G$ é um subgrupo, então $\varphi(K) \subseteq H$ também é um subgrupo. Se K é um subgrupo abeliano de G, então $\varphi(K)$ também é subgrupo abeliano de H.

Teorema 5.1.1. Todo grupo G é isomorfo a um subgrupo do grupo das bijeções em G.

Corolário 5.1.1.1 (Teorema de Cayley)**.** Todo grupo finito é isomorfo a um subgrupo de um grupo de permutações.

Definição 5.1.5 (Núcleo do Homomorfismo)**.** Dado um homomorfismo de grupos $\varphi : G \to H$, definimos o Núcleo de φ, como o subconjunto

$$ker\,(\varphi) = \{a \in G : \; \varphi(a) = e_H\}\,.$$

Seja $\varphi : G \to H$ um homomorfismo de grupos.

1. O núcleo de φ é um subgrupo de G.
2. φ é injetivo se, e somente se $ker(\varphi) = \{e_G\}$.

Seja V um espaço vetorial de dimensão finita n, com uma base $B = \{e_1, \ldots, e_n\}$ e dada uma transformação linear $T : V \to V$, denotemos por $T]_B$ a matriz da transformação linear na base B. A aplicação

$$\begin{array}{rcl}]_B : GL(V) & \longrightarrow & GL(n, \mathbb{R}) \\ T & \longmapsto & T]_B \end{array}$$

é um isomorfismo de grupos.

Corolário 5.1.1.2. Considerando o isomorfismo da proposição anterior, a Proposição 5.1.2 e supondo que V é um espaço com produto interno e que a base escolhida seja ortonormal com relação a este produto interno, temos que

$$O(V) \equiv O(n).$$

Exemplo 5.1.1.1. A aplicação

$$\begin{array}{rcl} det : GL(n, \mathbb{R}) & \longrightarrow & \mathbb{R}^* \\ T & \longmapsto & \det(T) \end{array}$$

onde $\mathbb{R}^*$ é o grupo multiplicativo dos reais não nulos, é um homomorfismo de grupos, devido à propriedade multiplicativa dos determinantes. Note que o núcleo dessa aplicação determinante é o conjunto das matrizes de determinante igual a 1, ou seja,

$$ker(\det) = SL(n, \mathbb{R}).$$

Seja G um grupo e H um subgrupo. As relações

1. $$g \equiv_E h \Leftrightarrow g^{-1}h \in H$$

2. $$g \equiv_D h \Leftrightarrow gh^{-1} \in H$$

são relações de equivalência em G.

Definição 5.1.6 (Classes Laterais)**.** Dado um subgrupo H de um grupo G e um elemento $a \in G$, definimos a Classe Lateral à Esquerda de a em relação a H como o conjunto:

$$aH = \{k \in G : k \equiv_E a\}.$$

Similarmente, a Classe Lateral à Direita de a em relação a H é o conjunto

$$Ha = \{k \in G : k \equiv_D a\}.$$

Podemos também caracterizar uma classe lateral à esquerda aH como o conjunto dos elementos $g \in G$ tais que podem ser escritos como $g = ab$, para algum $b \in H$, isto é,

$$aH = \{g \in G : \ g = ab, \text{ para algum } b \in H\}$$

Vamos assumir que as classes laterais sejam classes laterais à esquerda, a menos que se seja mencionado o contrário.

Duas classes laterais à esquerda a_1H e a_2H ou são disjuntas ou são iguais.

Mostre que a aplicação

$$\begin{aligned} L_a : H &\longrightarrow aH \\ b &\longmapsto ab \end{aligned}$$

é uma bijeção (não necessariamente homomorfismo) entre H e G.

Definição 5.1.7 (Ordem de um Grupo)**.** Seja G um grupo. A ordem de um grupo é a sua cardinalidade.

A ordem de um elemento a do grupo é o menor valor inteiro positivo n tal que $a^n = 1$, se este número existir.

Se este número não existe, o elemento tem ordem infinita.

Se um grupo G tem ordem finita, então todos os seus elementos também possuem ordem finita e a ordem de cada elemento divide a ordem do grupo. (Veja o Teorema de Lagrange, 5.1.2)

A ordem de um grupo G e de um elemento a representadas por $|G|$ e $|a|$, respectivamente.

Teorema 5.1.2 (Teorema de Lagrange)**.** Seja G um grupo finito e H um subgrupo e sejam $|G|$ e $|H|$ suas respectivas ordens (número de elementos). Então a quantidade de classes laterais distintas, $\#C$ e H é igual a

$$\#C = \frac{|G|}{|H|}.$$

Corolário 5.1.2.1. A ordem de um subgrupo de um grupo finito é sempre um divisor da ordem do grupo.

Se um grupo G não é abeliano, e H é um subgrupo qualquer, não é verdade que as classes laterais à esquerda coincidem com as classes laterais a direita.

Definição 5.1.8 (Subgrupo Normal)**.** Seja G um grupo e $H \subseteq G$ um subgrupo. Se as classes laterais à esquerda e à direita de H coincidem, dizemos que H é um Subgrupo Normal de G, denotado como $H \trianglelefteq G$.

Seja G um grupo e $H \subseteq G$ um subgrupo. Então são equivalentes:

1. H é subgrupo normal;
2. Para qualquer $a \in G$, temos que $aHa^{-1} = H$.
3. Para qualquer $a \in G$, temos que $aHa^{-1} \subseteq H$.

Considere $\varphi : G \to H$ um homomorfismo de grupos. O núcleo de φ é um subgrupo normal de G.

5.1.3 *Grupo Quociente*

Seja H um subgrupo normal de G podemos definir no conjunto quociente, G/H, uma estrutura de grupo. Observe que

$$G/H = \{aH : \ a \in G\}$$

De fato, definimos uma operação em G/H por

$$\begin{array}{rcl} G/H \times G/H : & \longrightarrow & G/H \\ (aH, bH) & \longmapsto & abH \end{array}$$

Observamos que

1. Como H é um subgrupo normal é indiferente se as classes são à direita ou à esquerda.
2. Esta operação está bem definida.
3. Esta operação estrutura G/H como um grupo.

Seja G um grupo e $a \in G$. A aplicação can^onica,

$$\begin{aligned} \pi : G &\longrightarrow G/H \\ a &\longmapsto aH \end{aligned}$$

denominada **Aplicação Canônica** é sobrejetora.

Teorema 5.1.3 (Teorema do Isomorfismo)**.** Seja $\varphi : G \to H$ um homomorfismo de grupos, então existe um único isomorfismo $\overline{\varphi} : G/ker(\varphi) \to Im(\varphi)$ tal que o diagrama abaixo comuta

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & H \\ G/ker(\varphi) \arrow[r, "\overline{\varphi}"'] & Im(\varphi) \arrow[u, "i"'] \end{tikzcd}$$

onde $i : Im(\varphi) \to H$ é a inclusão canônica.

