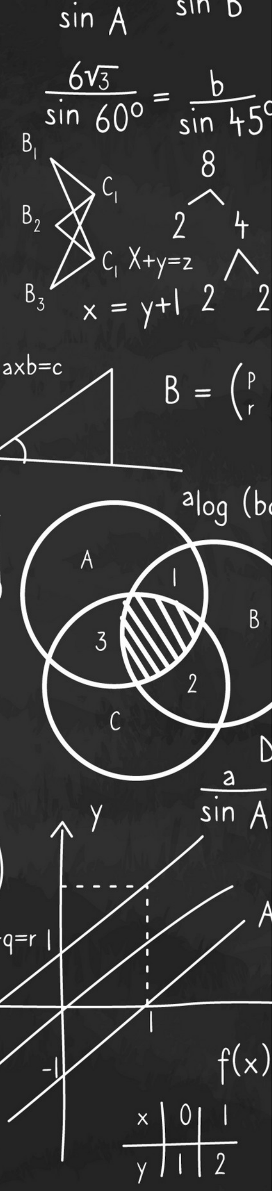


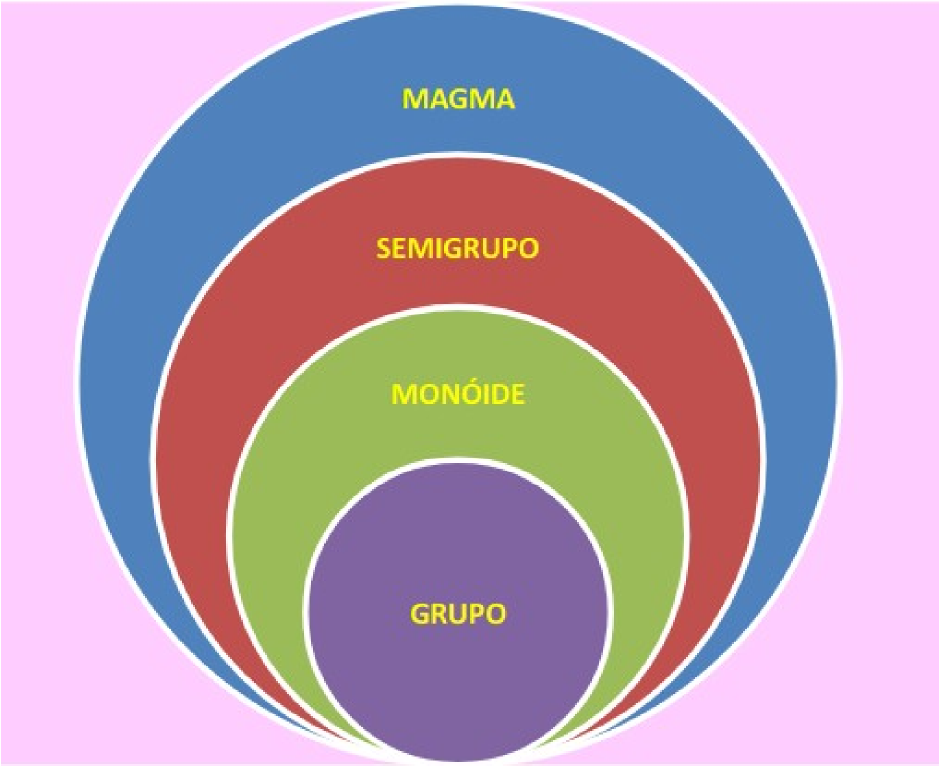
MATEMÁTICA DISCRETA 2

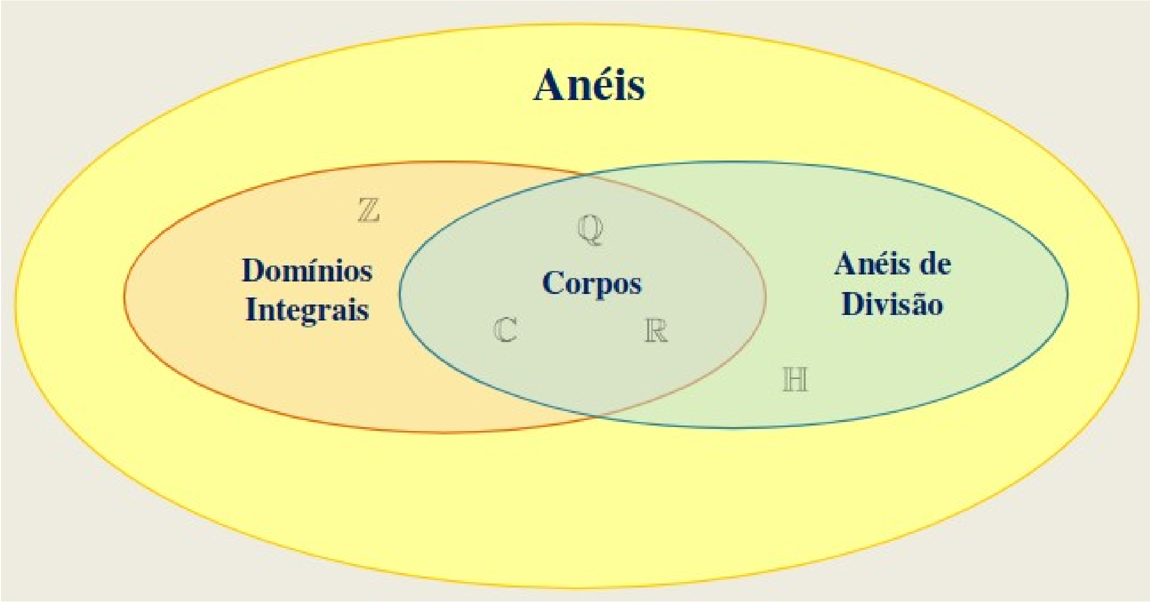
Aula 19
Estruturas Algébricas
Grupos

Cristiane Loesch

Brasília
2025

Estruturas Algébricas





Fonte: Paiva, C. R. (2010)

Estruturas Algébricas

ÁLGEBRA :

- estudo das operações, regras de cálculo e procedimentos para a solução de equações.

