# Álgebra Linear Avançada

## Aula 1 - Estruturas Algébricas

Daniel Miranda Machado

18 de Setembro

UFABC

# Operações Binárias

# Operação Binária

**Definição**

*Seja $A$ um conjunto não vazio. Uma **operação binária** em $A$ é uma função*

$$\mu : A \times A \to A.$$

- Se $a$ e $b$ são elementos de $A$, geralmente escrevemos $ab$ em vez de $\mu(a,\ b)$.
- Expressões como $a \cdot b$, $a + b$ ou $a * b$ são usadas para enfatizar o papel da operação, especialmente quando mais de uma operação binária estiver sendo considerada.
- O par ordenado $(A, \cdot)$ significa um conjunto não vazio equipado com uma operação binária $\cdot$.

# Exemplos

1. As operações de adição, multiplicação e subtração são operações binárias em $\mathbb{Z}$, o conjunto dos números inteiros.
2. A divisão não é uma operação binária em $\mathbb{Z}$, pois, por exemplo, $1 \div 2$ e $1 \div 0$ não representam números inteiros.
3. Adição, multiplicação e exponenciação são operações binárias no conjunto $\mathbb{Z}^+$.
4. Sejam $X$ um conjunto arbitrário e $X^X$ o conjunto de todas as funções $f : X \to X$. A composição da função, $\mu(g, f) = g \circ f$, é uma operação binária em $X^X$.
5. Seja $X$ um conjunto arbitrário. O operador de interseção define uma operação binária em $A = \mathscr{P}(X)$, o conjunto das partes de $X$. Da mesma forma, o operador de união define uma operação binária em $\mathscr{P}(X)$.

Quando $A$ é um conjunto finito de $n$ elementos, uma operação binária pode ser representada por uma **tabela de Cayley**, uma lista tabular $n \times n$ de todos os produtos, com $\mu(a, b) = ab$ sendo colocado na coluna do $a$ e na linha do $b$.

**Exemplo**

$A = \{P, I\}$ um conjunto com dois elementos, que representam um inteiro genérico par $P$ e inteiro genérico ímpar $I$. A tabela de Cayley

| $+$ | $P$ | $I$ |
|---|---|---|
| $P$ | $P$ | $I$ |
| $I$ | $I$ | $P$ |

expressa o fato que uma soma de dois inteiros pares ou dois inteiros ímpares é par, enquanto a soma de um número inteiro par e ímpar é ímpar.

## Exemplo

Seja $A = \{a, b, c\}$ um conjunto com três elementos. As tabelas Cayley a seguir definem operações binárias em $A$:

| $\mu_1$ | a | b | c |
|---|---|---|---|
| a | a | c | b |
| b | b | a | c |
| c | c | b | a |

| $\mu_2$ | a | b | c |
|---|---|---|---|
| a | a | b | c |
| b | b | c | a |
| c | c | a | b |

| $\mu_3$ | a | b | c |
|---|---|---|---|
| a | a | a | a |
| b | a | b | c |
| c | a | c | b |

Temos, por exemplo, $\mu_1(b, a) = b$ (segunda linha, primeira coluna da primeira tabela), enquanto $\mu_1(a, b) = c, \mu_2(a, b) = b$ e $\mu_3(a, b) = a$ da primeira linha, segunda coluna das respectivas tabelas.

# Operação Induzida

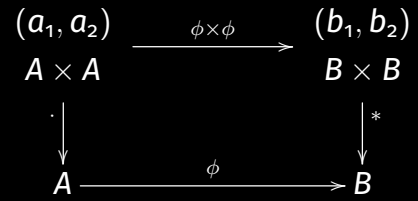
**Definição (Operação Induzida)**

*Seja* $(A, \cdot)$ *um conjunto não vazio equipado com uma operação binária e seja* $\phi : A \to B$ *uma bijeção. A operação binária em* $B$ *induzida por* $\phi$ *é definida por* $\phi(a_1) * \phi(a_2) = \phi(a_1 \cdot a_2)$ *para todos os* $a_1$ *e* $a_2$ *em* $A$.

