

# Grupos Cíclicos

José Antônio O. Freitas

MAT-UnB

29 de outubro de 2020

Seja  $(G, *)$  um grupo.

Seja  $(G, *)$  um grupo.

Caso a operação  $*$  seja do tipo multiplicativa, vamos escrever  
 $(G, *) =$

Seja  $(G, *)$  um grupo.

Caso a operação  $*$  seja do tipo multiplicativa, vamos escrever  
 $(G, *) = (G, \cdot)$ .

Seja  $(G, *)$  um grupo.

Caso a operação  $*$  seja do tipo multiplicativa, vamos escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

Seja  $(G, *)$  um grupo.

Caso a operação  $*$  seja do tipo multiplicativa, vamos escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x \underline{*} y =$$

Seja  $(G, *)$  um grupo.

Caso a operação  $*$  seja do tipo multiplicativa, vamos escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x \cdot y =$$

Seja  $(G, *)$  um grupo.

Caso a operação  $*$  seja do tipo multiplicativa, vamos escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x \cdot y = \underline{xy}.$$

Caso a operação  $\underline{*}$  seja do tipo aditiva, vamos escrever  $(G, \underline{*}) =$

Seja  $(G, *)$  um grupo.

Caso a operação  $*$  seja do tipo multiplicativa, vamos escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x \cdot y = xy.$$

Caso a operação  $*$  seja do tipo aditiva, vamos escrever  $(G, *) = (G, +)$ .

Seja  $(G, *)$  um grupo.

Caso a operação  $*$  seja do tipo multiplicativa, vamos escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x \cdot y = xy.$$

Caso a operação  $*$  seja do tipo aditiva, vamos escrever  $(G, *) = (G, +)$ .

Assim, dados  $x, y \in G$  vamos denotar

Seja  $(G, *)$  um grupo.

Caso a operação  $*$  seja do tipo multiplicativa, vamos escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x \cdot y = xy.$$

Caso a operação  $*$  seja do tipo aditiva, vamos escrever  $(G, *) = (G, +)$ .

Assim, dados  $x, y \in G$  vamos denotar

$$x \underline{*} y =$$

Seja  $(G, *)$  um grupo.

Caso a operação  $*$  seja do tipo multiplicativa, vamos escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x \cdot y = xy.$$

Caso a operação  $*$  seja do tipo aditiva, vamos escrever  $(G, *) = (G, +)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x + y$$

Com a notação multiplicativa

Seja  $(G, *)$  um grupo.

Caso a operação  $*$  seja do tipo multiplicativa, vamos escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x \cdot y = xy.$$

Caso a operação  $*$  seja do tipo aditiva, vamos escrever  $(G, *) = (G, +)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x + y$$

Com a notação multiplicativa o inverso de um elemento  $x \in G$

Seja  $(G, *)$  um grupo.

Caso a operação  $*$  seja do tipo multiplicativa, vamos escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x \cdot y = xy.$$

Caso a operação  $*$  seja do tipo aditiva, vamos escrever  $(G, *) = (G, +)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x + y$$

Com a notação multiplicativa o inverso de um elemento  $x \in G$  será denotado por  $\underline{x}^{-1}$

Seja  $(G, *)$  um grupo.

Caso a operação  $*$  seja do tipo multiplicativa, vamos escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x \cdot y = xy.$$

Caso a operação  $*$  seja do tipo aditiva, vamos escrever  $(G, *) = (G, +)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x + y$$

Com a notação multiplicativa o inverso de um elemento  $x \in G$  será denotado por  $x^{-1}$  e no caso da notação aditiva

Seja  $(G, *)$  um grupo.

Caso a operação  $*$  seja do tipo multiplicativa, vamos escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x \cdot y = xy.$$

Caso a operação  $*$  seja do tipo aditiva, vamos escrever  $(G, *) = (G, +)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x + y$$

Com a notação multiplicativa o inverso de um elemento  $x \in G$  será denotado por  $x^{-1}$  e no caso da notação aditiva o oposto de  $x \in G$

# e ELEMENTO NEUTRO

Seja  $(G, *)$  um grupo.

Caso a operação  $*$  seja do tipo multiplicativa, vamos escrever

$(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x \cdot y = xy.$$

Caso a operação  $*$  seja do tipo aditiva, vamos escrever  $(G, *) = (G, +)$ .

Assim, dados  $x, y \in G$  vamos denotar

$$x * y = x + y$$

Com a notação multiplicativa o inverso de um elemento  $x \in G$  será denotado por  $x^{-1}$  e no caso da notação aditiva o oposto de  $x \in G$  será denotado por  $-x$ .

$$x * y = ? \Rightarrow y * x$$

Seja  $G$  um grupo multiplicativo

Seja  $G$  um grupo multiplicativo e denote por  $\underline{e}$  o elemento neutro de  $\underline{G}$ .