EXPANSÃO DO DOMÍNIO DA ÁLGEBRA:

- é possível estudar propriedades de qualquer operação algébrica sem especificar a natureza dos objetos sobre os quais a operação atua, nem descrever como o resultado da operação deve ser calculado.

- postula-se um determinado conjunto de propriedades algébricas básicas que a operação deve verificar.

Exemplo: comutatividade e associatividade

ÁLGEBRA AXIOMÁTICA:

- definição de estruturas algébricas abstratas
  - preocupação em relação a conjuntos nos quais pode-se operar algebricamente seus elementos, combinando dois deles afim de definir um terceiro com características dos dois primeiros
  - regras determinam natureza do conjuntos
  - incluem operações aritméticas não limitadas a si, mas que ditam as propriedades algébricas de cada conjunto

ESTRUTURA ALGÉBRICA ABSTRATA:

- *é formada por um conjunto não vazio X, dito suporte da estrutura, e uma operação binária em X, ou seja, uma função .*

$$\mu : X \times X \rightarrow X$$

- *diferentes conjuntos de suposições, ou axiomas, exigidos a esta operação, conduzem à definição de diferentes estruturas algébricas abstratas*

CONVENÇÕES:

Se $\mu : X \times X \to X$ for uma operação binária em X, é comum escolher um símbolo:

$+$ para representar $x + y$

ou

$*$ para representar $x * y$

em vez de $\mu(x, y)$.

→ escreve-se, frequentemente, xy ao invés de $\mu(x, y)$.

CONVENÇÕES:

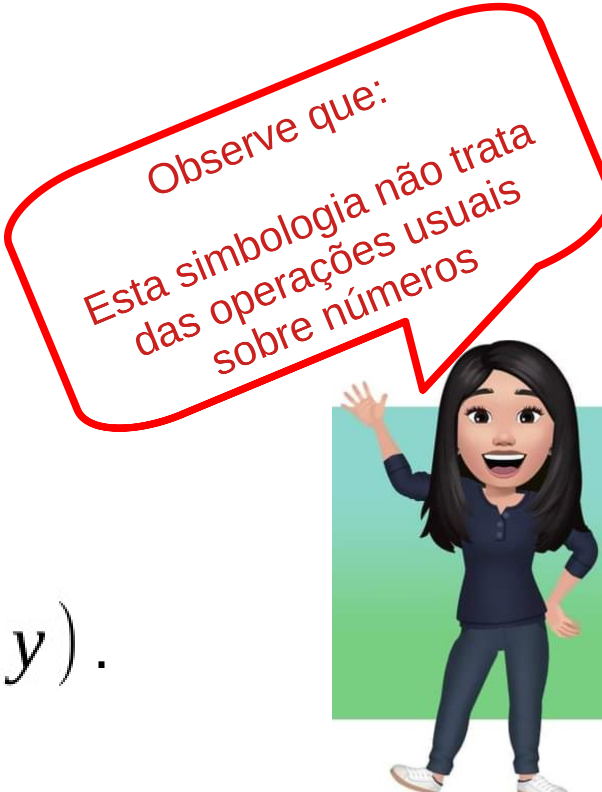
Se $\mu: X \times X \to X$ for uma operação binária em X, é comum escolher um símbolo:

$+$ para representar $x + y$

ou

$*$ para representar $x * y$

em vez de $\mu(x, y)$.



$\rightarrow$ escreve-se, frequentemente, xy ao invés de $\mu(x, y)$.

$+$ → usado, por convenção, para designar operações comutativas

notação aditiva

$$\mu(x, y)=\mu(y, x)$$

$*$ → usado, por convenção, para designar operações comutativas

notação multiplicativa

$$x*(y*z)=\mu(x,\mu(y,z))$$

é diferente de

$$(x*y)*z=\mu(\mu(x,y),z)$$

ELEMENTOS DE ÁLGEBRA

Notações:

$\mathbb{Z}$ → conjunto dos números inteiros

$\mathbb{Q}$ → conjunto dos números racionais

$\mathbb{R}$ → conjunto dos números reais

$\mathbb{C}$ → conjunto dos números complexos

$\mathbb{R}-\mathbb{Q}$ → conjunto dos números irracionais

$A \times B$ → produto cartesiano do conjunto A pelo conjunto B

$$A \times B = \{(a,b), a \in A, b \in B\}$$

Seja A um conjunto, uma operação (binária) de A é uma função

$$*: A \times A \to A,$$

assim uma operação em A associa a cada par de elementos de A um elemento de A.

Seja A um conjunto, uma operação (binária) de A é uma função

$$*: A \times A \to A,$$

assim uma operação em A associa a cada par de elementos de A um elemento de A.