# Diagrama Comutativos

A operação induzida pode ser visualizada em um diagrama comutativo.

Começando com um par $(a_1,\ a_2)$ em $A \times A$, existem duas maneiras de chegar a um elemento de $B$:



# Propriedades Algébricas

## Definição

- *Uma operação binária $\mu$ em um conjunto A é* ***associativa*** *se $a(bc) = (ab)c$ para todos os $a, b$ e $\mathbb{C}$ em A.*
- *Seja $(A, \mu)$ um conjunto equipado com uma operação binária. Um elemento e em A é um* ***elemento neutro*** *ou* ***identidade*** *para $\mu$ se $ea = ae = a$ para todos os a em A.*
- *Seja $(A, \mu)$ um conjunto equipado com uma operação binaria e assuma que existe uma identidade para $\mu$. Se $a \in A$, um elemento b em A é um* ***inverso*** *de a (com relação a $\mu$) se*

$$ab = ba = e.$$

**Proposição**

*Se $\mu$ for associativa e possuir uma identidade e, cada elemento a terá no máximo um inverso.*

# Estrutura algébrica

**Definição**

*Uma **estrutura algébrica** consiste em*

- *um conjunto não vazio A, dito conjunto subjacente ou domínio;*
- *uma coleção de operações em A ;*
- *um conjunto finito de identidades, conhecidas como axiomas, que essas operações devem satisfazer.*

A definição de algumas estruturas algébricas pode envolver algum conjunto auxiliar (como por exemplo os reais).

# Homomorfismos

Um **homomorfismo** é um aplicação entre duas estruturas algébricas do mesmo tipo (como dois grupos, dois anéis ou dois espaços vetoriais) que preserva a estrutura.

**Definição**

*Um **homomorfismo** é uma função $f : A \to B$ entre dois conjuntos $A, B$ equipados com a mesma estrutura, de modo que, se $\cdot$ é uma operação da estrutura (que por simplificação, supomos ser uma operação binária), então*

$$f(x \cdot y) = f(x) \cdot f(y)$$

*para $x, y \in A$. Dizemos nesse caso que $f$ preserva a operação ou que $f$ é compatível com a operação.*

Um homomorfismo deve também preservar as constantes.

Em particular, quando um elemento identidade é exigido num tipo de estrutura, o elemento identidade da primeira estrutura deve ser mapeado para o elemento identidade correspondente da segunda estrutura.

# Grupos

**Definição (Grupo)**

*Um* ***grupo*** *$G$ é um conjunto não vazio com uma operação binária que satisfaz os axiomas a seguir:*

- **G1** *associatividade - para todos os $g, h, j \in G, g \cdot (h \cdot j) = (g\ h)j$;*
- **G2** *existe um elemento único $e \in G$ com a propriedade: para todo $g \in G$,*

$$ge = eg = g,$$

*$e$ é denominado* ***elemento neutro*** *ou* ***identidade***

- **G3** *para cada $g \in G$, existe um único elemento $j \in G$ com a propriedade:*

$$gj = jg = e,$$

*esse elemento geralmente é denotado por $g^{-1}$.*

É importante observar que um grupo é na realidade um par $(G,\ (g,h) \to g \cdot h)$ consistindo em um

- conjunto não vazio
- $G$ juntamente com uma função de $G \times G \to G$ e satisfazendo os axiomas G1-G4.

Agumas vezes (por exemplo num espaço vetorial), usamos a notação aditiva escrevendo $+$ e 0 para $e$ e $-g$ para $g^{-1}$

## Exemplos (de Grupos)

1. os números inteiros $\mathbb{Z}$ com adição,
2. os números racionais positivos com multiplicação,
3. os números complexos diferentes de zero com multiplicação,
4. os números inteiros que estão entre 0 e $n-1$ inclusive, com adição módulo $n$. Esse grupo geralmente é indicado por $\mathbb{Z}/n\mathbb{Z}$.
5. O conjunto $\{0\}$ com operação $0+0=0$ é um grupo abeliano.
6. o conjunto de permutações em um conjunto finito $X$, com composição como operação.
7. O conjunto das matrizes invertíveis com a operação de multiplicação de matrizes.