Seja  $G$  um grupo multiplicativo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$

Seja  $G$  um grupo multiplicativo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ ,

Seja  $G$  um grupo multiplicativo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , a potência  $m$ -ésima de  $x$ ,

Seja  $G$  um grupo multiplicativo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , a **potência  $m$ -ésima** de  $x$ , ou **potência de  $x$  de expoente  $m$** ,

Seja  $G$  um grupo multiplicativo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , a **potência  $m$ -ésima** de  $x$ , ou **potência de  $x$  de expoente  $m$** , é o elemento de  $G$  denotado por

Seja  $G$  um grupo multiplicativo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , a **potência  $m$ -ésima** de  $x$ , ou **potência de  $x$  de expoente  $m$** , é o elemento de  $G$  denotado por

$$x^m$$

Seja  $G$  um grupo multiplicativo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , a **potência  $m$ -ésima** de  $x$ , ou **potência de  $x$  de expoente  $m$** , é o elemento de  $G$  denotado por

$$x^m$$

e definido por:

Seja  $G$  um grupo multiplicativo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , a **potência  $m$ -ésima** de  $x$ , ou **potência de  $x$  de expoente  $m$** , é o elemento de  $G$  denotado por

$$x^m$$

e definido por:

$$x^m =$$

Seja  $G$  um grupo multiplicativo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , a **potência  $m$ -ésima** de  $x$ , ou **potência de  $x$  de expoente  $m$** , é o elemento de  $G$  denotado por

$$x^m$$

e definido por:

$$x^m = \begin{cases} e & \text{se } m = 0, \\ \end{cases}$$

Seja  $G$  um grupo multiplicativo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , a **potência  $m$ -ésima** de  $x$ , ou **potência de  $x$  de expoente  $m$** , é o elemento de  $G$  denotado por

$$x^m$$

e definido por:

$$x^m = \begin{cases} e, & \text{se } m = 0, \\ x^{m-1}x, & \text{outros casos.} \end{cases}$$

Seja  $G$  um grupo multiplicativo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , a **potência  $m$ -ésima** de  $x$ , ou **potência de  $x$  de expoente  $m$** , é o elemento de  $G$  denotado por

$$x^m$$

e definido por:

$$x^m = \begin{cases} e, & \text{se } m = 0, \\ \underbrace{x^{m-1}x}, & \text{se } m \geq 1 \end{cases}$$

$$x^2 = x^{2-1} \cdot x = x \cdot x$$

$$x^3 = x^{3-1} \cdot x = x^2 \cdot x$$

Seja  $G$  um grupo multiplicativo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , a **potência  $m$ -ésima** de  $x$ , ou **potência de  $x$  de expoente  $m$** , é o elemento de  $G$  denotado por

$$x^m$$

e definido por:

$$x^m = \begin{cases} e, & \text{se } m = 0, \\ x^{m-1}x, & \text{se } m \geq 1 \\ (x^{-m})^{-1}, & \end{cases}$$

Seja  $G$  um grupo multiplicativo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , a **potência  $m$ -ésima** de  $x$ , ou **potência de  $x$  de expoente  $m$** , é o elemento de  $G$  denotado por

$$\underline{x^m}$$

e definido por:

$$\rightarrow x^m = \begin{cases} e, & \text{se } m = 0, \\ x^{m-1}x, & \text{se } m \geq 1 \\ (\cancel{x^{-m}})^{-1}, & \text{se } \underline{m < 0}. \end{cases}$$

$$x^{-3} = [x^{-(\cdot -3)}]^{-1} = (x^3)^{-1}$$

$$GL_m(\mathbb{R}) = \{A \in M_m(\mathbb{R}) \mid \det(A) \neq 0\}$$

## Exemplos

1) No grupo multiplicativo  $\underline{GL}_2(\mathbb{R})$

## Exemplos

1) No grupo multiplicativo  $GL_2(\mathbb{R})$  seja

## Exemplos

1) No grupo multiplicativo  $GL_2(\mathbb{R})$  seja

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}.$$

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

$$A^2 = A \cdot A = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 8 & 11 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}; \quad A^{-2} = (A^2)^{-1} = \begin{pmatrix} 1 & -4 \\ -8 & 3 \end{pmatrix}$$

$$A^n, \quad n \in \mathbb{Z}.$$

## Exemplos

2) No grupo multiplicativo  $\mathbb{Z}_5^*$

## Exemplos

2) No grupo multiplicativo  $\mathbb{Z}_5^*$  seja  $a = \bar{2}$ .