Figura 18: Diagrama Comutativo: Teorema do Isomorfismo

Isto é.

$$i \circ \overline{\varphi} \circ \pi = \varphi.$$

Corolário 5.1.3.1. Se $\varphi : G \to H$ é um homomorfismo sobrejetor então $H \equiv G/ker(\varphi)$.

5.2 AÇÕES DE GRUPOS

Sabemos que todo grupo é isomorfo a um subgrupo de um grupo de bijeções em um conjunto (em particular, das bijeções no próprio grupo).

As situações onde um grupo pode ser visto como grupo de bijeções são as que realmente aparecem nas aplicações da teoria. É agindo como um grupo de bijeções que o grupo se concretiza, se incorpora e pode ser utilizado como uma ferramenta para o estudo das simetrias.

Definição 5.2.1 (Ação)**.** Uma ação à esquerda de um grupo G em um conjunto X não-vazio é um homomorfismo de G no grupo das bijeções em X, $Bij(X)$.

Vamos supor que as ações são feitas à esquerda mas é possível construir toda a teoria para ações à direita. Para isto, primeiramente precisamos definir o conceito de Grupo Oposto.

Definição 5.2.2 (Grupo Oposto)**.** Dado um grupo G, definimos o seu grupo oposto, G_{op} como o conjunto G munido com uma operação dada por

$$\begin{array}{rcl} \bullet : G \times G & \longrightarrow & G \\ (a,b) & \longmapsto & a \bullet b = ba \end{array}$$

Definição 5.2.3 (Ação de Grupo)**.** Uma ação à direita sobre um grupo G em um conjunto X não-vazio é um homomorfismo de G_{op} no grupo das bijeções em X.

Vamos denotar uma ação (á esquerda) por

$$\begin{array}{rcl} \alpha : G & \longrightarrow & Bij(X) \\ a & \longmapsto & \begin{array}{rcl} \alpha_a : X & \to & X \\ x & \mapsto & \alpha_a(x) \end{array} \end{array}$$

Como α é um homomorfismo, então temos que

1. Sejam $a, b \in G$ e $x \in X$

$$\alpha_a\left(\alpha_b\left(x\right)\right) = \alpha_{ab}\left(x\right).$$

2. Para todo $x \in X$,
$$\alpha_{e_G} = Id_X,$$
ou seja, $\alpha_{e_G}(x) = x$.

3. Para todo $a \in G$,
$$\alpha^{-1}{}_a = \alpha_{a^{-1}}$$

Definição 5.2.4 (Órbita)**.** Seja α uma ação de um grupo G sobre um conjunto X e considere um elemento $x \in X$. Definimos a órbita do elemento x como sendo o conjunto
$$O_x = \{\alpha_a(x) : \ a \in G\}.$$

Uma ação α de um grupo G sobre um conjunto X introduz uma relação de equivalência em X.

Corolário 5.2.0.1. Duas órbitas pela ação de um grupo ou são disjuntas ou coincidentes.

Definição 5.2.5 (Domínio Fundamental)**.** Sejam X um conjunto e α uma ação de um grupo G sobre X. Um subconjunto $F \subseteq X$ é dito ser um Domínio Fundamental se, para todo $x \in X$, existem únicos $y \in F$ e $a \in G$ tal que $x = \alpha_a(y)$.

Note que não pode haver dois elementos da mesma órbita no domínio fundamental e todas as órbitas devem estar contempladas no domínio, assim qualquer ponto de X pode ser alcançado atráves da ação agindo sobre pontos de F.

5.2.1 *Exemplos*

1. Seja o grupo aditivo $\mathbb{Z}$ agindo sobre a reta real $\mathbb{R}$ da seguinte maneira:
$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ x & \longmapsto & \alpha_n(x) = x + n. \end{array}$$

Observe que α é uma ação, pois

- Para todo $n, m \in \mathbb{Z}$ e todo $x \in \mathbb{R}$ temos
$$\alpha_n\left(\alpha_m\left(x\right)\right) = \alpha_n\left(x+m\right) = x+m+n = \alpha_{n+m}\left(x\right);$$
- Para todo $x \in \mathbb{R}$ temos
$$\alpha_0(x) = x + 0 = x.$$

Dado um elemento $x \in \mathbb{R}$, sua órbita será o conjunto
$$O_x = \left\{x + n : n \in \mathbb{Z}\right\}.$$

Assim, se tomarmos um intervalo da forma $[n, n+1[$, com $n \in \mathbb{Z}$ teremos um domínio fundamental, pois para quaisquer dois pontos, x, y deste intervalo, temos que $|x - y| < 1$, portanto não podem existir dois pontos da mesma órbita neste intervalo.

Por outro lado, seja $x \in \mathbb{R}$ um número qualquer, então
$$\begin{aligned} x &= n + x - n \\ &= n + (x - n - [x-n]) + [x-n] \\ &= [x-n] + n + (x - n - [x-n]) \\ &= \alpha_{[x-n]}\left(n + (x - n - [x-n])\right), \end{aligned}$$

onde $[a]$ denota o maior inteiro menor que a, e $a[a] \in [0, 1[$ é a parte fracionária do número a.

Assim, o número x é a ação do número inteiro $[x-n]$ sobre $n + (xn - [x-n]) \in [n, n+1[$, o que mostra que este intervalo é um domínio fundamental.

Por outro lado, o quociente é o conjunto das órbitas e podemos caracterizá-lo como a circunferência unitária através da função
$$\begin{aligned} f : \mathbb{R}/\mathbb{Z} &\longrightarrow S^1 \\ O_x &\longmapsto (\cos(2\pi x), \sin(2\pi x)) \end{aligned}$$

Esta aplicação está bem definida, pois se $O_x = O_y$ isto significa que $y = x + n$, para algum número inteiro n. Então

$$\begin{aligned} f(O_y) &= (\cos(2\pi y), \sin(2\pi y)) \\ &= (\cos(2\pi(x+n)), \sin(2\pi(x+n))) \\ &= (cos2x, sin2x) \\ &= f(Ox). \end{aligned}$$

Também podemos ver a injetividade, pois se $f(O_y) = f(O_x)$, então

$$(\cos(2\pi y), \sin(2\pi y)) = (\cos(2\pi x), \sin(2\pi x)),$$

o que implica que

$$\cos(2\pi y) = \cos(2\pi x) \text{ e } \sin(2\pi y) = \sin(2\pi x).$$

Isto somente ocorre quando existe um inteiro n tal que $y = x + n$, ou ainda, quando $y \in O_x$, que equivale a dizer que $O_x = O_y$.

