# Grupos Cíclicos

José Antônio O. Freitas

MAT-UnB

29 de outubro de 2020





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



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



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



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

$$x * y =$$



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

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



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, \*) =



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, +).



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



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

$$x * y =$$



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



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  $x \in G$ 



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  $x^{-1}$ 



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



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  $x \in G$ 



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,







x<sup>m</sup>



 $x^{m}$ 

e definido por:

e definido por:

$$x^m =$$

e definido por:

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

e definido por:

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



e definido por:

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



e definido por:

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



e definido por:

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



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



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



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

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



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

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

Então:



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



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



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



3) No grupo multiplicativo  $S_3$ 



3) No grupo multiplicativo  $S_3$  seja

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



3) No grupo multiplicativo  $S_3$  seja

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

Então:



Seja G um grupo multiplicativo.



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







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



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



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



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

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



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



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



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



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



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



- 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





 $m \cdot x$ 



$$m \cdot x$$

$$m \cdot x =$$

$$m \cdot x$$

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

$$m \cdot x$$

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



$$m \cdot x$$

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



$$m \cdot x$$

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



$$m \cdot x$$

e definido por:

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

8 / 20



Seja G um grupo aditivo.



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





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



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



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

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



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

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



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

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

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



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  $x \in G$ . Denote por [x]





$$[x] =$$



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



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



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



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

# Proposição

Seja G um grupo multiplicativo



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

## Proposição



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

# Proposição

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

1) O subconjunto [a]



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

# Proposição

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

1) O subconjunto [a] é um subgrupo de G.



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

## Proposição

- 1) O subconjunto [a] é um subgrupo de G.
- 2) Se H é um subgrupo de G



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

## Proposição

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



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

#### Proposição

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



Um grupo multiplicativo G



Um grupo multiplicativo G será chamado de grupo cíclico



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



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



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

$$G = [x].$$



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

$$G = [x].$$

Nessas condições, o elemento x



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.



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



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



2) No grupo  $S_3$ ,



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

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



Todo subgrupo de um grupo cíclico é também cíclico.



Seja G um grupo com elemento neutro e.



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



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





1) 
$$x^h = e$$



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



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



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



- 1)  $x^h = e^{-x^h}$
- 2)  $x^r \neq e$  qualquer que seja o inteiro r tal que 0 < r < h diremos que a **ordem**



- 1)  $x^h = e^{-x^h}$
- 2)  $x^r \neq e$  qualquer que seja o inteiro r tal que 0 < r < h diremos que a **ordem** ou **período**



- 1)  $x^h = e^{-x^h}$
- 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.



- 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| = 1



- 1)  $x^h = e^{-x^h}$
- 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.



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

- 1)  $x^h = e^{-x^h}$
- 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



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

- 1)  $x^h = e^{-x^h}$
- 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  $r \neq 0$ ,



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

- 1)  $x^h = e^{-x^h}$
- 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  $r \neq 0$ ,  $x^r \neq e$ ,



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**.



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



2) Em S<sub>3</sub> temos:



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



# Exemplos 4) $Em \mathbb{Z}$



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



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



Seja x um elemento de ordem h > 0





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



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



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