$$\bar{2}^0 = \bar{1}$$

$$\bar{2}^1 = 2$$

$$\bar{2}^2 = \bar{2} \odot \bar{2} = \bar{4}$$

$$\left| \begin{array}{l} \bar{2}^3 = (\bar{2})^2 \cdot \bar{2} = \bar{4} \cdot \bar{2} = \bar{3} \\ \bar{2}^4 = (\bar{2})^3 \cdot \bar{2} = \bar{3} \cdot \bar{2} = \bar{1} \end{array} \right.$$

$$(\bar{z})^{-1} = \bar{z}$$

$$(\bar{z})^{-2} = (\bar{z}^2)^{-1} = (\bar{4})^{-1} = \bar{4}$$

$$(\bar{z})^{-3} = (\bar{z}^3)^{-1} = (\bar{3})^{-1} = \bar{z}$$

$$(\bar{z})^{-4} = (\bar{z}^4)^{-1} = (\bar{1})^{-1} = \bar{1}$$

## Exemplos

3) No grupo multiplicativo  $S_3$

## Exemplos

3) No grupo multiplicativo  $S_3$  seja

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

## Exemplos

3) No grupo multiplicativo  $S_3$  seja

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Então:

$$a^0 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = e$$

$$a^1 = a$$

$$a^2 = a \circ a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = a^2$$

$$\underline{a}^3 = \underline{a}^2 \cdot \underline{a} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \underline{c}$$

$$\underline{a}^4 = \underline{a}^3 \cdot \underline{a} = \underline{c} \cdot \underline{a} = \underline{a}$$

$$\underline{a}^5 = \underline{a}^4 \cdot \underline{a} = \underline{a} \cdot \underline{a} = \underline{a}^2$$

$$a^{-2} = a^2$$

$$a^{-2} = (a^2)^{-1} = a$$

$$a^{-3} = (a^3)^{-1} = e^{-1} = e$$

⋮

## Proposição

Seja  $G$  um grupo multiplicativo.

## Proposição

Seja  $G$  um grupo multiplicativo. Se  $\underline{m}$  e  $\underline{n}$  são números inteiros

## Proposição

Seja  $G$  um grupo multiplicativo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ ,

## Proposição

Seja  $G$  um grupo multiplicativo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

## Proposição

Seja  $G$  um grupo multiplicativo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

1)  $x^m x^n =$

## Proposição

Seja  $G$  um grupo multiplicativo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

$$1) x^m x^n = \cancel{x}^{m+n}$$

## Proposição

Seja  $G$  um grupo multiplicativo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

$$1) x^m x^n = x^{m+n}$$

$$2) x^{-m} =$$

## Proposição

Seja  $G$  um grupo multiplicativo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

- 1)  $x^m x^n = x^{m+n}$
- 2)  $x^{-m} = (x^m)^{-1}$

## Proposição

Seja  $G$  um grupo multiplicativo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

$$1) x^m x^n = x^{m+n}$$

$$2) x^{-m} = (x^m)^{-1}$$

$$3) (x^m)^n =$$

## Proposição

Seja  $G$  um grupo multiplicativo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

- 1)  $x^m x^n = x^{m+n}$
- 2)  $x^{-m} = (x^m)^{-1}$
- 3)  $(x^m)^n = x^{\cancel{mn}}$

## Proposição

Seja  $G$  um grupo multiplicativo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

$$1) x^m x^n = x^{m+n}$$

$$2) x^{-m} = (x^m)^{-1}$$

$$3) (x^m)^n = x^{mn}$$

$$4) \cancel{x^m} \cdot \cancel{x^n} =$$

## Proposição

Seja  $G$  um grupo multiplicativo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

- 1)  $x^m x^n = x^{m+n}$
- 2)  $x^{-m} = (x^m)^{-1}$
- 3)  $(x^m)^n = x^{mn}$
- 4)  $x^m x^n = x^{m+n}$

## Proposição

Seja  $G$  um grupo multiplicativo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

$$1) x^m x^n = x^{m+n}$$

$$2) x^{-m} = (x^m)^{-1}$$

$$3) (x^m)^n = x^{mn}$$

$$\cancel{4) x^m x^n = x^{m+n}}$$

$$5) x^m x^n =$$

## Proposição

Seja  $G$  um grupo multiplicativo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

- 1)  $x^m x^n = x^{m+n}$
- 2)  $x^{-m} = (x^m)^{-1}$
- 3)  $(x^m)^n = x^{mn}$
- 4)  ~~$x^m x^n = x^{m+n}$~~
- 5)  ~~$x^m x^n = x^n x^m$~~

Seja  $G$  um grupo aditivo

Seja  $G$  um grupo aditivo e denote por  $\underline{e}$  o elemento neutro de  $G$ .