A sobrejetividade decorre imediatamente do fato que todo ponto $p \in S^1$ possui coordenadas $p = (\cos(\theta), \sin(\theta))$, para $\theta \in [0, 2\pi[$, assim $p = f(O_{\theta/2\pi})$.

Dada uma ação de um grupo G sobre um conjunto X, podemos definir outros subconjuntos que caracterizarão tipos específicos de ações.

Definição 5.2.6 (Estabilizador)**.** Considere uma ação α de um grupo G sobre um conjunto X. O subgrupo Estabilizador de um elemento $x \in X$ é definido como

$$Stab_x = \{a \in G : \alpha_a(x) = x\}$$

De forma semelhante, podemos falar do subgrupo estabilizador de um subconjunto $Y \subseteq X$

$$Stab_Y = \{a \in G : \alpha_a(Y) \subseteq Y\}.$$

Note que os elementos de um subconjunto não precisam ficar fixos pela ação do grupo, apenas que suas órbitas precisam estar contidas neste subconjunto.

Quando $Stab_Y = G$, dizemos que $Y \subseteq X$ é um subconjunto invariante pela ação do grupo G.

Uma definição dual é o conjunto dos pontos fixos pela ação de um determinado elemento ou subgrupo de G.

Definição 5.2.7 (Ponto Fixo)**.** O subconjunto dos Pontos Fixos de um elemento $a \in G$ é o conjunto

$$Fix_a = \{x \in X : \alpha_a(x) = x\}.$$

Se $H \subseteq G$ é um subgrupo de G, o conjunto dos pontos fixos pela ação de H é definido por

$$Fix_H = xX|g(x) = x, gH.$$

Definição 5.2.8 (Tipos de Ações)**.** Uma açãoo α de G em X é dita ser

1. Fiel, se dado $a \in G$ tal que $Fix_a = X$, então $a = e_G$.

2. Livre, se dado $a \in G$ tal que $Fix_a \neq \emptyset$, então $a = e_G$.

3. Transitiva, se $O_x = X$, para todo elemento $x \in X$. Ou, equivalentemente, se $x, y \in X$ então existe $a \in G$ tal que $y = \alpha_a(x)$.

Teorema 5.2.1. Seja α uma ação de um grupo G sobre um grupo H por homomorfismos em si mesmo. Então, o produto cartesiano $H \times G$ pode ser munido com uma operação dada por

$$(b_1, a_1) \cdot (b_2, a_2) = (b_1 \alpha_{a_1} (b_2), a_1 a_2).$$

Com esta operação, o produto cartesiano é investido de uma estrutura de grupo, denotado por $H \propto_\alpha G$ e denominado **Produto Semidireto** de H por G.

Além disso

1. As inclusões

$$\begin{aligned} i_1 : H &\longrightarrow H \propto_\alpha G \\ b &\longmapsto (b, e_G) \end{aligned}$$

   e

$$\begin{aligned} i_2 : H &\longrightarrow H \propto_\alpha G \\ a &\longmapsto (e_H, a) \end{aligned}$$

   são homomorfismos de grupo injetores.

2. O subgrupo $i_1(H)$ é subgrupo normal.

3. A ação de G em H é escrita como um homomorfismo interno de $H \propto_\alpha G$ nele mesmo, isto é,

$$i_1 (\alpha_a (b)) = i_2 (a) \cdot i_1 (b) \cdot (i_2 (a))^{-1}$$

   Por outro lado, se K é um grupo tal que

   (a) Os grupos G e H são subgrupos de K e $H \trianglelefteq K$.

   (b) Para todo $c \in K$ existem $a \in G$ e $b \in H$ tal que $c = ba$, isto é, $K = HG$.

   (c) Para todo $a \in G$ e todo $b \in H$, temos que $ab = \alpha_a (b) a$ então $K \equiv H \propto_\alpha G$.

6

ISOMETRIA

Vamos apresentar noções básica de isometrias, que possuem a propriedade de preservar a distância entre dois pontos. Entre as isometrias se encontram as translações, as rotações e as reflexões.

6.1 TRANSFORMAÇÃO NO PLANO

Definição 6.1.1 (Transformação)**.** Uma transformação em um espaço euclidiano $n-$dimensional é uma função $T : \mathbb{E}^n \to \mathbb{E}^n$.

Dada uma transformação estamos interessados em estudar como ela transforma figuras geométricas do plano. Ao estabelecer um sistema cartesiano podemos descrever uma transformação através de suas coordenadas, ou seja, escrevendo

$$T(x_1, x_2) = (y_1, y_2)$$

e expressando x_2 e y_2 como equações com variáveis x_1 e y_1.

Exemplo 6.1.0.1. Consideremos a transformação do plano

$$\begin{array}{rcl} T : \mathbb{E}^2 & \longrightarrow & \mathbb{E}^2 \\ (x_1, x_2) & \longmapsto & T(x_1, x_2) = \left(\frac{x_1 - x_2}{\sqrt{2}}, \frac{x_1 + x_2}{\sqrt{2}}\right) \end{array}$$

Seja $r = \{(x_1, x_2) : x_1 = x_2\}$ a reta diagonal. A imagem de (x_1, x_1) por T é $(0, \sqrt{2}x_1)$, isto é,

$$T(x_1, x_1) = \left(0, \frac{2x_1}{\sqrt{2}}\right).$$

Logo essa imagem está no eixo O_{x_2}.

Por outro lado, todo ponto do eixo O_{x_2} é imagem por T de um ponto de $\mathbb{E}^2$. De fato, dado $(0, y_2) \in 0_{x_2}$, seja

$$(0, y_2) = T(x_1, x_2) \Rightarrow (0, y_2) = \left(\frac{x_1 - x_2}{\sqrt{2}}, \frac{x_1 + x_2}{\sqrt{2}}\right)$$

temos $x_1 = x_2$ e $x_2 = \sqrt{2}/2y_2$ portanto

$$(x_1, x_2) = (\sqrt{2}/2y_2, \sqrt{2}/2y_2) \in r.$$

Além disso, a restrição $T : r \to O_{x_2}$ é injetiva, pois

$$\begin{aligned} T(x_1, x_1) = T(y_1, y_1) \quad &\Rightarrow \quad (0, \sqrt{2}x_1) = (0, \sqrt{2}y_1) \\ &\Rightarrow \quad x_1 = y_1 \\ &\Rightarrow \quad (x_1, x_1) = (y_1, y_1). \end{aligned}$$

Logo T leva a reta r bijetivamente sobre a reta O_{x_2}.

6.1.1 *Isometria no Plano*

Dentre as transformações no plano, estudaremos aquelas que preservam a congruência de triângulos. Assim, vamos colocar condições sobre uma transformação $T : \mathbb{E}^2 \to \mathbb{E}^2$ para qualquer triângulo do plano seja congruente com sua imagem via T.