**Proposição**

*G seja um grupo, então temos*

1. *cancelamento - para todos* $g, h, j \in G$, *se* $gh = gj$, *ou* $hg = jg$, *então* $h = j$
2. *para todos* $g, h \in G, (gh)^{-1} = h^{-1}g^{-1}$, *e* $(g^{-1})^{-1} = g$
3. *A equação* $gx = j$ *possui uma única solução* $x = g^{-1}j$

# Grupos de Permutações

# Notação

**Notação**

Usaremos a notação $[1,\ n]$ para representar o conjunto $\{1, 2, \ldots, n\}$.

$$[1,\ n] = \{1, 2, \ldots, n\}$$

**Definição**

*O* ***grupo de permutações*** $S_n$ *consiste em todas as bijeções*

$$\sigma : [1,\ n] \to [1,\ n]$$

*onde* $[1, n] = \{1, \ldots, n\}$*, com a operação de composição*

$$\sigma_1 \circ \sigma_2(k) = \sigma_1(\sigma_2(k)) \text{ para } 1 \leq k \leq n$$

*como a operação do grupo. O elemento de identidade e é o mapa de identidade* $e = \mathrm{I}_{[1,n]}$ *de modo que* $e(k) = k$*, para todos os* $k \in [1,\ n]$*.*

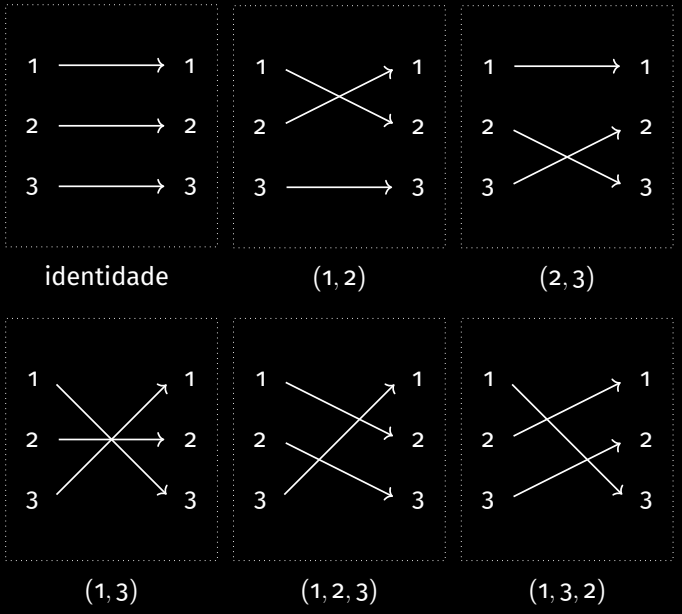



**Figura 1:** Grupo de permutação de três elementos.

As permutações mais simples são os $k$-ciclos.

**Definição**

*Uma lista ordenada* $(i_1, \ldots, i_k)$ *de k índices distintos em* $[1, n] = \{1, \ldots, n\}$ *determina um k-**ciclo** em* $S_n$*, a permutação que atua da seguinte maneira no conjunto* $X = [1, n]$.

$$\sigma \text{ mapeia } \begin{cases} i_1 \to i_2 \to \ldots \to i_k \to i_1 \text{ para os elementos na lista} \\ j \to j \text{ para todos os } j \text{ que não estão na lista } i_1, \ldots, i_k\} \end{cases}$$

- O 1-ciclo $(k)$ é apenas o mapa de identidade $\mathrm{I}_X$.
- O suporte de um $k$-ciclo é o conjunto de entradas $\mathrm{supp}(\sigma) = \{i_1, \ldots, i_k\}$.
- O suporte de um 1-ciclo $(k)$ é o conjunto de um ponto $\{k\}$.