Seja  $G$  um grupo aditivo e denote por  $e$  o elemento neutro de  $G$ . Se  $\underline{x} \in G$

Seja  $G$  um grupo aditivo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ ,

Seja  $G$  um grupo aditivo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , o **múltiplo  $m$ -ésimo** de  $x$

Seja  $G$  um grupo aditivo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , o **múltiplo  $m$ -ésimo** de  $x$  é o elemento de  $G$  denotado por

Seja  $G$  um grupo aditivo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , o **múltiplo  $m$ -ésimo** de  $x$  é o elemento de  $G$  denotado por

$$\underline{\underline{m \cdot x}}$$

Seja  $G$  um grupo aditivo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , o **múltiplo  $m$ -ésimo** de  $x$  é o elemento de  $G$  denotado por

$$m \cdot x$$

e definido por:

$$\underline{m} \cdot x =$$

Seja  $G$  um grupo aditivo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , o **múltiplo  $m$ -ésimo** de  $x$  é o elemento de  $G$  denotado por

$$m \cdot x$$

e definido por:

$$m \cdot x = \begin{cases} e, & \text{se } m = 0, \\ \text{(definição de multiplicação em } G\text{)} & \end{cases}$$

Seja  $G$  um grupo aditivo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , o **múltiplo  $m$ -ésimo** de  $x$  é o elemento de  $G$  denotado por

$$m \cdot x$$

e definido por:

$$m \cdot x = \begin{cases} e, & \text{se } m = 0, \\ (m - 1) \cdot x + x, & \text{outros casos.} \end{cases}$$

Seja  $G$  um grupo aditivo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , o **múltiplo  $m$ -ésimo** de  $x$  é o elemento de  $G$  denotado por

$$m \cdot x$$

e definido por:

$$\underline{m} \cdot x = \begin{cases} e, & \text{se } m = 0, \\ (\underline{m - 1}) \cdot x + x, & \text{se } \underline{m \geq 1} \end{cases}$$

$$2x = (2-1)x + x = x + x$$

$$3x = (3-1)x + x = 2x + x$$

Seja  $G$  um grupo aditivo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , o **múltiplo  $m$ -ésimo** de  $x$  é o elemento de  $G$  denotado por

$$m \cdot x$$

e definido por:

$$m \cdot x = \begin{cases} e, & \text{se } m = 0, \\ (m - 1) \cdot x + x, & \text{se } m \geq 1 \\ -[(-m) \cdot x], & \text{se } m < 0 \end{cases}$$

Seja  $G$  um grupo aditivo e denote por  $e$  o elemento neutro de  $G$ . Se  $x \in G$  e  $m \in \mathbb{Z}$ , o **múltiplo  $m$ -ésimo** de  $x$  é o elemento de  $G$  denotado por

$$m \cdot x$$

e definido por:

$$m \cdot x = \begin{cases} e, & \text{se } m = 0, \\ (m - 1) \cdot x + x, & \text{se } m \geq 1 \\ \ominus[(\textcolor{red}{-m}) \cdot x], & \text{se } m < 0. \end{cases}$$

$$-2x = -[-(-2) \cdot x] = \ominus[2x]$$

$$-3x = -[3x]$$

## Proposição

*Seja  $G$  um grupo aditivo.*

## Proposição

Seja  $G$  um grupo aditivo. Se  $m$  e  $n$  são números inteiros

## Proposição

*Seja  $G$  um grupo aditivo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então*

## Proposição

Seja  $G$  um grupo aditivo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

1)  $\underline{m \cdot x} + \underline{n \cdot x} =$

## Proposição

Seja  $G$  um grupo aditivo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

$$1) m \cdot x + n \cdot x = (\underline{m} + \underline{n}) \cdot \underline{x}$$

## Proposição

Seja  $G$  um grupo aditivo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

$$1) m \cdot x + n \cdot x = (m + n) \cdot x$$

$$2) (\underline{-m}) \cdot \underline{x} =$$

## Proposição

Seja  $G$  um grupo aditivo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

$$1) m \cdot x + n \cdot x = (m + n) \cdot x$$

$$2) (-m) \cdot x = \cancel{-(m \cdot x)}$$

## Proposição

Seja  $G$  um grupo aditivo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

$$1) m \cdot x + n \cdot x = (m + n) \cdot x$$

$$2) (-m) \cdot x = - (m \cdot x)$$

$$3) \underline{n} \cdot (\underline{m} \cdot \underline{x}) =$$

## Proposição

Seja  $G$  um grupo aditivo. Se  $m$  e  $n$  são números inteiros e  $x \in G$ , então

- 1)  $m \cdot x + n \cdot x = (m + n) \cdot x$
- 2)  $(-m) \cdot x = - (m \cdot x)$
- 3)  $n \cdot (m \cdot x) = (\underline{nm}) \cdot \underline{x}$

Seja  $G$  um grupo multiplicativo

Seja  $G$  um grupo multiplicativo e  $x \in G$ .