Definição 6.1.2 (Isometria)**.** Uma isometria um espaço euclidiano $n-$dimensional é uma transformação $T : \mathbb{E}^n \to \mathbb{E}^n$

que preserva distância, d, determinada pelo produto interno do espaço, ou seja, T é uma isometria quando

$$d(T(u), T(v)) = d(u, v)$$

para quaisquer u e v de $\mathbb{E}^n$.

Exemplo 6.1.0.2. Considere o espaço euclidiano $2-$dimensional $\mathbb{R}^2$ munido da métrica usual

$$\begin{aligned} d(u,v) &= d\left((x_1, x_2), (y_1, y_2)\right) \\ &= ||(x_1, x_2) - (y_1, y_2)|| \\ &= \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}. \end{aligned}$$

A transformação

$$\begin{array}{rcl} T : \mathbb{E}^2 & \longrightarrow & \mathbb{E}^2 \\ (x_1, x_2) & \longmapsto & T(x_1, x_2) = \left(\frac{x_1 - x_2}{\sqrt{2}}, \frac{x_1 + x_2}{\sqrt{2}}\right) \end{array}$$

é uma isometria. De fato,

$$\begin{aligned} d(T(u), T(v)) &= d\left(T(x_1, x_2), T(y_1, y_2)\right) \\ &= d\left(\frac{x_1 - x_2}{\sqrt{2}}, \frac{x_1 + x_2}{\sqrt{2}}\right) \\ &= d(u, v) \end{aligned}$$

Exemplo 6.1.0.3 (Translação)**.** Sejam a e b números reais. Consideremos a transformação do plano

$$\begin{array}{rcl} T : \mathbb{E}^2 & \longrightarrow & \mathbb{E}^2 \\ (x_1, x_2) & \longmapsto & T(x_1, x_2) = (x_1 + a, x_2 + b) \end{array}$$

Essa transformação é chamada de **Translação**

Uma translação é uma isometria.

Propriedades de Isometria

Toda isometria $T : \mathbb{E}^2 \to \mathbb{E}^2$ é injetiva.

Sejam P e Q pontos distintos de $\mathbb{E}^2$ e $T : \mathbb{E}^2 \to \mathbb{E}^2$ uma isometria. Então T leva o segmento $\vec{PQ}$ sobre o segmento $T(P)\vec{T}(Q)$.

A propriedade acima mostra que toda isometria leva pontos colineares em pontos colineares, mantendo a sua ordenação e suas distâncias. Notemos também que a imagem por uma isometria de três pontos P, Q e R não colineares não são colineares.

Pois, por exemplo, se $T(Q)$ estivesse entre $T(P)$ e $T(R)$, teríamos

$$d\left(T\left(P\right), T\left(Q\right)\right) + d\left(T\left(Q\right), T\left(R\right)\right) = d\left(T\left(P\right), T\left(R\right)\right),$$

mas

$$d\left(P, Q\right) + d\left(Q, R\right) > d\left(P, R\right),$$

contrariando a definição de T.

A imagem de uma reta por uma isometria é uma reta.

As imagens de retas paralelas por uma isometria são retas paralelas.

A proposição acima não significa que a imagem de uma reta por uma isometria seja uma reta paralela a inicial.

Seja $\triangle PQR$ um triângulo retângulo com ângulo reto em P. Sua imagem por uma isometria é o triângulo retângulo $\triangle T(P)T(Q)T(R)$ com ângulo reto em $T(P)$.

Dado um ângulo $< PQR$ e uma isometria T, então $T\left(< PQR\right)$ é o ângulo $< T(P)T(Q)T(R)$ e ambos sâo congruentes.

Toda isometria $T : \mathbb{E}^2 \to \mathbb{E}^2$ é sobrejetiva.

Logo, toda isometria é uma bijeção.

A inversa de qualquer isometria é uma isometria.

A composta de duas isometrias é uma isometria.

Todos esses resultados nos permitem concluir que o conjunto das isometrias munido com a operação de composição usual é um grupo.

Teorema 6.1.1 (Grupo da Isometria)**.** O conjunto das isometrias munido com a operação de composição é um grupo.

1. A composição de isometrias é isometria;
2. A identidade $Id_{\mathbb{E}^2}$ é uma isometria;
3. A operação inversa de uma isometria é uma isometria;

Definição 6.1.3 (Ponto Fixo)**.** Seja $T : \mathbb{E}^2 \to \mathbb{E}^2$ uma transformação. Um ponto fixo da transformação T é todo ponto P tal que $T(P) = P$.

Quantos pontos fixos pode ter uma isometria? Quais são as propriedades dos pontos fixos de uma isometria?

Se P e Q são pontos fixos de uma isometria T, então todos os pontos da reta que passa por P e Q são pontos fixos.

Sejam S e T isometrias e r uma reta do plano. Se existirem pontos $P \neq Q$ em r tais que $S(P) = T(P)$ e $S(Q) = T(Q)$ então $S(x) = T(x)$ para todo $x \in r$.

Teorema 6.1.2. Se uma isometria T fixa três pontos não colineares, então T é a identidade.

Teorema 6.1.3. Se duas isometrias T e S coincidem em três pontos não colineares, então $T = S$.

Assim, podemos classificar as isometrias em três tipos diferentes não triviais:

1. Com 2 pontos fixos (e, portanto, com uma reta fixa);
2. Com 1 ponto fixo;
3. Com nenhum ponto fixo.

É interessante notar que esses resultados só dependem dos axiomas básicos da Geometria Euclidiana.

Congruências e Isometrias

A imagem de um triângulo por uma isometria é um triângulo congruente ao primeiro. O estudo das isometrias nos fornece uma maneira de estudar o conceito de congruência atráves de movimentos herdados via isometrias.

Teorema 6.1.4. A imagem de um triângulo por uma isometria é congruente ao próprio triângulo original.

6.1.2 *Reflexão*

As reflexões constituem um tipo importante de isometria.

Definição 6.1.4 (Ponto Simétrico)**.** Sejam P e P_0 pontos e r uma reta. Dizemos que P_0 é simétrico a P se r for a mediatriz do segmento $\vec{PP_0}$.

No caso de P pertencer à reta r o ponto simètrico de P será o próprio P.

Definição 6.1.5 (Reflexão)**.** Dada uma reta r, chama-se reflexão em torno da reta r a transformação T tal que a todo ponto P, o ponto $P_0 = T(P)$ é o simétrico de P em relação a r.

Observemos que a reflexão em torno de uma reta fixa os pontos da reta e nenhum outro.

Na verdade, essa transformação é uma isometria.

Teorema 6.1.5. Toda reflexão é uma isometria.

Propriedades das Reflexão

Sejam P e P_0 dois pontos. Então existe uma única reflexão levando P em P_0.

Vejamos agora como levar um triângulo sobre outro congruente a ele. Come¸caremos com o caso particular em que os triângulos têm em comum um lado.