Exemplo:

Em $\mathbb{Z}$ estão definidas duas operações

- ***i) adição*** $+: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$

  ii) multiplicação $\cdot: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$

associam a cada par (a, b) de números inteiros, respectivamente, o número $a+b \in Z$ ou $a \cdot b \in Z$

Em particular estas duas operações nos apresentam as seguintes propriedades:

1) $a+b=b+a$ comutativa

2) $(a+b)+c=a+(b+c)$, $\forall a,b,c\in Z$ associativa

3) $\exists 0\in Z$ tal que $a+0=a$ elemento neutro

4) dado $a\in Z, \exists a\in Z$, tal que $a+(-a)=0$

5) $a*(b+c)=a*b+a*c$ distributiva

6) $(a+b)\cdot c=a\cdot c+b\cdot c$

7) $a\cdot(b\cdot c)=(a\cdot b)\cdot b$ associativa da multiplicação

ESTRUTURA ALGÉBRICA

É todo par composto por um conjunto não vazio e uma operação interna $*$ em A

$$\langle\ A, *\ \rangle \quad \text{ou} \quad (\ A, *\ )$$

em que $*$ é uma operação binária no conjunto A.

Notações:

$+$ → notação aditiva => representa $x + y$

$*$ → notação multiplicativa => representa $x * y$

Propriedades:

1) Comutativa

$$x * y = y * x \quad , \quad \forall x, y \in A$$

Propriedades:

1) Comutativa

$$x * y = y * x \quad , \quad \forall x, y \in A$$

2) Associativa

$$(x * y) * z = x * (y * z) \quad , \quad \forall x, y, z \in A$$

Propriedades:

1) Comutativa

$$x * y = y * x \quad , \quad \forall x, y \in A$$

2) Associativa

$$(x * y) * z = x * (y * z) \quad , \quad \forall x, y, z \in A$$

3) Elemento Neutro

$$x * e = e * x = x \quad , \quad \forall x \in A$$

- designa-se, comumente, elemento neutro por:
- “zero”,”0” em notação aditiva
- “um”, “1”, “I” (identidade) em notação multiplicativa

Propriedades:

1) Comutativa

$$x * y = y * x \quad , \quad \forall\, x , y \in A$$

2) Associativa

$$(x * y) * z = x * (y * z) \quad , \quad \forall\, x , y , z \in A$$

3) Elemento Neutro

$$x * e = e * x = x \quad , \quad \forall\, x \in A$$

4) Elemento invertível ou simetrizável

$$x * y = y * x = e \quad , \quad \forall\, x , y \in A$$

Propriedades:

4) Elemento invertível ou simetrizável

$$x * y = y * x = e \quad , \quad \forall x, y \in A$$

- y é o inverso de x
- na notação aditiva inversos dizem-se simétricos
- se, tem-se apenas

$$x * y = e$$

- Proposição:
  Seja $*$ uma operação associativa em A se xϵA tem inverso à direita y, e inverso à esquerda z, logo y = z e x é invertível.

$$x * y = e \longrightarrow z * (x * y) = z \longrightarrow (z * x) * y = z \longrightarrow e * y = z \longrightarrow y = z$$

Propriedades:

4) Elemento invertível ou simetrizável

$$x * y = y * x = e \quad , \quad \forall x, y \in A$$

- y é o inverso de x
- na notação aditiva inversos dizem-se simétricos
- se, tem-se apenas

$$x * y = e$$

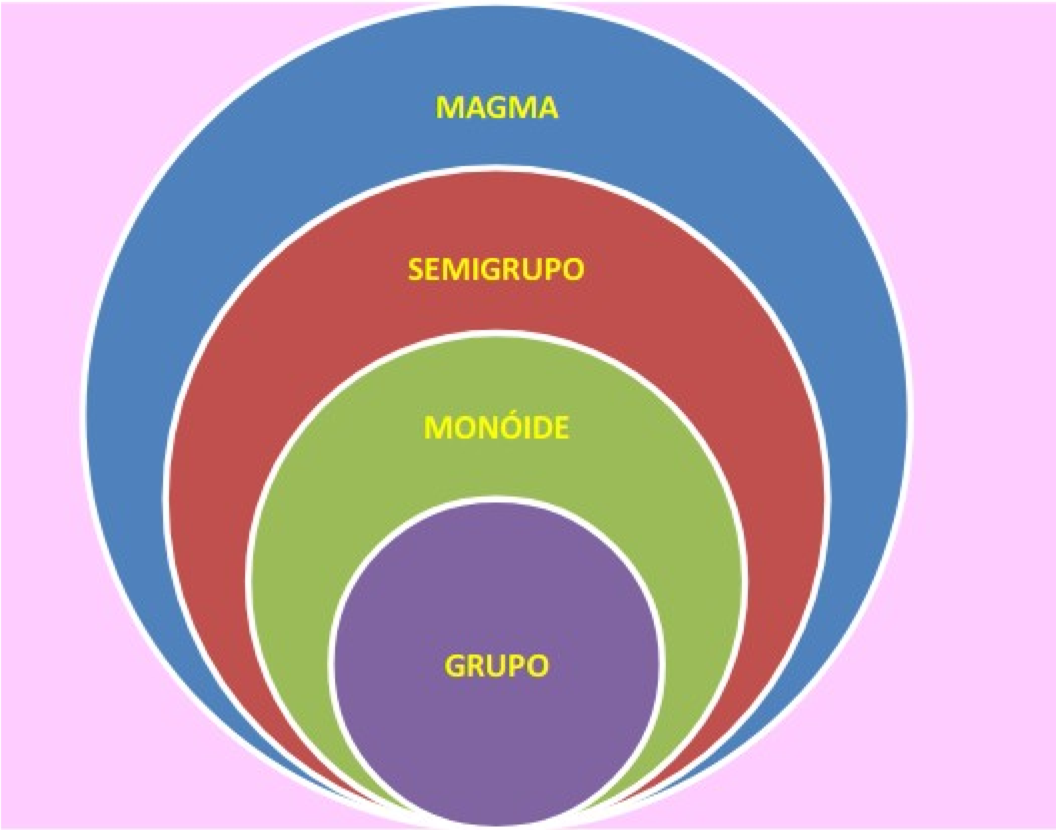
- Proposição:
  Seja $*$ uma operação associativa em A se x∊A tem inverso à direita y, e inverso à esquerda z, logo y = z e x é invertível.