Seja  $G$  um grupo multiplicativo e  $x \in G$ . Denote por  $[x]$

Seja  $G$  um grupo multiplicativo e  $x \in G$ . Denote por  $[x]$  o seguinte conjunto

Seja  $G$  um grupo multiplicativo e  $x \in G$ . Denote por  $[x]$  o seguinte conjunto

$$[\underline{x}] =$$

Seja  $G$  um grupo multiplicativo e  $x \in G$ . Denote por  $[x]$  o seguinte conjunto

$$[x] = \{\underline{x}^m$$

Seja  $G$  um grupo multiplicativo e  $x \in G$ . Denote por  $[x]$  o seguinte conjunto

$$[x] = \{x^m \mid \underline{m \in \mathbb{Z}}\}$$

Seja  $\underline{G}$  um grupo multiplicativo e  $x \in G$ . Denote por  $[x]$  o seguinte conjunto

$$\rightarrow [x] = \{x^m \mid m \in \mathbb{Z}\} \subseteq G.$$

Seja  $G$  um grupo multiplicativo e  $x \in G$ . Denote por  $[x]$  o seguinte conjunto

$$[x] = \{x^m \mid m \in \mathbb{Z}\} \subset G.$$

## Proposição

Seja  $G$  um grupo multiplicativo

Seja  $G$  um grupo multiplicativo e  $x \in G$ . Denote por  $[x]$  o seguinte conjunto

$$[x] = \{x^m \mid m \in \mathbb{Z}\} \subset G.$$

## Proposição

Seja  $G$  um grupo multiplicativo e  $x \in G$ .

Seja  $G$  um grupo multiplicativo e  $x \in G$ . Denote por  $[x]$  o seguinte conjunto

$$[x] = \{x^m \mid m \in \mathbb{Z}\} \subset G.$$

## Proposição

Seja  $G$  um grupo multiplicativo e  $x \in G$ .

- 1) O subconjunto  $\textcolor{red}{[X]}$

Seja  $G$  um grupo multiplicativo e  $x \in G$ . Denote por  $[x]$  o seguinte conjunto

$$[x] = \{x^m \mid m \in \mathbb{Z}\} \subset G.$$

## Proposição

Seja  $G$  um grupo multiplicativo e  $x \in G$ .

- 1) O subconjunto  $\boxed{x}$  é um subgrupo de  $G$ .

Seja  $G$  um grupo multiplicativo e  $x \in G$ . Denote por  $[x]$  o seguinte conjunto

$$[x] = \{x^m \mid m \in \mathbb{Z}\} \subset G.$$

## Proposição

Seja  $G$  um grupo multiplicativo e  $x \in G$ .

- 1) O subconjunto  $\cancel{[x]}$  é um subgrupo de  $G$ .
- 2) Se  $H$  é um subgrupo de  $G$

Seja  $G$  um grupo multiplicativo e  $x \in G$ . Denote por  $[x]$  o seguinte conjunto

$$[x] = \{x^m \mid m \in \mathbb{Z}\} \subset G.$$

## Proposição

Seja  $G$  um grupo multiplicativo e  $x \in G$ .

- 1) O subconjunto  $\cancel{[x]}$  é um subgrupo de  $G$ .
- 2) Se  $H$  é um subgrupo de  $G$  tal que  $\cancel{x} \in H$ ,

Seja  $G$  um grupo multiplicativo e  $x \in G$ . Denote por  $[x]$  o seguinte conjunto

$$\rightarrow [x] = \{ \underbrace{x^m}_{\in} \mid m \in \mathbb{Z} \} \subset G.$$

## Proposição

Seja  $G$  um grupo multiplicativo e  $x \in G$ .

- 1) O subconjunto  $[x]$  é um subgrupo de  $G$ .
- 2) Se  $H$  é um subgrupo de  $G$  tal que  $x \in H$ , então  $[x] \subset H$ .

$$[a] \neq \emptyset$$

$$x \in [a]; \quad x^{-1} \in [a]$$

$$y \in [a]; \quad x \cdot y \in [a]$$

PROVA: i) COMO  $x^0 = e$ , ENTÃO  $e \in [x]$ .  
DA:  $[x] \neq \emptyset$ .