Se dois triângulos diferentes e congruentes têm um lado em comum, então existe uma reflexão levando um sobre o outro.

Se dois triângulos congruentes têm em comum apenas um vértice, então existe uma isometria levando um sobre o outro.

Essa isometria é uma reflexão ou a composta de duas reflexões.

Teorema 6.1.6. Dados dois triângulos congruentes, existe uma isometria que leva um sobre o outro.

Essa isometria pode ser a identidade, uma reflexão, ou a composta de duas ou três reflexões.

Teorema 6.1.7. Toda isometria é a identidade, uma reflexão, ou a composta de duas ou três reflexões.

6.1.3 *Translação*

Definição 6.1.6 (Translação)**.** Sejam a_1 e a_2 números reais. A transformação do plano $T : \mathbb{E}^2 \to \mathbb{E}^2$ definida por

$$T(x_1, x_2) = (x_1 + a_1, x_2 + a_2)$$

chama-se translação determinada por (a_1, a_2).

Propriedades da Translação

Toda translação é uma isometria.

Considerando $\vec{v} = (a_1, a_2)$ como um vetor, a translação determinada por (a_1, a_2) pode ser definida por

$$T_{\vec{v}}(P) = P + \vec{v}.$$

Ela desloca todos os pontos do plano na mesma direção e na distância $|\vec{v}|$.

Teorema 6.1.8. Toda translação que não é a identidade é composta de duas reflexões em torno de duas retas paralelas.

6.1.4 *Rotação*

As rotações constituem um tipo especial de isometria.

Definição 6.1.7 (Rotação)**.** Sejam Q um ponto e $\alpha \in [0, 2\pi)$ um ângulo. A rotação

$$T : \mathbb{E}^2 \rightarrow \mathbb{E}^2$$

é uma transformação do plano definida da seguinte forma:

1. $T(Q) = Q$;

2. Se $P \neq Q$ é um ponto qualquer, $T(P)$ é o ponto tal que $Q\vec{T}(P) = \vec{Q}P$;

3. A medida do ângulo $< PQT(P)$ no sentido horário a partir da semirreta $\vec{Q}P$ é α.

Propriedades de Rotação

Teorema 6.1.9. Toda rotação é uma isometria.

6.1.5 *Propriedades Gerais*

Teorema 6.1.10. As translaçõees e as rotações são isometrias que preservam a orientação e as reflexões são isometrias que invertem a orientação.

Teorema 6.1.11. Toda rotação diferente da identidade é a composta de duas reflexões.

Definição 6.1.8 (Reflexão! Com deslizamento)**.** Uma Reflexão com Deslizamento é uma composição de uma reflexão em torno da reta r com uma translação com vetor de deslocamento $\vec{v} \neq 0$ paralelo à reta r.

Teorema 6.1.12. As isometrias do plano são: a identidade, as translações, as rotações, as reflexões e as reflexões com deslizamento.

6.2 EXEMPLO

[Grupo Diedral D_n] Um grupo diedral o grupo de simetrias de um polgono regular de n lados, denotado por D_n ou D_{2n}.

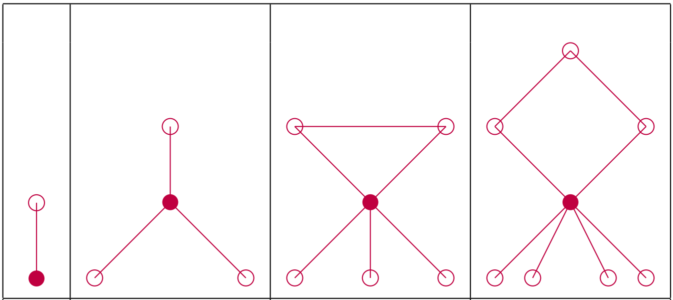
Sua representao dada por

$$D_n = \langle x, y : \; x^n = 1, \; y^2 = 1, \; (xy)^2 = 1 \rangle.$$

Propriedades

- O grupo possui $2n$ elementos:
  - O elemento neutro;
  - $n - 1$ rotaes prprias;
  - n reflexes.
- Para $n > 2$, o grupo no abeliano.
- O subgrupo das rotaes isomorfo ao grupo cclico $\mathbb{Z}_n$

Grafo de Ciclos



D_1	D_2	D_3	D_4

Vamos considerar o D_4:

Considere o quadrado com vrtices consecutivos, numerados por $1,2,3,4$, centrados na origem do plano xy com lados paralelos aos eixos.

