

# Grupos Cíclicos

José Antônio O. Freitas

MAT-UnB

28 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

$$x * y =$$

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

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

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



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  $(G, *) = (G, +)$ .

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

$$x * y =$$

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  $x^{-1}$

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  $x \in G$



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  $-x$ .

Seja  $G$  um grupo multiplicativo

Seja  $G$  um grupo multiplicativo e denote por  $e$  o elemento neutro de  $G$ .

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:

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

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:

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

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

$$x^m$$

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

$$x^m$$

e definido por:

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



## Exemplos

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

## Exemplos

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

## Exemplos

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

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

## Exemplos

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

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

Então:

## Exemplos

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

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

Então:

## Exemplos

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

## Exemplos

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

## Exemplos

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



## Exemplos

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

## 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:

## Proposição

*Seja  $G$  um grupo multiplicativo.*

## Proposição

*Seja  $G$  um grupo multiplicativo. Se  $m$  e  $n$  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*

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

## 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*

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

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

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

## Proposição

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

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

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

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

$$4) \ x^m x^n =$$

## Proposição

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

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

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

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

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



## Proposição

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

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

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

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

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

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

## 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  $e$  o elemento neutro de  $G$ .

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

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

$$m \cdot x$$

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:

$$m \cdot x =$$

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:

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

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:

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

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:

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

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:

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

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:

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

## 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*

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

## Proposição

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

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

## Proposição

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

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

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

## Proposição

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

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

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

## Proposição

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

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

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

$$3) \ n \cdot (m \cdot x) =$$

## Proposição

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

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

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

$$3) \ n \cdot (m \cdot x) = (nm) \cdot x$$



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

$$[x] =$$

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

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

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

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

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

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



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  $[a]$*

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  $[a]$  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  $[a]$  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  $[a]$  é um subgrupo de  $G$ .*
- 2) Se  $H$  é um subgrupo de  $G$  tal que  $a \in H$ ,*

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  $[a]$  é um subgrupo de  $G$ .*
- 2) Se  $H$  é um subgrupo de  $G$  tal que  $a \in H$ , então  $[a] \subset H$ .*

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  $[a]$  é um subgrupo de  $G$ .*
- 2) Se  $H$  é um subgrupo de  $G$  tal que  $a \in H$ , então  $[a] \subset H$ .*



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

$$G = [x].$$

## Definição

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

$$G = [x].$$

Nessas condições, o elemento  $x$

## Definição

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

$$G = [x].$$

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

## Definição

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

$$G = [x].$$

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



## Exemplos

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

## Exemplos

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

## Exemplos

- 1) No grupo multiplicativo  $\mathbb{C}^*$ , encontre o subgrupo gerado por  $i$ .
- 2) No grupo  $S_3$ ,

## Exemplos

- 1) No grupo multiplicativo  $\mathbb{C}^*$ , encontre o subgrupo gerado por  $i$ .
- 2) No grupo  $S_3$ , encontre o subgrupo gerado por

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

## Proposição

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

## Proposição

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

## 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*

$$1) \ x^h = e$$

## Definição

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

$$1) x^h = e$$

$$2) x^r \neq e$$

## 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

$$1) x^h = e$$

$$2) x^r \neq e \text{ qualquer que seja o inteiro } r \text{ tal que } 0 < r < h$$

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

$$1) x^h = e$$

$$2) x^r \neq e \text{ qualquer que seja o inteiro } r \text{ tal que } 0 < r < h$$

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

## Definição

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

$$1) x^h = e$$

$$2) x^r \neq e \text{ qualquer que seja o inteiro } r \text{ tal que } 0 < r < h$$

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

## Definição

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

$$1) x^h = e$$

$$2) x^r \neq e \text{ qualquer que seja o inteiro } r \text{ tal que } 0 < r < h$$

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

$$1) x^h = e$$

$$2) x^r \neq e \text{ qualquer que seja o inteiro } r \text{ tal que } 0 < r < h$$

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

$$1) x^h = e$$

$$2) x^r \neq e \text{ qualquer que seja o inteiro } r \text{ tal que } 0 < r < h$$

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**.

## Definição

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

$$1) x^h = e$$

$$2) x^r \neq e \text{ qualquer que seja o inteiro } r \text{ tal que } 0 < r < h$$

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**.



## Exemplos

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

## Exemplos

- 1) No grupo multiplicativo  $\mathbb{C}^*$  temos:
- 2) Em  $S_3$  temos:

## Exemplos

- 1) No grupo multiplicativo  $\mathbb{C}^*$  temos:
- 2) Em  $S_3$  temos:
- 3) Em  $\mathbb{Z}_5$  temos:

## Exemplos

- 1) No grupo multiplicativo  $\mathbb{C}^*$  temos:
- 2) Em  $S_3$  temos:
- 3) Em  $\mathbb{Z}_5$  temos:
- 4) Em  $\mathbb{Z}$

## Exemplos

- 1) *No grupo multiplicativo  $\mathbb{C}^*$  temos:*
- 2) *Em  $S_3$  temos:*
- 3) *Em  $\mathbb{Z}_5$  temos:*
- 4) *Em  $\mathbb{Z}$  o único elemento de ordem diferente de zero*

## Exemplos

- 1) No grupo multiplicativo  $\mathbb{C}^*$  temos:
- 2) Em  $S_3$  temos:
- 3) Em  $\mathbb{Z}_5$  temos:
- 4) Em  $\mathbb{Z}$  o único elemento de ordem diferente de zero é o elemento neutro.

## Exemplos

- 1) No grupo multiplicativo  $\mathbb{C}^*$  temos:
- 2) Em  $S_3$  temos:
- 3) Em  $\mathbb{Z}_5$  temos:
- 4) Em  $\mathbb{Z}$  o único elemento de ordem diferente de zero é o elemento neutro.

## Proposição

*Seja  $x$  um elemento de ordem  $h > 0$*



## Proposição

*Seja  $x$  um elemento de ordem  $h > 0$  de um grupo  $G$ .*

## 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,  $h \mid m$ .*

## Proposição

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