$$x * y = e \longrightarrow z * (x * y) = z \longrightarrow (z * x) * y = z \longrightarrow e * y = z \longrightarrow y = z$$

y é inverso de x, se e somente se for inverso à direita e à esquerda

CLASSIFICAÇÃO:

- Grupóide ou Magma
- Semigrupo
- Monóide
- Grupo
- Anel
- Corpo



Fonte: Paiva, C. R. (2010)

Dado um conjunto não-vazio *A* dotado de uma operação binária $A \times A \to A$ denotada por $(A, *)$ que satisfaz a(s) propriedade(s):

- do fechamento → Grupóide
- do fechamento e associativa → Semi-grupo
- do fechamento, associativa e elemento neutro → Monóide
- do fechamento, associativa, elemento neutro e elemento invertível → Grupo

Obs: estruturas algébricas que satisfazem a propriedade comutativa recebem a característica "extra" de Abeliano.

- Exemplo: Monóide Abeliano

Grupo

Conjunto não-vazio *G* dotado de uma operação binária $G \times G \rightarrow G$ denotada por $(G, *)$ e uma operação unária $G \rightarrow G$ denotada por $^{-1}$ (inversa) que satisfaz as propriedades:

i) fechamento

ii) associativa $a, b, c \in G \rightarrow (a * b) * c = a * (b * c)$

iii) elemento neutro $a, e \in G \rightarrow a * e = e * a = a$

iv) elemento invertível ou simétrico $a, b \in G \rightarrow a * b = b * a = e \rightarrow b = a^{-1}$

Grupo abeliano

→ grupo que satisfaz também a propriedade comutativa

→ Ou seja, um monóide $(G, *)$ diz-se um **grupo** se, e somente se,todos seus elementos forem invertíveis.

EXERCÍCIO

Seja $\langle G, * \rangle$ um grupo com $x, y \in G$. Prove que $(x * y)' = x' * y'$

CARACTERÍSTICAS DE GRUPOS

- Grupo Abeliano ou Comutativo

  Quando o Grupo satisfaz a propriedade comutativa da operação binária em questão.

- Grupo Aditivo

  Quando a operação binária considerada sobre ele é a adição. Nesses grupos, denota-se a operação pelo sinal “+” de adição.

- Grupo Multiplicativo

  Quando a operação binária considerada sobre ele é a multiplicação. Nesses grupos, denota-se a operação pelo sinal “·” de multiplicação ou apenas por justaposição.

PROPRIEDADES DE GRUPOS

1. $e \in G$, e é único (e = elemento neutro)

2. $\forall a \in G$, $\exists$ um único inverso

3. $\forall a, b \in G \Rightarrow (a * b)^{-1} = b^{-1} * a^{-1}$

4. $\forall a \in G \Rightarrow (a^{-1})^{-1} = a$

5. $\forall a, b, c \in G: a * b = a * c \Rightarrow b = c$ (LEI DO CANCELAMENTO)

Propriedade do Cancelamento

$$\forall a, b, c \in G, \quad se \quad a*b=a*c \quad ou \quad b*a=c*a \;\rightarrow\; b=c$$

Propriedade do Cancelamento

$$\forall a, b, c \in G, \quad se \quad a*b=a*c \quad ou \quad b*a=c*a \;\rightarrow\; b=c$$

EXEMPLO: $G=\langle GL_{2,} \cdot \ \rangle \longrightarrow A \cdot B = C \cdot B$ **?**

$$A=\begin{pmatrix} 4 & 1 \\ 5 & 2 \end{pmatrix} \qquad B=\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad C=\begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}$$

Propriedade do Cancelamento

$$\forall a, b, c \in G, \quad se \quad a*b=a*c \quad ou \quad b*a=c*a \;\rightarrow\; b=c$$

EXEMPLO: $G=\langle GL_{2,} \cdot \ \rangle \longrightarrow A \cdot B = C \cdot B$ **?**

$$A=\begin{pmatrix} 4 & 1 \\ 5 & 2 \end{pmatrix} \qquad B=\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad C=\begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}$$

$$A \cdot B = C \cdot B = \begin{pmatrix} 4 & 1 \\ 5 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

Propriedade do Cancelamento

$$\forall a, b, c \in G, \quad se \quad a*b=a*c \quad ou \quad b*a=c*a \rightarrow b=c$$