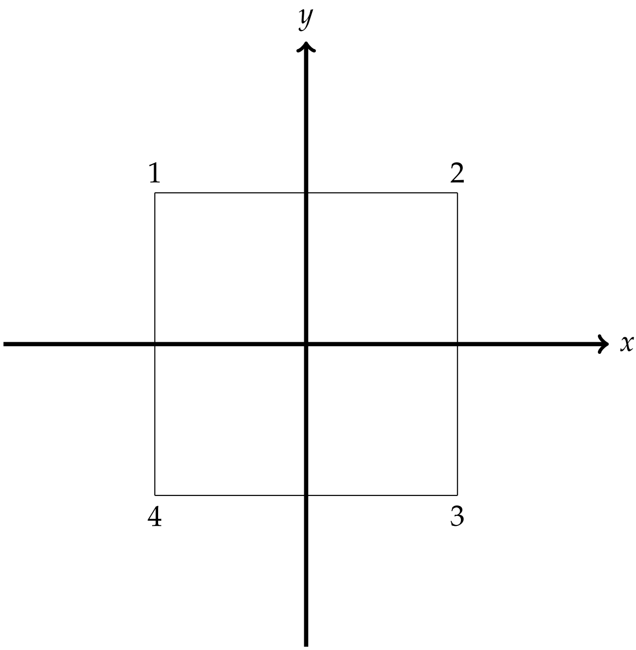
,

Seja D_4^* o conjunto das transformaes do quadrado, isto ,

$$D_4^* = \{R, R^2, R^3, Id, T_x, T_y, T_{1,3}, T_{2,4}\}$$

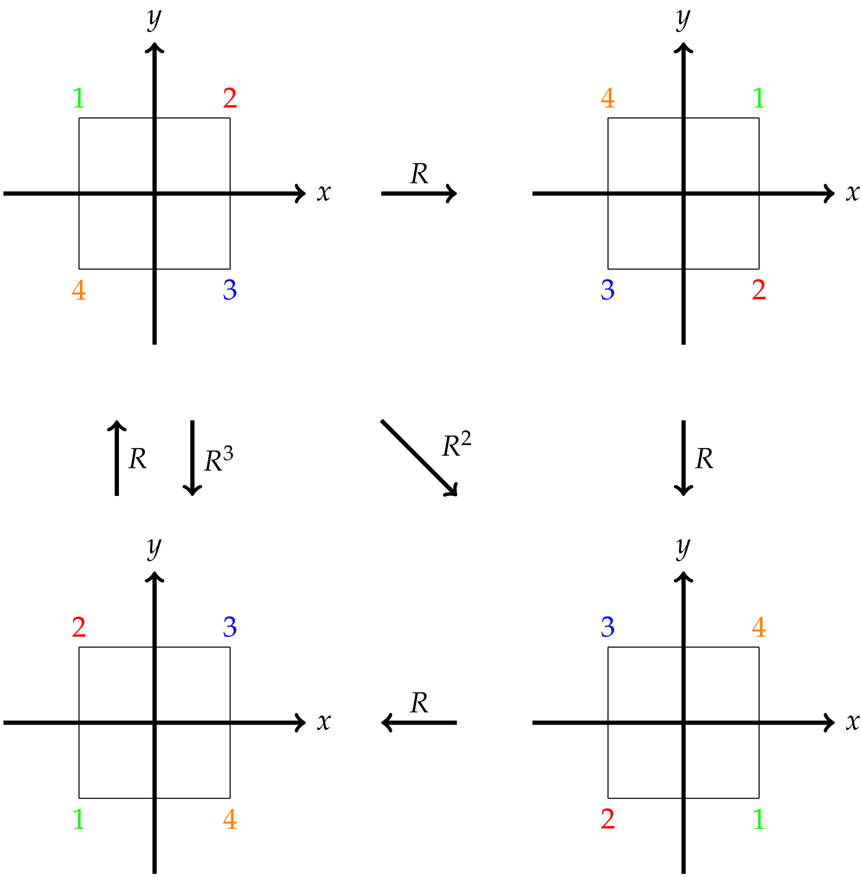
Rotaes

R uma rotao no sentido horrio na origem de 90^o,
R^2 uma rotao no sentido horrio na origem de 180^o,
R^3 uma rotao no sentido horrio na origem de 270^o,
Id uma rotao no sentido horrio na origem de 360^o,

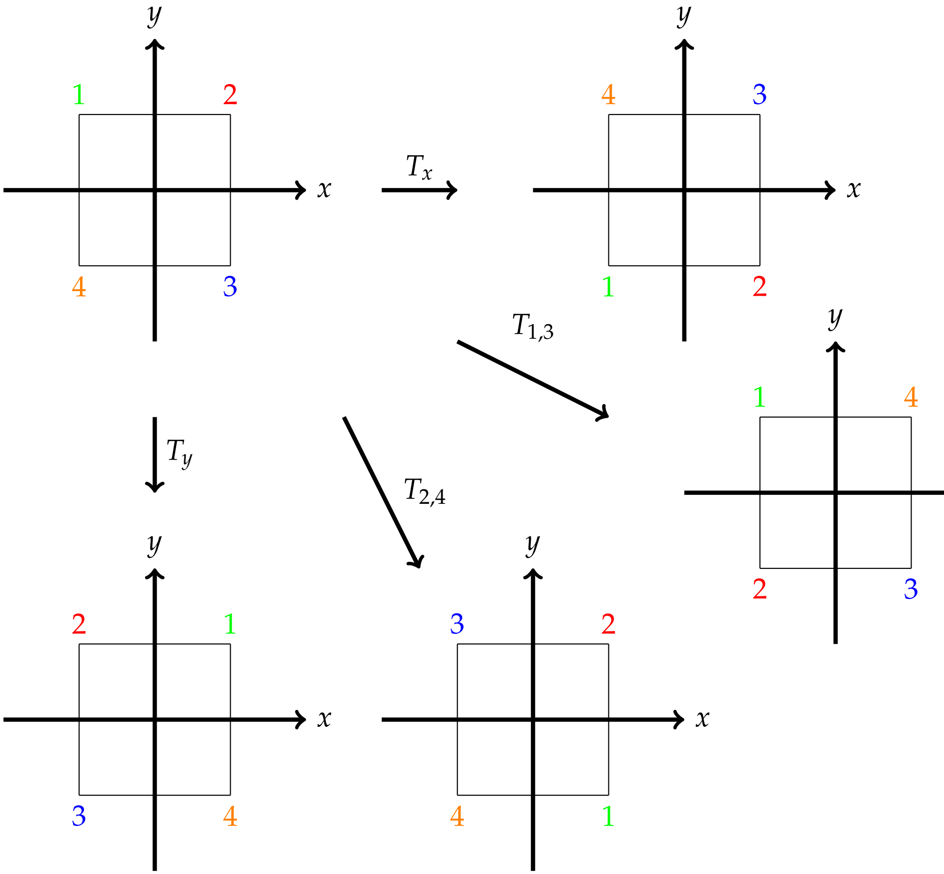


Reflexes

T_x uma reflexo no eixo-x,
T_y uma reflexo no eixo-y,
$T_{1,3}$ uma reflexo na diagonal de vrtices 1 e 3,
$T_{2,4}$ uma reflexo na diagonal de vrtices 2 e 4.



y
x
1
2
3
4
R
R^3
R^2



y
x
1
2
4
3
T_x
4
3
1
2
$T_{1,3}$
1
4
2
3
T_y
$T_{2,4}$
2
1
3
4
3
2
4
1

7

GRUPO ORTOGONAL

7.1 DEFINIÇÕES PRELIMINARES

Definição 7.1.1 (Corpo)**.** Um corpo K é um anel munido de duas operações, adição e multiplicação satisfazendo as seguintes condições:

1. Distributividade da multiplicação em relação a adição
$$a(b+c) = ab + ac;$$
2. K é um grupo abeliano sobre a adição, com identidade escrita como O_K.
3. $K \setminus \{0_K\}$ é um grupo abeliano sobre a multiplicação.

Um corpo não possui divisores de zero, isto é, se K é um corpo e $a \neq 0_K$ e $b \neq 0_K$ com $a, b \in K$ então $ab \neq 0_K$.

Definição 7.1.2 (Anel)**.** Um anel A é um conjunto que possui duas operações de adição e multiplicação satisfazendo as seguintes condições:

1. A é um grupo comutativo sobre a adição;
2. A multiplicação é associativa, isto é,
$$(ab)c = a(bc),\ \forall\ a, b, c \in A;$$

3. A adição é distributiva em relação à multiplicação, isto é
$$a(b+c) = ab + ac, \ \forall\ a, b, c \in A;$$
$$(a+b)c = ac + bc, \ \forall\ a, b, c \in A.$$

Geralmente o anel A é denotado por $(A, +, \cdot)$.