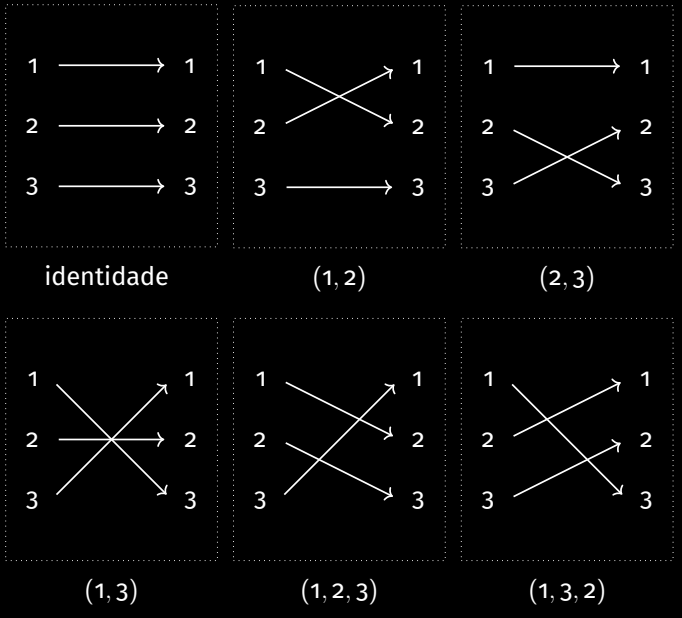



**Figura 2:** Grupo de permutação de três elementos.

A ordem das entradas no símbolo $\sigma = (i_1,\ \ldots,\ i_k)$ é importante, mas a notação do ciclo é ambígua: todos os $k$ símbolos diferentes

$$(i_1,\ \ldots,\ i_k) = (i_2,\ \ldots,\ i_k,\ i_1) = (i_3,\ \ldots,\ i_k,\ i_1,\ i_2) = \ldots = (i_k,\ i_1,\ \ldots,\ i_{k-1})$$

obtido por "mudanças cíclicas" das entradas da lista em $\sigma$ descrevem a mesma permutação em $S_n$.

Assim, $(1,\ 2,\ 3) = (2,3,1) = (3,1,2) \neq (1,3,2)$ porque $(1,\ 2,\ 3)$ envia $1 \to 2$ enquanto $(1,\ 3,\ 2)$ envia $1 \to 3$.

Uma maneira (complicada) de descrever os elementos gerais $\sigma \in S_n$ emprega uma matriz de dados para mostrar para onde cada $k \in [1,\ n]$ é mapeado:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & n \\ j_1 & j_2 & j_3 & j_n \end{pmatrix}$$

Uma notação mais eficiente é proporcionada pelo fato de que toda permutação $\sigma$ pode ser decomposta de maneira única como um produto de ciclos com suportes disjuntos, o que significa que os fatores comutam.

O produto de dois ciclos $\sigma\tau = \sigma \circ \tau$ é uma composição de operadores; portanto, a ação de $\sigma\tau = \sigma \circ \tau$ em um elemento $k \in [1,\ n]$ é avaliado inserindo $k$ no produto a partir da direita abaixo.

**Exemplo**

Tomando $\sigma = (1, 2)$ e $\tau = (1, 2, 3)$ em $S_5$, temos

$$\sigma\tau \ \ k \to (1,2)(1,2,3) \cdot k = (1,2) \cdot ((1,2,3) \cdot k) = ((1,2)(1,2,3) \cdot k)$$

Para determinarmos a composta, rastreamos o que acontece com cada $k$:

$$
\begin{array}{ccc}
 & (1,2)\,(1,2,3) & \\
1 & \to 2 \to 1 & 1 \to 1 \\
2 & \to 3 \to 3 & 2 \to 3 \\
3 & \to 1 \to 2 & 3 \to 2 \\
4 & \to 4 \to 4 & 4 \to 4 \\
5 & \to 5 \to 5 & 5 \to 5
\end{array}
$$

Assim, o produto $(1,\ 2)(1,2,3)$ é igual a $(2,\ 3) = (1)(2,3)(4)(5)$, quando incluímos 1-ciclos redundantes.