EXEMPLO: $G=\langle GL_{2,} \cdot \rangle \longrightarrow A \cdot B = C \cdot B$ **?**

$$A=\begin{pmatrix} 4 & 1 \\ 5 & 2 \end{pmatrix} \qquad B=\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad C=\begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}$$

$$A \cdot B = C \cdot B = \begin{pmatrix} 4 & 1 \\ 5 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

Propriedade do Cancelamento ❌

$$A \neq C$$

Propriedade do Cancelamento

EXEMPLO: $(\mathbb{Z}, \ +)$, $b*a=c*a$ → $b=c$ **?**

$$a+b=b+c \longrightarrow 3+b=5+3 \longrightarrow b=5$$

Propriedade do Cancelamento ✓

Propriedade do Cancelamento

EXEMPLO: $(\mathbb{Z}, +)$, $b*a=c*a$ → $b=c$ **?**

$$a+b=b+c \longrightarrow 3+b=5+3 \longrightarrow b=5$$

Propriedade do Cancelamento ✓

EXEMPLO: $(\mathbb{Z}, \cdot)$, $b*a=c*a$ → $b=c$ **?**

$$4\cdot 0=6\cdot 0 \longrightarrow 4\neq 6$$

Propriedade do Cancelamento ✗

Grupos Lineares de Grau n

→ grupos de matrizes mxn de entrada A

$$\langle M_{mxn}(A),\ *\ \rangle$$

EXEMPLOS:

$$\langle M_{mxn}(\mathbb{Z}),\ +\ \rangle$$
$$\langle M_{mxn}(\mathbb{Q}),\ +\ \rangle$$
$$\langle M_{mxn}(\mathbb{R}),\ +\ \rangle$$
$$\langle M_{mxn}(\mathbb{C}),\ +\ \rangle$$

Grupos abelianos aditivos das matrizes de ordem mxn

Grupos Lineares de Grau n

→ grupos lineares de matrizes quadradas de ordem nxn de entrada A

$$\langle GL_n(A),\ *\ \rangle$$

EXEMPLOS:

$$GL_n(\mathbb{Q})$$
$$GL_n(\mathbb{R})$$
$$GL_n(\mathbb{C})$$

Grupos Lineares de Grau n

EXEMPLO: Verifique se $M_n(\mathbb{Q})$ é grupo para operação de multiplicação

1) fechamento: $A_n \cdot B_n = C_n \in M_n(\mathbb{Q})$

2) Associativa: $A_n \cdot (B_n \cdot C_n) = (A_n \cdot B_n) \cdot C_n$

3) Elemento Neutro: $\exists I_n \in M_n(\mathbb{Q}) / A_{¿} I_n = I_n \cdot A_n = A$

4) Elemento Inverso:

Condição necessária:
Determinante de cada elemento seja diferente de zero.

Restrição para multiplicação de matrizes serem grupos:
Matrizes quadradas com elementos que possuem determinante não nulo

como $M_n(\mathbb{Q})$ é subconjunto de $GL_n(\mathbb{Q})$ então:

$$GL_n(\mathbb{Q}) = \{ A \in M_n(\mathbb{Q}) / \det A \neq 0 \}$$

este conjunto é o grupo chamado grupo linear de grau n

Grupos Finitos e Infinitos

Um grupo finito é um grupo $(G, \ *\ )$ em que o número de elementos de G é a ordem do grupo $(o(G))$. Caso contrário, diz-se que o grupo é infinito e que sua ordem é infinita.

EXEMPLO:

$$G=\{-i,-1,i,1\}$$

$$G=\{1,2,3\}$$

$$H=\{1,2,3,\ldots\}$$

Grupos Finitos e Infinitos

Um grupo finito é um grupo $(G, \ *\ )$ em que o número de elementos de G é a ordem do grupo $(o(G))$. Caso contrário, diz-se que o grupo é infinito e que sua ordem é infinita.

EXEMPLO:

$$G=\{-i,-1,i,1\} \longrightarrow o(G)=4$$

$$G=\{1,2,3\} \longrightarrow o(G)=3$$

$$H=\{1,2,3,\ldots\} \longrightarrow o(G)=grupo\, infinito$$

EXEMPLO: *Tabela de Cayley*

Considere o conjunto $G=\{-1,1\}$ e a operação binária usual. Será que $(G,\ \cdot\ )$ é um grupo finito?

EXEMPLO: *Tabela de Cayley*

Considere o conjunto $G=\{-1,1\}$ e a operação binária usual. Será que $(G, \cdot)$ é um grupo finito?

1º) construir a tabela operatória

$\cdot$	**-1**	**1**
-1	1	-1
1	-1	1

EXEMPLO: *Tabela de Cayley*

2º) Verificar as propriedades

a) Fechamento ✓

·	-1	1
-1	1	-1
1	-1	1

Todos os elementos resultantes da operação multiplicação pertencem a G => G é fechado

EXEMPLO: *Tabela de Cayley*

2º) Verificar as propriedades

a) Fechamento ✓

b) Associativa ✓

$\cdot$	-1	1
-1	1	-1
1	-1	1

$$-1\cdot(-1\cdot(-1))=(-1\cdot(-1))\cdot(-1)$$
$$-1\cdot(-1\cdot 1)=(-1\cdot(-1))\cdot 1$$
$$-1\cdot(1\cdot(-1))=(-1\cdot 1)\cdot(-1)$$
$$-1\cdot(1\cdot 1)=(-1\cdot 1)\cdot 1$$
$$1\cdot(-1\cdot(-1))=(1\cdot(-1))\cdot(-1)$$
$$1\cdot(-1\cdot 1)=(1\cdot(-1))\cdot 1$$
$$1\cdot(1\cdot(-1))=(1\cdot 1)\cdot(-1)$$
$$1\cdot(1\cdot 1)=(1\cdot 1)\cdot 1$$

Além disso, o conjunto G é formado por números inteiros e a associatividade é válida para o produto de números inteiros, por restrição, é válida, também, para G.