0 anel A é comutativo se a multiplicação for comutativa, isto é,
$$ab = ba\ \forall a, b \in A.$$

Um anel $(A, +, \cdot)$ é denominado uma álgebra sobre $\mathbb{R}$ se A é um espaço vetorial real tal que
$$\alpha(ab) = (\alpha a)b = a(\alpha b)$$
para todos $a, b \in A$ e $\alpha \in \mathbb{R}$.

Definição 7.1.3 (Unidade)**.** Se A é um anel, dizemos que um elemento $u \in A$ é uma unidade (ou elemento inversivel) se existe algum $u' \in A$ tal que $uu' = 1_A = u'u$, isto é, se u possui um inverso multiplicativo.

Se A é um anel e U é o conjunto das unidades em A, então U é um grupo sobre a multiplicação.

Observamos que o conjunto das matrizes quadradas de ordem n, $M_n(\mathbb{R})$ é uma álgebra. 0 grupo das unidades no algebra é o grupo $GL(n, \mathbb{R})$. Estes é um tipo de Grupo Lineares Gerais,

Note que uma matriz $A \in M_n(\mathbb{R})$ é uma unidade, se e somente se, A determina um automorfismo sobre $\mathbb{E}^n$, isto é,

$A \in GL(n, \mathbb{R}) \longleftrightarrow$ para todo $v \in \mathbb{E}^n$, $T(v) = Av$ é um isomorfismo.

7.2 O GRUPO ORTOGONAL

Consideramos o conjunto

$$0(n,\mathbb{R}) = \{A \in GL\,(n,\mathbb{R}) : \langle Ax, Ay\rangle = \langle x,y\rangle \text{ para todo } x,y \in \mathbb{E}^n\}\,.$$

[Grupo Ortogonal] O conjunto $0(n,\mathbb{R})$ é um grupo.

Demonstração. Observamos que

- O $0(n,\mathbb{R})$ é fechado para o produto de matrizes, pois

  $$\langle (AB)x, (AB)y\rangle = \langle A(Bx), A(By)\rangle = \langle Bx, By\rangle = \langle x,y\rangle$$

- A matriz identidade I_n, está em $0(n,\mathbb{R})$, pois

  $$\langle x,y\rangle = \langle I_n x, I_n y\rangle$$

- Dada uma matriz $A \in 0(n,\mathbb{R})$ e sendo $B = \{e_1,\ldots,e_n\}$ uma baser ortonormal de $\mathbb{E}^n$, temos que

  $$\left\langle Ae_i, Ae_j\right\rangle = \left\langle e_i, e_j\right\rangle = \delta_{ij} = \begin{cases} 1, & \text{se } i = j \\ 0, & \text{se } i \neq j \end{cases}$$

  Por outro lado, Ae_i é exatamente a $i-$esima linha de A e podemos ver que $\left\langle Ae_i, Ae_j\right\rangle$ é exatamente a entrada ij do produto AA^t. Assim $AA^t = I_n$. De forma análoga, $A^tA = I_n$ portanto $A^t = A^{-1}$. Além disso,

  $$\begin{aligned} \langle x,y\rangle &= \langle I_n x, I_n y\rangle \\ &= \left\langle (AA^{-1})x, (AA^{-1})y\right\rangle \\ &= \left\langle A(A^{-1}x), A(A^{-1}y)\right\rangle \\ &= \left\langle A^{-1}x, A^{-1}y\right\rangle \end{aligned}$$

  Logo $A^{-1} \in 0(n,\mathbb{R})$.

□

Definição 7.2.1 (Grupo Ortogonal)**.** Chamamos de Grupo Ortogonal o conjunto

$$0\,(n,\mathbb{R}) = \{A \in GL(n,\mathbb{R}) : \langle Ax, Ay\rangle = \langle x,y\rangle\,,\ \text{para todo } x,y \in \mathbb{E}^n\}$$

Seja $A \in M_n(\mathbb{R})$. Então as seguintes condições são equivalentes:

1. $A \in 0(n,\mathbb{R})$;
2. $\left\langle Ae_i, A_{ej}\right\rangle = \delta_{ij}$;
3. A leva base ortonormal em base ortonormal;
4. As linhas de A formam uma base ortonormal;
5. As colunas de A formam uma base ortonormal
6. $A^t = A^{-1}$.

A Proposição acima nos diz que os elementos do grupo ortogonal estão associados à transformações lineares ortogonais.

Seja $A \in M_n\,(\mathbb{R})$. Então $A \in 0(n,\mathbb{R})$, se e somente se, A preservar a norma, isto é,

$$\langle Ax, Ax\rangle = \langle x,x\rangle \Leftrightarrow ||Ax|| = ||x||.$$

Definição 7.2.2 (Grupo Ortogonal Especial)**.** Definimos

$$SO(n) = \{A \in O(n,\mathbb{R} :\ \det(A) = 1\}$$

è chamamos de Grupo Ortogonal Especial (ou chamado Grupo de Rotações).

Um exemplo de um elemento de $0(2,\mathbb{R})$ é o elemento

$$A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

Pois temos $\det(A) = 1$. Além disso, observe que sendo $B = \{e_1 = (1,0), e_2 = (0,1)\}$ a base canônica de $\mathbb{E}^2$ temos

$$Ae_1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix} = -e_1$$

$$Ae_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -e_2$$

Isto é exatamente a reflexão para o quarto quadrante.

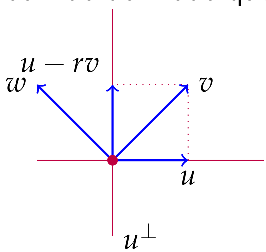
7.3 REFLEXÕES EM E^n

Seja u um vetor unitário em E^n. O conjunto

$$u^{\perp} = \{x \in \mathbb{E}^n : \langle x, u \rangle = 0\}$$

é chamado de de complemento ortogonal de u.

A projeção de um vetor v sobre $u^{\perp}$ é $v - ru$, onde $r \in \mathbb{R}$ é escolhido de modo que $v - ru$ está em $u^{\perp}$.



Assim

$$0 = \langle v - ru, u \rangle = \langle v, u \rangle - r \langle u, u \rangle = \langle v, u \rangle - r \Rightarrow r = \langle v, u \rangle$$

Podemos considerar uma reflexão de um vetor v em $u^{\perp}$

$$w = \phi(v) = v - 2ru = v - 2 \langle v, u \rangle u.$$

Exemplo 7.3.0.1. Em $\mathbb{E}^2$, consideramos o vetor u unitário escrito como

$$u = (\cos(\alpha), \sin(\alpha)).$$

Então $v = (-\sin(\alpha), \cos(\alpha))$ é um vetor unitário em $u^{\perp}$. A matriz A manda $e_1 = (1,0)$ para u e $e_2 = (0,1)$ para v precisando satisfazer

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} (1,0) = (\cos(\alpha), \sin(\alpha))$$

e

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} (0,1) = (-\sin(\alpha), \cos(\alpha))$$

assim

$$A = \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

Então a matriz que dá a reflexão em $u^{\perp}$ é

$$\begin{aligned}
\phi &= \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \\
&= \begin{pmatrix} -\cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \\
&= \begin{pmatrix} -\cos^2(\alpha) + \sin^2(\alpha) & \cos(\alpha)\sin(\alpha) + \sin(\alpha)\cos(\alpha) \\ \sin(\alpha)\cos(\alpha) + \cos(\alpha)\sin(\alpha) & -\sin^2(\alpha) + \cos^2(\alpha) \end{pmatrix} \\
&= \begin{pmatrix} -\cos(2\alpha) & \sin(2\alpha) \\ \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}.
\end{aligned}$$

A matriz A é uma rotação de um ângulo α.