Por outro lado, $(1,\ 2,\ 3)(1,2) = (1,3)$, o que mostra que os ciclos não precisam ser comutar se seus suportes se sobrepuserem. Como outro exemplo, temos

$$(1,2,3,4)^2 = (1,3)(2,4)$$

que mostra que uma potência $\sigma^k$ de um ciclo não precisa ser um ciclo, embora seja um produto de ciclos disjuntos.

**Teorema (Decomposição em Ciclos de Permutações)**

*Todo $\sigma \in S_n$ que não é a identidade é um produto de ciclos disjuntos. Essa decomposição é única (a menos da ordem dos fatores da decomposição) se incluirmos os 1 ciclos necessários para contabilizar todos os índices $k \in [1,\ n]$.*

# Idéia da Demonstração

# Demonstração

Seja $\sigma \in S_n$ com $\sigma$ não sendo a identidade.

Seja o primeiro menor elemento tal que $\sigma(a_1) \neq a_1$. Então, para algum $a_2, a_3, \ldots, a_k \in \{1, 2, \ldots, n\}$ temos que

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_{k-1}) = a_k.$$

Seja $k$ tal que $\sigma(a_k) = a_i$ para algum $i \in \{1, 2, \ldots, k\}$. Se $\sigma(a_k) = a_2$, temos uma contradição, pois $\sigma(a_1) = \sigma(a_2)$ e logo $\sigma$ não seria injetiva (e todas as permutações são bijetivas por definição).

Se $\sigma(a_k) = a_3$ ou $\sigma(a_k) = a_4$ , ou $\sigma(a_k) = a_k$, então o mesmo tipo de contradição surge. Portanto, $\sigma(a_k) = a_1$ e, portanto:

Portanto $(a_1 a_2 \dots a_k)$ é um ciclo.

Agora seja $b_1 \in \{1, 2, \dots, n\}$ o menor elemento tal que $\sigma(b_1) \neq b_1$ e tal que $b_1 \notin \{a_1, a_2, \dots, a_k\}$. Repetimos o processo descrito acima para obter um ciclo $(b_1 b_2 \dots b_j)$ onde $a_s \neq b_t$ para todo $s \in \{1, 2, \dots, k\}$ e para todo $t \in \{1, 2, \dots, j\}$.

Visto que $\{1, 2, \dots, n\}$ é um conjunto finito, este processo deve eventualmente terminar decompondo $\sigma$ como um produto finito de ciclos disjuntos.

Observaremos a seguir que os 2 ciclos $(i,\ j)$ geram todo o grupo $S_n$ no sentido de que todo $\sigma \in S_n$ pode ser escrito como um produto $\sigma = \tau_1 \cdot \ldots \cdot \tau_r$ de dois ciclos.

No entanto, esses fatores não são necessariamente disjuntos e não precisam comutar, e essas decomposições estão longe de serem únicas, pois temos, por exemplo,

$$e = (1,2)^2 = (1,2)^4 = (1,3)^2 \text{ etc.}$$

# Paridade de uma permutação

No entanto, um aspecto importante de tais fatorações é único, a saber, sua paridade

$$\text{sinal}(\sigma) = (-1)^r$$

onde

$$r = \#\left[2 - \text{ ciclos na fatoração de } \sigma = (\tau_1, \ \ldots, \ \tau_r)\right].$$

Isso significa que os elementos $\sigma \in S_n$ se enquadram em duas classes disjuntas: **permutações pares** que podem ser escritas como um produto de um número par de 2 ciclos e **permutações ímpares.** Não é óbvio que as decomposições de em 2-ciclos de uma dada permutação tenham a mesma paridade. Provamos isso a seguir e mostramos como calcular $\text{sinal}(\sigma)$ de maneira eficaz.

Primeiro observamos que sempre existe uma decomposição de uma permutação como produto de 2 ciclos. Pelo Teorema ??, basta mostrar que qualquer ciclo $k$ pode ser decomposto.