EXEMPLO: *Tabela de Cayley*

2º) Verificar as propriedades

a) Fechamento ✓

b) Associativa ✓

·	-1	1
-1	1	-1
1	-1	1

c) Elemento Neutro ✓

O elemento neutro na multiplicação é o 1

EXEMPLO: *Tabela de Cayley*

2º) Verificar as propriedades

a) Fechamento ✓

b) Associativa ✓

·	-1	1
-1	1	-1
1	-1	1

c) Elemento Neutro ✓

d) Elemento Invertível ✓

O inverso de -1 é -1, pois

$$-1 \cdot (-1) = 1$$

1 é o elemento neutro da multiplicação. O inverso de 1 é 1.

EXEMPLO: *Tabela de Cayley*

2º) Verificar as propriedades

a) Fechamento ✓

b) Associativa ✓

$\cdot$	-1	1
-1	1	-1
1	-1	1

c) Elemento Neutro ✓

d) Elemento Invertível ✓

Logo,

G é grupo em relação à multiplicação.

EXEMPLO: *Tabela de Cayley*

2º) Verificar as propriedades

a) Fechamento ✓

b) Associativa ✓

$\cdot$	-1	1
-1	1	-1
1	-1	1

c) Elemento Neutro ✓

d) Elemento Invertível ✓

Observe, também, que existe simetria dos elementos da tabela em relação à diagonal principal.

EXEMPLO: *Tabela de Cayley*

2º) Verificar as propriedades

a) Fechamento

b) Associativa

·	-1	1
-1	1	-1
1	-1	1

c) Elemento Neutro

d) Elemento Invertível

Observe, também, que existe simetria dos elementos da tabela em relação à diagonal principal. Logo, existe comutatividade da operação sobre G.

EXEMPLO: *Tabela de Cayley*

2º) Verificar as propriedades

a) Fechamento ✓

b) Associativa ✓

$\cdot$	-1	1
-1	1	-1
1	-1	1

c) Elemento Neutro ✓

d) Elemento Invertível ✓

e) Comutativa ✓

$(G, \cdot)$ **é um Grupo Abeliano Finito de ordem 2**

FONTE: Soares, M. (2012)
https://www.uniasselvi.com.br/extranet/layout/request/trilha/materiais/livro/livro.php?codigo=7272

Permutação

- Possíveis maneiras de se ordenar os elementos do conjunto sem repetir nenhum e usando todos

<u>*Definição:*</u>

Seja A um conjunto. Uma permutação sobre A é uma bijeção de A em si mesmo.

EXEMPLO:

$$A = \{1,2,3,4,5\} \qquad f : A \rightarrow A$$

$$f = \{(1,2),(2,4),(3,1),(4,3),(5,5)\}$$

Permutação

Representação:

→ Por letras minúsculas gregas (π, σ, τ)

→ Número de permutações: $n!$

→ Conjunto de todas as permutações: $|S_n| = n!$

Propriedades

$$\forall\, \pi, \sigma, \tau \in S_n, \pi \circ \sigma \in S_n$$

$$\forall\, \pi, \sigma, \tau \in S_n, \pi \circ (\sigma \circ \tau) = (\pi \circ \sigma) \circ \tau$$

$$\forall\, \pi \in S_n, \pi \circ \iota = \iota \circ \pi = \pi$$

$$\forall\, \pi \in S_n, \pi^{-1} \in S_n \, e \, \pi \circ \pi^{-1} = \pi^{-1} \circ \pi = \iota$$

Permutação

<u>FORMAS DE REPRESENTAÇÃO DA PERMUTAÇÃO:</u>

EXEMPLO: Seja a permutação S_5 a seguir:

$$\pi = \{(1,2),(2,4),(3,1),(4,3),(5,5)\}$$

a) expresse-a na forma de tabela:

b) expresse-a na forma de quadro:

c) expresse-a na forma de ciclos:

Permutação

FORMAS DE REPRESENTAÇÃO DA PERMUTAÇÃO:

EXEMPLO: $\pi = \{(1,2),(2,4),(3,1),(4,3),(5,5)\}$

a) Tabela:

x	$\pi(x)$
1	2
2	4
3	1
4	3
5	5

b) Quadro

c) Ciclos

Permutação

FORMAS DE REPRESENTAÇÃO DA PERMUTAÇÃO:

EXEMPLO: $\pi = \{(1,2),(2,4),(3,1),(4,3),(5,5)\}$

a) Tabela:

x	$\pi(x)$
1	2
2	4
3	1
4	3
5	5

b) Quadro

$$\pi = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{Bmatrix}$$

c) Ciclos

Permutação

FORMAS DE REPRESENTAÇÃO DA PERMUTAÇÃO:

EXEMPLO: $\pi = \{(1,2),(2,4),(3,1),(4,3),(5,5)\}$

a) Tabela:

x	$\pi(x)$
1	2
2	4
3	1
4	3
5	5

b) Quadro

$$\pi = \left\{\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{matrix}\right\}$$

c) Ciclos $\pi = (1,2,3,4)(5)$

Permutação

FORMAS DE REPRESENTAÇÃO DA PERMUTAÇÃO:

EXEMPLO: $\pi = \{(1,2),(2,4),(3,1),(4,3),(5,5)\}$

a) Tabela:

x	$\pi(x)$
1	2
2	4
3	1
4	3
5	5

b) Quadro

$$\pi = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{Bmatrix}$$

c) Ciclos $\pi = (1,2,3,4)(5)$

$$1 \longmapsto 2 \longmapsto 4 \longmapsto 3 \longmapsto 1$$

$\pi(1) = 2$

$\pi(2) = 4$

$\pi(5) = 5$

$\pi(4) = 3$

$\pi(3) = 1$

Permutação

FORMAS DE REPRESENTAÇÃO DA PERMUTAÇÃO:

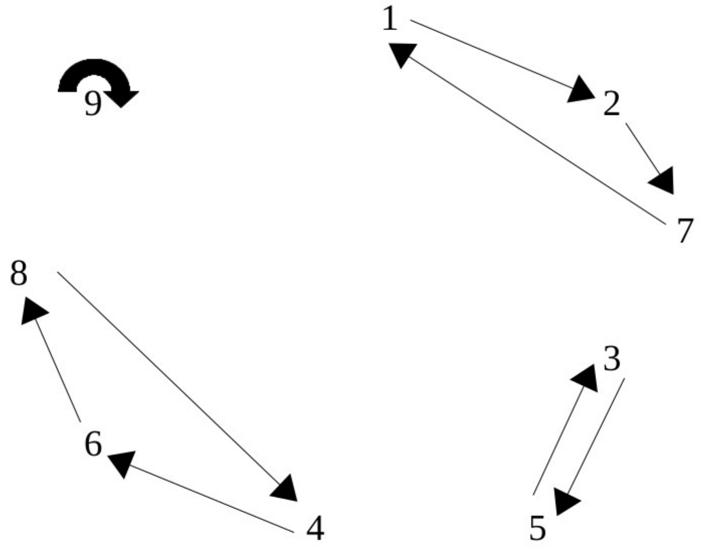
EXEMPLO:

$$\pi = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 5 & 6 & 3 & 8 & 1 & 4 & 9 \end{Bmatrix} \in S_9$$

Ciclos:

$$(1,2,7)(3,5)(4,6,8)(9)$$

Grafos:



Permutação

<u>INVERSA:</u>

$\pi(k)=j$ → se j segue k em um ciclo π ,

$\pi^{-1}(j)=k$ → k segue j em um ciclo π^{-1}

EXEMPLO:

$$\pi=(1,2,7,9,8)(5,6,3)(4) \quad \in S_9$$

$$\pi^{-1}=(8,9,7,2,1)(3,6,5)(4)$$

GRUPOS DE PERMUTAÇÃO

Seja A um conjunto não vazio. Denotaremos por $P(A)=\{f:A \rightarrow A, f \text{ é bijetora}\}$
Então, $(P(A), \circ, i_A)$ é um grupo em que a operação $\circ$ é a composição de funções e o elemento neutro é a função identidade de A, denotado i_A.

O grupo $(P(A), \circ, i_A)$ é chamado grupo das permutação de A.

GRUPOS DE PERMUTAÇÃO

EXEMPLO: S_3(P) , P={1,2,3} , operação composição de funções

n! = 3! = 6 bijeções

S_3= {f_0, f_1, f_2, f_3, f_4, f_5, f_6}

$$f_0=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} \qquad f_3=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

$$f_1=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} \qquad f_4=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$$

$$f_2=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} \qquad f_5=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$

GRUPOS DE PERMUTAÇÃO

EXEMPLO: S_3(P) , P={1,2,3}

$\circ$	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_2	f_0	f_4	f_5	f_3
f_2	f_2	f_0	f_1	f_5	f_3	f_4
f_3	f_3	f_5	f_4	f_0	f_2	f_1
f_4	f_4	f_3	f_5	f_1	f_0	f_2
f_5	f_5	f_4	f_3	f_2	f_1	f_0

GRUPOS DE PERMUTAÇÃO

EXEMPLO: $S=\{1,2,3\}$, $f, g \in S_3$, calcule $(f \circ g)$ e $(g \circ f)$, dados:

$$f:\begin{cases} f(1)=2 \\ f(2)=1 \\ f(3)=3 \end{cases} \qquad g:\begin{cases} g(1)=2 \\ g(2)=3 \\ g(3)=1 \end{cases}$$

Verifique se é comutativa.