8

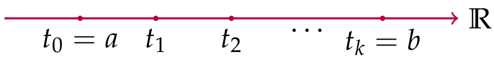
COMPRIMENTO DE ARCO E GEODÉSICAS

8.1 COMPRIMENTO DE ARCO

Definição 8.1.1 (Partição)**.** Seja $[a,b]$ um intervalo não degenerado da reta $\mathbb{R}$. Uma Partição de $[a,b]$ é um conjunto finito de pontos $P = \{t_0, t_1, \ldots, t_k\}$ tal que

$$t_0 = a < t_1 < t_2 < \ldots < t_k = b.$$

Partição de $[a,b]$:

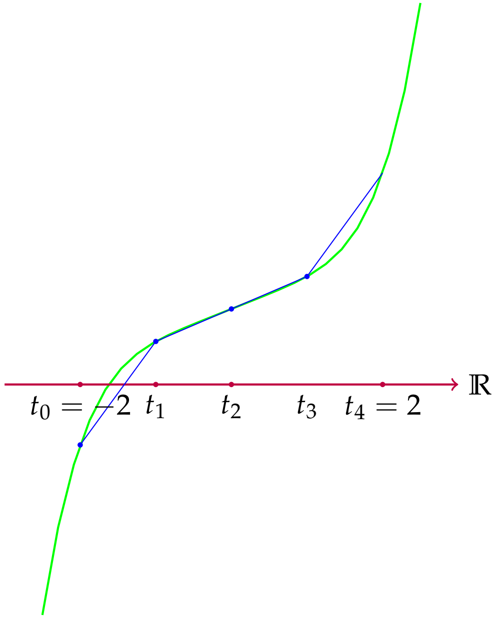


Seja $\alpha : [a,b] \to \mathbb{E}^n$ uma curva e $P = \{t_0, t_1, \ldots, t_k\}$ uma partição de $[a,b]$. Defina o número,

$$l(\alpha, P) = \sum_{i=1}^{k} \|\alpha(t_i) - \alpha(t_{i-1})\| = \sum_{i=1}^{k} d(\alpha(t_i), \alpha(t_{i-1})).$$

Então, $l(\alpha, P)$ é o comprimento da linha poligonal com vértices nos pontos $\alpha(t_i),\ i = 0, 1, \ldots, k$.

Exemplo para a curva $\alpha : (0.5x)^5 + 0.4x + 1$**:**



Definição 8.1.2 (Comprimento da curva)**.** Dada uma curva $\alpha : [a, b] \to \mathbb{E}^n$ define-se o comprimento $l(\alpha)$ de α como o menor número que $l(\alpha, P)$ não pode ultrapassar para qualquer partição P de $[a, b]$, ou seja,

$$l(\alpha) = sup\{l(\alpha, P) : \text{P é partição de } [a, b]\}.$$

Em geral, $l(\alpha)$ mede a distância total percorrida por $\alpha(t)$ quando t varia de a até b.

Não é necessariamente o comprimento do traço $\alpha([a, b])$, pois $\alpha(t)$ pode percorrer um mesmo trecho várias vezes.

Se α percorre o traço $\alpha([a, b])$ uma única vez, então de fato $l(\alpha)$ é o comprimento do traço.

8.2 GEODÉSICAS

Agora, dados dois pontos $A, B \in \mathbb{E}^n$ denote por $l(A, B)$ o conjunto de todas as curvas que ligam A e B.

Teorema 8.2.1. Dados $A, B \in \mathbb{E}^n$, tem que $d(A, B)$ é o maior número que não ultrapassa $l(\alpha)$ qualquer que seja $\alpha \in l(A, B)$, ou seja,

$$d(A, B) = inf\{l(\alpha) : \alpha \in l(A, B)\}.$$

Demonstração. Considere a curva

$$r(t) = A + t(AB),\ t \in [0, 1].$$

Dada uma partição $P = \{t_0, t_1, \ldots, t_n\}$ de $[0, 1]$, temos que

$$l(r, P) = \sum_{i=1}^{n} \|r(t_i) - r(t_{i-1})\| = \|AB\|,$$

ou seja,

$$l(r, P) = d(A, B).$$

Logo, $l(r) = d(A, B)$. Portanto, $inf\{l(\alpha) : \alpha \in l(A, B)\} \leq d(A, B)$.

Por outro lado, seja $\alpha \in l(A, B)$. Então, α tem domínio $[a, b]$ com $\alpha(a) = A$ e $\alpha(b) = B$. Dada uma partição qualquer $P = \{t_0, t_1, \ldots, t_n\}$ de $[a, b]$, temos que

$$\begin{aligned}
l(\alpha, P) &= \sum_{i=1}^{n} \|\alpha(t_i) - \alpha(t_{i-1})\| \\
&= \|\alpha(b) - \alpha(t_{n-1})\| + \|\alpha(t_{n-1}) - \alpha(t_{n-2})\| + \ldots \\
&\quad \ldots + \|\alpha(t_2) - \alpha(t_1)\| + \|\alpha(t_1) - \alpha(a)\| \\
&\geq \|\alpha(b) - \alpha(a)\| = \|AB\|.
\end{aligned}$$

Logo,

$$l(\alpha) \geq l(\alpha, P) \geq d(A, B).$$

Assim,

$$inf\{l(\alpha) : \alpha \in l(A, B)\} \geq d(A, B).$$

Portanto,

$$d(A, B) = inf\{l(\alpha) : \alpha \in l(A, B)\}.$$

□

O resultado direto deste teorema diz que no espaço euclidiano a curva de menor comprimento que liga dois pontos A e B é o segmento de reta

$$r(t) = A + t(AB),\ t \in [0, 1].$$

Definição 8.2.1 (Geodésica)**.** Uma curva $\gamma \in l(A, B)$ é chamada de **geodésica** minimizante, se o comprimento $l(\gamma)$ minimiza o comprimento das curvas em $l(A, B)$

Portanto, na Geometria Euclidiana, as **geodésicas** são as retas ou segmentos de reta.

ÍNDICE REMISSIVO