Para 1 ciclo, isso é óbvio, já que $(k) = e = (1,2) \cdot (1,2)$. Quando $k > 1$ é fácil verificar se

$$(1, 2, \ldots, k) = (1, k) \cdot \ldots \cdot (1,3)(1,2) \quad \text{(com } k-1 \text{ fatores)}$$

Depois de verificarmos que a paridade está bem definida, isso nos diz como reconhecer a paridade de qualquer ciclo $k$

$$\text{sinal}(i_1, i_2, \ldots, i_k) = (-1)^{k-1} \quad \text{para todos os } k > 0$$

**Teorema (da Paridade)**

*Todas as decomposições* $\sigma = \tau_1 \cdot \ldots \cdot \tau_r$ *de uma permutação como um produto de* 2 *ciclos têm a mesma paridade* $\text{sinal}(\sigma) = (-1)^r$

O grupo $S_n$ atua no espaço dos polinômios $\mathbb{K}[\mathbf{x}] = \mathbb{K}[x_1, \ldots, x_n]$ permutando as variáveis

$$(\sigma \cdot f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

Por exemplo $(1,2,3) \cdot f(x_1, x_2, x_3, x_4, x_5) = f(x_2, x_3, x_1, x_4, x_5)$.

Sejam $x_1, \ldots, x_n$ $n$ variáveis e considere

$$\Delta = \prod_{1 \leq i < j \leq n} (x_j - x_i).$$

Por exemplo, para $n = 4$, teríamos

$$\Delta = (x_2 - x_1)(x_3 - x_1)(x_4 - x_1)(x_3 - x_2)(x_4 - x_2)(x_4 - x_3).$$

Dada uma permutação $\sigma \in S_n$, defina uma função $f_\sigma : \{\Delta, -\Delta\} \to \{\Delta, -\Delta\}$ por

$$f_\sigma(\Delta) = \prod_{1 \le i < j \le n} (x_{\sigma(j)} - x_{\sigma(i)}),$$

e $f_\sigma(-\Delta) = -f_\sigma\Delta$.

Observe que, como $\sigma$ é uma permutação, $f_\sigma(\Delta) = \Delta$ ou $f_\sigma(\Delta) = -\Delta$. Além disso, se $\sigma, \rho$ são duas permutações, então $f_\sigma \circ f_\rho = f_{\sigma\rho}$, como é fácil de verificar.

- Lembrando que
$$\Delta = \prod_{1 \leq i < j \leq n} (x_j - x_i).$$
- Agora, vamos considerar o que uma transposição $\tau = (a, b)$ faz com $\Delta$.
- Sem perda de generalidade, assumimos $a < b$.
- Os fatores $(x_j - x_i)$ onde nem $i$ nem $j$ são iguais a $a$ ou $b$ permanecem inalterados.

- Lembrando que

$$\Delta = \prod_{1 \le i < j \le n} (x_j - x_i).$$

- Para os pares com exatamente um índice em $\{a, b\}$, temos duas classes:
  - aquelas em que o outro índice está entre $a$ e $b$,
  - aquelas em que o outro índice não está entre $a$ e $b$.

- Lembrando que
$$\Delta = \prod_{1 \le i < j \le n} (x_j - x_i).$$
- Para os pares com exatamente um índice em $\{a, b\}$, temos duas classes:
  - aquelas em que o outro índice está entre $a$ e $b$,
  - aquelas em que o outro índice não está entre $a$ e $b$.

---

- Se o outro índice estiver entre $a$ e $b$, então $x_j - x_a$ é enviado para $-(x_b - x_j)$ e $x_b - x_j$ é enviado para $-(x_j - x_a)$; as duas mudanças de sinal se cancelam.
- Se o outro índice for maior que $b$, então $x_j - x_a$ e $x_j - x_b$ são trocados, sem mudanças de sinal.
- Se o outro índice for menor que $a$, então $x_a - x_i$ e $x_b - x_i$ são trocados, sem mudanças de sinal.