AGORA SEJAM  $a, b \in [x]$ . ASSIM

EXISTEM  $\underline{l}, \underline{n} \in \mathbb{N}$  TAI'S QUE

$$a = x^{\underline{l}}$$

$$b = x^{\underline{n}}.$$

$$-l \in \mathbb{Z}$$

ASSIM

$$\bar{a} = (x^l)^{-1} = x^{-l} \in [x]$$

$$a \cdot b = x^l \cdot x^n = x^{l+n} \stackrel{l+n \in \mathbb{Z}}{\in} [x]$$

POR TANTO,  $[x]$  É UM SUBGRUPO

DE  $G$ .

$$\{\underline{x}^m \mid m \in \mathbb{Z}\}$$

2) SE  $x \in H$   $\in H$  È SUBGRUPO,  
ENTÃO

$$\begin{aligned}x^m &= x^{m-1} \cdot x \in H \\&= \underbrace{x \cdot x \cdot \dots \cdot x}_{m \text{ VEZES}} \in H\end{aligned}$$

Logo,  $[x] \subseteq H$ .  $\#$

## Definição

*Um grupo multiplicativo  $G$*

## Definição

Um grupo multiplicativo  $G$  será chamado de grupo cíclico

## Definição

Um grupo multiplicativo  $G$  será chamado de **grupo cíclico** se, para algum  $x \in G$ ,

## Definição

Um grupo multiplicativo  $G$  será chamado de **grupo cíclico** se, para algum  $x \in G$ , vale

## Definição

Um grupo multiplicativo  $\underline{G}$  será chamado de **grupo cíclico** se, para algum  $x \in G$ , vale

$$\underline{G} = [\underline{x}].$$

## Definição

Um grupo multiplicativo  $G$  será chamado de **grupo cíclico** se, para algum  $x \in G$ , vale

$$G = [x].$$

Nessas condições, o elemento  $\underline{x}$

## Definição

Um grupo multiplicativo  $G$  será chamado de grupo cíclico se, para algum  $x \in G$ , vale

$$\rightarrow G = [x].$$

Nessas condições, o elemento  $x$  é chamado de gerador do grupo  $G$ .

$$a, b \in G = [x]; \quad a = x^l \\ b = x^n \\ a \cdot b = x^l \cdot x^n = x^{l+n} = x^{n+l}$$

$$b \cdot a = x^n \cdot x^l = x^{n+l} = x^{l+n} = a \cdot b$$

## Exemplos

1) No grupo multiplicativo  $\underline{\mathbb{C}}^*$ ,

$\chi^{-}$

## Exemplos

1) No grupo multiplicativo  $\mathbb{C}^*$ , encontre o subgrupo gerado por  $i$ .

$$[i] = \{ i^m \mid m \in \mathbb{Z} \}$$

$$[i] = \{ i^0, i^1, i^2, \dots, i^{-1}, i^{-2}, \dots \}$$

$$[i] = \{ i^0, i^1, i^2, i^3 \} = \{ 1, i, -1, -i \}$$

## Exemplos

2) No grupo  $S_3$ ,

## Exemplos

2) No grupo  $S_3$ , encontre o subgrupo gerado por

$$\rightarrow f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

$$[f] = \left\{ f^m \mid m \in \mathbb{Z} \right\} = \{e, f, f^2\}$$

$$\text{“} f \circ f \circ f \cdots f$$

$$\begin{aligned} f^3 &= e \\ f^4 &= f \cdot f^3 = f^2 \end{aligned}$$

$[f]$  = { $e, f, f^2$ } é um SUBGRUPO

COMUTATIVO DE  $S_3$   
mas não é  
COMUTATIVO.

## Proposição

*Todo subgrupo de um grupo cíclico é também cíclico.*

SEJA UM GRUPO CÍCLICO. ISTO É,  
 $\rightarrow G = [x]$ . SE  $H$  É SUBGRUPO DE  
 $G$ , ENTÃO  $H$  É CÍCLICO.  
 $\rightarrow H = [y]$ .

PROVA: SEJA  $G = \langle x \rangle$  UM GRUPO CICLICO. TOME  $H \subseteq G$  UM SUBGRUPO.

COMO OS ELEMENTOS DE  $G$  SÃO DA FORMA  $x^m$ , PARA  $m \in \mathbb{Z}$ .  
ENTÃO OS ELEMENTOS DE  $H$  SÃO POTÊNCIAS DE  $x$ .

SE  $H = \{e\} = \{x^0\}$ , ENTÃO  $H = [c]$ .

SUPONHA QUE  $H \neq \{e\}$ . ASSIM

EXISTE  $\underline{x}^l \in H$  com  $l \neq 0$ . COMO

$H$  É SUBGRUPO, ENTÃO  $(x^l)^{-1} \in H$

PARA TODOS  $x^l \in H$ . OU SEJA, EXISTE  
EM  $H$  PELÔ MENOS UM ELEMENTO  
 $x^n$  COM  $n > 0$ .