GRUPOS DE PERMUTAÇÃO

EXEMPLO: $S=\{1,2,3\}$, $f, g \in S_3$, calcule $(f \circ g)$ e $(g \circ f)$, dados:

$$f: \begin{cases} f(1)=2 \\ \underline{f(2)=1} \\ f(3)=3 \end{cases} \qquad g: \begin{cases} \underline{g(1)=2} \\ g(2)=3 \\ g(3)=1 \end{cases}$$

$$f \circ g(1) = f(g(1)) = f(2) = 1$$

GRUPOS DE PERMUTAÇÃO

EXEMPLO: $S=\{1,2,3\}$, $f,g\in S_3$, calcule $(f\circ g)$ e $(g\circ f)$, dados:

$$f:\begin{cases} f(1)=2 \\ f(2)=1 \\ f(3)=3 \end{cases} \qquad g:\begin{cases} g(1)=2 \\ g(2)=3 \\ g(3)=1 \end{cases}$$

$$f\circ g(1)=f(g(1))=f(2)=1 \quad \neq \quad g\circ f(1)=g(f(1))=g(2)=3$$

$$f\circ g(2)=f(g(2))=f(3)=3 \quad \neq \quad g\circ f(2)=g(f(2))=g(1)=2$$

$$f\circ g(3)=f(g(3))=f(1)=2 \quad \neq \quad g\circ f(3)=g(f(3))=g(3)=1$$

$$f\circ g\neq g\circ f$$

não é grupo comutativo

GRUPOS DE PERMUTAÇÃO

Outra notação: $f = \begin{bmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \ldots & f(n) \end{bmatrix}$

EXEMPLO: Em S_4 calcule $(f \circ g)$ e $(g \circ f)$, dados:

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix} \qquad g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix}$$

Verifique se é comutativa.

GRUPOS DE PERMUTAÇÃO

Outra notação: $f = \begin{bmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \ldots & f(n) \end{bmatrix}$

EXEMPLO: Em S_4 calcule $(f \circ g)$ e $(g \circ f)$, dados:

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix} \qquad g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix}$$

$f(g(1)) =$

GRUPOS DE PERMUTAÇÃO

Outra notação: $f=\begin{bmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \ldots & f(n) \end{bmatrix}$

EXEMPLO: Em S_4 calcule $(f \circ g)$ e $(g \circ f)$, dados:

$$f=\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix} \quad g=\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix}$$

$f(g(1))=f(1)=3$ $\quad$ $f(g(3))=f(4)=4$

$f(g(2))=f(3)=2$ $\quad$ $f(g(4))=f(2)=1$

GRUPOS DE PERMUTAÇÃO

Outra notação: $f = \begin{bmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \ldots & f(n) \end{bmatrix}$

EXEMPLO: Em S_4 calcule $(f \circ g)$ e $(g \circ f)$, dados:

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix} \qquad g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix}$$

$$f \circ g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix}$$

GRUPOS DE PERMUTAÇÃO

Outra notação: $f = \begin{bmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{bmatrix}$

EXEMPLO: Em S_4 calcule $(f \circ g)$ e $(g \circ f)$, dados:

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix} \qquad g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix}$$

$$g(f(1)) = g(3) = 4 \qquad g(f(3)) = g(2) = 3$$

$$f \circ g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix}$$

$$g(f(2)) = g(1) = 1 \qquad g(f(4)) = g(4) = 2$$

GRUPOS DE PERMUTAÇÃO

Outra notação: $f = \begin{bmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \ldots & f(n) \end{bmatrix}$

EXEMPLO: Em S_4 calcule $(f \circ g)$ e $(g \circ f)$, dados:

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix} \qquad g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix}$$

$$f \circ g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix} \qquad g \circ f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{bmatrix}$$

GRUPOS DE PERMUTAÇÃO

Outra notação: $f = \begin{bmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{bmatrix}$

EXEMPLO: Em S_4 calcule $(f \circ g)$ e $(g \circ f)$, dados:

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix} \qquad g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix}$$

$$f \circ g = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix} \qquad g \circ f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{bmatrix}$$

$$f \circ g \neq g \circ f$$ não é grupo comutativo

GRUPOS CÍCLICOS

Sejam $(G, \cdot, e)$ um grupo, $a \in G$ e $n \in \mathbb{N}$, definimos a potência do elemento a recursivamente por:

$$a^0 = e \quad \text{e} \quad a^{n+1} = a^n \cdot a$$

sendo seu inverso denotado por a^{-1}.

Ou seja, um grupo cíclico é um conjunto formado por um gerador a, contanto que cada elemento de G seja uma potência de a

Obs:se o grupo for aditivo $(G, +, 0)$ entenda a^n como $n \cdot a$ e a^{-1} como $-a$.

GRUPOS CÍCLICOS

Propriedades:

- $a^{n+m} = a^n \cdot a^m$
- $(a^n)^m = a^{n \cdot m}$
- $(a^n)^{-1} = a^{-n}$
- $(a^{-n})^{-1} = a^n$

GRUPOS CÍCLICOS

Propriedades:

- $a^{n+m}=a^n \cdot a^m$
- $(a^n)^m=a^{n\cdot m}$
- $(a^n)^{-1}=a^{-n}$
- $(a^{-n})^{-1}=a^n$

Notação: $(G, \cdot, e)$, $a \in G \longrightarrow \langle a \rangle=\{a^n, n\in\mathbb{Z}\}$

$(G, +, e)$, $a \in G \longrightarrow \langle a \rangle=\{n\cdot a, n\in\mathbb{Z}\}$ (Notação aditiva)

GRUPOS CÍCLICOS

EXEMPLO:

a) $G = \{a^0,\ a^1,\ a^2,\ a^3,\ a^4\}$

GRUPOS CÍCLICOS

EXEMPLO:

a) $G = \{a^0,\ a^1,\ a^2,\ a^3,\ a^4\}$

b) $a = \{3,2,1\}$

$$G = \{\{1,2,3\},\{3,2,1\},\{1,2,3\},\{3,2,1\},\{1,2,3\}\}$$