Finalmente, o fator $x_b - x_a$ é enviado para $-(x_b - x_a)$.

Em resumo, se $\tau$ é uma transposição, então $f_\tau(\Delta) = -\Delta, f_\tau(-\Delta) = \Delta$.

Agora pegue uma permutação arbitrária $\sigma$ e expresse-a como um produto de transposições de duas maneiras diferentes:

$$\sigma = \tau_1 \cdots \tau_r = \rho_1 \cdots \rho_s.$$

Então

$$f_\sigma(\Delta) = f_{\tau_1 \cdots \tau_r}(\Delta) = f_{\tau_1} \circ \cdots \circ f_{\tau_r}(\Delta) = (-1)^r \Delta$$

e

$$f_\sigma(\Delta) = f_{\rho_1 \cdots \rho_s}(\Delta) = f_{\rho_1} \circ \cdots \circ f_{\rho_s}(\Delta) = (-1)^s \Delta.$$

Portanto, $(-1)^r \Delta = (-1)^s \Delta$, então $r$ e $s$ têm a mesma paridade.

**Proposição**

*A aplicação de paridade* $\text{sinal} : S_n \to \{\pm 1\}$, *definida por* $\text{sinal}(\sigma) = (-1)^r$ *se* $\sigma$ *puder ser decomposto como um produto de r dois ciclos, possui as seguintes propriedades algébricas*

a. $\text{sinal}(e) = +1$;

b. $\text{sinal}(\sigma\tau) = \text{sinal}(\sigma) \cdot \text{sinal}(\tau)$;

c. $\text{sinal}(\sigma^{-1}) = (\text{sinal}(\sigma))^{-1} = \text{sinal}(\sigma)$( *pois* $\text{sinal} = \pm 1$).

# Demonstração

Exercício.

# Corpos

Um corpo é um conjunto munido de duas operações: adição e multiplicação e tal que essas operações se comportam de maneira similar as operações correspondentes nos números racionais, reais e complexos.

# Corpos

Um conjunto não vazio $\mathbb{K}$ munido de duas funções $(x, y) \to x + y$ e $(x, y) \to x \cdot y$ de $\mathbb{K} \times \mathbb{K}$ para $\mathbb{K}$ é dito um **corpo** se os nove axiomas a seguir forem atendidos:

- K1 $x + y = y + x$ para todos os $x, y \in \mathbb{K}$.
- K2 $x + (y + z) = (x + y) + z$ para todos os $x, y, z \in \mathbb{K}$.
- K3 Existe um único elemento $0 \in \mathbb{K}$ tal que $x + 0 = x$ para todos os $x \in \mathbb{K}$.
- K4 Para cada $x \in \mathbb{K}$, existe um único elemento $-x \in \mathbb{K}$, de modo que $x + (-x) = 0$.
- K5 $x + y = y + x$ para todos os $x, y \in \mathbb{K}$.
- K6 $x\,(yz) = (xy)z$ para todos os $x, y, z \in \mathbb{K}$

1. Existe um único elemento $1 \neq 0$ em $\mathbb{K}$ tal que $1x = x$ para todos os $x \in \mathbb{K}$.
2. Para cada $x \neq 0$ em $\mathbb{K}$, existe um único $y \in \mathbb{K}$, tal que $xy = 1$.
3. $x(y + z) = xy + xz$ para todos os $x, y, z \in \mathbb{K}$.

Estritamente falando, um corpo é um tripla ordenada $(\mathbb{K}, (x, y) \to x + y, (x, y) \to xy)$ satisfazendo os axiomas K1-K9 acima.

O mapa de $\mathbb{K} \times \mathbb{K} \to \mathbb{K}$ fornecido por $(x, y) \to x + y$ é denominado **adição**, e o mapa $(x, y) \to xy$ é denominado **multiplicação**.