SEJA  $\alpha > 0$  O MENOR NÚMERO  
INTERO TAL QUE  $x^\alpha \in H$ .  
DENOTE

$$x^\alpha = b.$$

VAMOS MOSTRAR QUE

$$H = \underline{[b]}.$$

COMO  $b = x \in H$ , ENTÃO  $\underline{[b]} \subseteq H$ .

A GORA SEJA  $y \in \underline{H} \subseteq \underline{G} = \underline{[x]}$ .

Q:  $y = x^{\frac{t}{\alpha}}$ ,  $t \in \mathbb{Z}$ .

EFEITUANDO A DIVISÃO INTESA  
DE  $t$  POR  $\alpha$  PODEMOS ESCREVER.

$$\rightarrow t = q\alpha + r$$

ONDE  $0 \leq r < \alpha$ .

Assim

$$\underline{b}^{-q} \in H$$

$$y = x^t = x^{qd+r} = (x^q)^d x^r = \underbrace{b^q}_H \cdot \underbrace{x^r}_H$$

DA:

$$x^r = \underbrace{b^r}_H \cdot \underbrace{y^r}_H \in H$$

OU SEJA,  $\underline{x}^{\underline{\lambda}} \in H$ . MAS  $\propto \in'$

O MÉTODO INTEIRO POSITIVO TAL  
QUE  $x^\alpha \in H$ . Daí,  $\underline{\lambda} = 0$ . com ISSO

$$y = x^{q\alpha + \underline{\lambda}} = x^{q\alpha + 0} = (x^\alpha)^q = b^q \in [b].$$

LOGO,  $y \in [b]$ .

Pontanto,

$$H = [\underline{b}] \quad \#$$

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ .

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$  se existir um inteiro  $h > 0$

## Definição

*Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$  se existir um inteiro  $h > 0$  tal que*

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$  se existir um inteiro  $h > 0$  tal que

1)  $\underline{x}^h = e$

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$  se existir um inteiro  $h > 0$  tal que

- 1)  $x^h = e$
- 2)  $\underline{x^r} \neq e$

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$  se existir um inteiro  $h > 0$  tal que

- 1)  $x^h = e$
- 2)  $x^r \neq e$  qualquer que seja o inteiro  $r$

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$  se existir um inteiro  $h > 0$  tal que

- 1)  $x^h = e$
- 2)  $x^r \neq e$  qualquer que seja o inteiro  $r$  tal que  $0 < r < h$

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$  se existir um inteiro  $h > 0$  tal que

- 1)  $x^h = e$
- 2)  $x^r \neq e$  qualquer que seja o inteiro  $r$  tal que  $0 < r < h$

diremos que a ordem

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$  se existir um inteiro  $h > 0$  tal que

- 1)  $x^h = e$
- 2)  $x^r \neq e$  qualquer que seja o inteiro  $r$  tal que  $0 < r < h$

diremos que a **ordem** ou período

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$  se existir um inteiro  $h > 0$  tal que

- 1)  $x^h = e$
- 2)  $x^r \neq e$  qualquer que seja o inteiro  $r$  tal que  $0 < r < h$

diremos que a **ordem** ou **período** de  $x$  é  $h$ .

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$  se existir um inteiro  $h > 0$  tal que

- 1)  $x^h = e$
- 2)  $x^r \neq e$  qualquer que seja o inteiro  $r$  tal que  $0 < r < h$

diremos que a **ordem** ou **período** de  $x$  é  $h$ . Nesse caso escreveremos

$$\underline{|x|} =$$

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$  se existir um inteiro  $\underline{h > 0}$  tal que

- $\left. \begin{array}{l} 1) x^h = e \\ 2) x^{\underline{r}} \neq e \text{ qualquer que seja o inteiro } r \text{ tal que } 0 < r < h \end{array} \right\}$

diremos que a **ordem** ou **período** de  $x$  é  $h$ . Nesse caso escreveremos  $|x| = \underline{o(x)} = h$ .

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$  se existir um inteiro  $h > 0$  tal que

- 1)  $x^h = e$
- 2)  $x^r \neq e$  qualquer que seja o inteiro  $r$  tal que  $0 < r < h$

diremos que a **ordem** ou **período** de  $x$  é  $h$ . Nesse caso escreveremos  $|x| = o(x) = h$ .

Se para qualquer inteiro

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$  se existir um inteiro  $h > 0$  tal que

- | 1)  $x^h = e$
- | 2)  $x^r \neq e$  qualquer que seja o inteiro  $r$  tal que  $0 < r < h$

diremos que a **ordem** ou **período** de  $x$  é  $h$ . Nesse caso escreveremos  $|x| = o(x) = h$ .