Ao se referir a algum corpo $(\mathbb{K}, x, y) \to x + y, (x, y) \to xy)$, as referências à adição e multiplicação são eliminadas da notação e a letra $\mathbb{K}$ é usada para denotar o conjunto e os dois mapas que satisfazem os axiomas K1-K9.

# Exemplos de Corpos

**Exemplo**

Sejam $\mathbb{Q}$ o conjunto de números racionais, $\mathbb{R}$, o conjunto de números reais e $\mathbb{C}$, o conjunto de números complexos. Com a adição e multiplicação usual, $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são todos corpos com $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

# Exemplos de Corpos

**Exemplo**

Seja $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Dados $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ e $c + d\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$, definimos a soma e o produto, respectivamente, como:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) \triangleq (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \quad (1)$$

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) \triangleq (ac, 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2}). \quad (2)$$

Então $\mathbb{Q}(\sqrt{2})$ é um corpo.

Os corpos dos Exemplos ?? e ?? são todos infinitos.

**Exemplo**

Seja $\mathbb{Z}$ conjunto de números inteiros com a adição e a multiplicação usual. Seja $p$ um primo positivo em $\mathbb{Z}$ e defina $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$. Então $\mathbb{Z}_p$ torna-se corpo (finito) se definimos a adição $\oplus$ e a multiplicação módulo $p$.

| $+$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{0}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{3}$ | $\overline{3}$ | $\overline{4}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
| $\overline{4}$ | $\overline{4}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |

| $\cdot$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{4}$ | $\overline{1}$ | $\overline{3}$ |
| $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{1}$ | $\overline{4}$ | $\overline{2}$ |
| $\overline{4}$ | $\overline{0}$ | $\overline{4}$ | $\overline{3}$ | $\overline{2}$ | $\overline{1}$ |

**Tabela 1:** Tabelas de Cayley da adição e multiplicação em $\mathbb{Z}_5$

O leitor pode verificar facilmente que $(\mathbb{K}_p, \oplus, \cdot)$ satisfaz os axiomas K1-K9. Portanto, $\mathbb{K}_p$ é um corpo finito de cardinalidade $p$.

**Exemplo**

o conjunto das matrizes $2 \times 2$ com entradas em números reais, $M(2, \mathbb{R})$, com adição e multiplicação de matrizes não é um corpo porque a multiplicação não é comutativa, não há divisão e existem divisores de 0.

**Proposição**

*Seja $\mathbb{K}$ um corpo.*

1. $\mathbb{K}$ *possui pelo menos dois elementos* $0$ *e* $1$ *e* $0 \neq 1$.
2. *Para todos os* $a \in \mathbb{K}$, $a0 = 0a = 0$.
3. *Para todos os* $a, b \in \mathbb{K}$, *se* $ab = 0$, *então* $a = 0$ *ou* $b = 0$, *dizemos que* $\mathbb{K}$ *não tem* ***divisores de zero***.

Se $\mathbb{F}$ for um corpo e $\mathbb{F} \subset \mathbb{K}$ então $\mathbb{F}$ é dito **subcorpo** de e nesse caso $\mathbb{K}$ será dito extensão de $\mathbb{F}$. Por exemplo, $\mathbb{R}$ é um subcorpo de $\mathbb{C}$ e uma extensão de corpo dos racionais $\mathbb{Q}$.

Se $a \in \mathbb{K}$ e $a + a + \cdots + a = 0$ então $a$ pode, ou não, ser igual a zero; por exemplo, se $\mathbb{K} = \mathbb{Q}$, então $a = 0$, mas se $\mathbb{K} = \mathbb{F}_5$, $5 = 1 + 1 + 1 + 1 + 1 = 0$ e claramente $1 \neq 0$.

**Definição**

*A característica de um corpo $\mathbb{K}$ é o menor n positivo tal que*

$$\underbrace{1 + \cdots + 1}_{n \text{ termos}} = 0$$

*se tal n existir; caso contrário diremos que o corpo tem característica zero.*

**Exemplos**

Os corpos $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ têm a característica zero e $\mathbb{F}_p$ têm a característica $p$

# Comentários Finais.