Se para qualquer inteiro  $r \neq 0$ ,

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$  se existir um inteiro  $h > 0$  tal que

- 1)  $x^h = e$
- 2)  $x^r \neq e$  qualquer que seja o inteiro  $r$  tal que  $0 < r < h$

diremos que a **ordem** ou **período** de  $x$  é  $h$ . Nesse caso escreveremos  $|x| = o(x) = h$ .

Se para qualquer inteiro  $r \neq 0$ ,  $x^r \neq e$ ,

## Definição

Seja  $G$  um grupo com elemento neutro  $e$ . Dado  $x \in G$  se existir um inteiro  $h > 0$  tal que

- 1)  $x^h = e$
- 2)  $x^r \neq e$  qualquer que seja o inteiro  $r$  tal que  $0 < r < h$

diremos que a **ordem** ou **período** de  $x$  é  $h$ . Nesse caso escreveremos  $|x| = o(x) = h$ .

Se para qualquer inteiro  $r \neq 0$ ,  $x^r \neq e$ , diremos que a **ordem** de  $x$  é zero.

$$\overset{\circ}{x}$$

## Exemplos

1) No grupo multiplicativo  $\mathbb{C}^*$  temos:

$$\Theta(\zeta) = \zeta ; \quad \zeta^4 = 1$$

$$\Theta(i) = i \quad \text{pois}$$

$$i^0 = 1; \quad i^1 = i, \quad i^2 = -1, \quad i^3 = -i, \quad i^4 = 1$$

$$\Theta(-i) = i$$

$$2i \in \mathbb{C}^* \Leftrightarrow \theta(2i) = 0$$

$$(2i)^k = 2^k \cdot i^k \neq 1 \quad ; \quad \forall k \in \mathbb{Z}$$

$$\text{lo g}_0 \theta(2i) = 0$$

## Exemplos

2) Em  $S_3$  temos:

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}; \quad a \neq e$$

$$a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\theta(a) = 2$$

$$b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$b^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$b^2 \cdot b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

$$\operatorname{o}(b) = 3.$$

$$x^h ; \underline{h}x$$

## Exemplos

3) Em  $\mathbb{Z}_5$  temos:

$$\bar{0}; \theta(\bar{0}) = \bar{0}$$

$$\bar{1}; \bar{1} + \bar{1} \neq \bar{0}; \bar{1} + \bar{1} + \bar{1} \neq \bar{0}, \bar{1} + \bar{1} + \bar{1} + \bar{1} \neq \bar{0}$$

$$\bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{0}$$

$$\theta(\bar{1}) = \bar{5}$$

$$\theta(\bar{z}) = \bar{s} = \theta(\bar{z}) = \theta(\bar{q}) \quad (?)$$

## Exemplos

4) Em  $\mathbb{Z}$

## Exemplos

4) Em  $\mathbb{Z}$  o único elemento de ordem diferente de zero

## Exemplos

4) Em  $\mathbb{Z}$  o único elemento de ordem diferente de zero é o elemento neutro.

$$0, \theta(0) = 1$$

## Proposição

Seja  $x$  um elemento de ordem  $\underline{h} > 0$

h

## Proposição

*Seja  $x$  um elemento de ordem  $h > 0$  de um grupo  $\underline{G}$ .*

## Proposição

Seja  $x$  um elemento de ordem  $h > 0$  de um grupo  $G$ . Então  $a^m = e$

## Proposição

Seja  $x$  um elemento de ordem  $h > 0$  de um grupo  $G$ . Então  $a^m = e$  se, e somente se,  $h \mid m$ .  $m = h k$

$$m = h \cdot l + o$$

Prova: i) Se  $a^m = e$ , então  $h|m$ .

→ ii) Se  $h|m$ , então  $a^m = e$ .

Para prova (ii), suponha que  $\theta(a) = h$  é  $h|m$ .

Da: EXISTE  $n \in \mathbb{Z}$  TAL QUE

$$m = h \cdot h \cdot \log$$

$$a^m = a^{h \cdot h} = (a^h)^h = e^h = e.$$

PARA PROVAR (i) SUPONHA

$$\text{que } \ln(a) = h \Leftrightarrow a^m = e.$$

COMO  $h > 0$ , PODEMOS EFETUAR

A DIVISÃO INTEIRA DE  $m$  POR  $h$ .

Assim

$$m = hq + r \leftarrow$$

com  $0 \leq r < h$ .

ou;

$$\boxed{r} = a^m = a^{hq+r} = a^{hq} \cdot a^r$$

$$= (a^h)^q \cdot a^r = e \cdot a^r = \boxed{a^r}$$

Assim  $a^r = e$ , MAS  $\vartheta(a) = h \in$   
 $0 \leq r < h$ . LOGO,  $r = 0 \in \text{ENTAS}$

$$m = hq$$

ou SEJA,  $h | m$ . #