Grupos Cíclicos

José Antônio O. Freitas

MAT-UnB





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^{m}



 x^{m}

$$x^{m}$$

$$x^m =$$

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

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

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

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

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



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



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

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

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

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

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

Então:



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



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



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



iii) No grupo multiplicativo S_3



iii) No grupo multiplicativo S₃ seja

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

iii) No grupo multiplicativo S₃ 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





$$i) x^m x^n =$$



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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$iv) x^m x^n =$$

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

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

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

$$iv) x^m x^n = x^n x^m$$



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





$$m \cdot x$$

$$m \cdot x$$

$$m \cdot x =$$

$$m \cdot x$$

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

$$m \cdot x$$

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

$$m \cdot x$$

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

$$m \cdot x$$

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

$$m \cdot x$$

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



Seja G um grupo aditivo.



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





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



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

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

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



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

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

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

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

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

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

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

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



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 $x \in G$.

i) O subconjunto [x]



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

Proposição

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

i) O subconjunto [x] é um subgrupo de G.



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

Proposição

- i) O subconjunto [x] é um subgrupo de G.
- ii) Se H é um subgrupo de G



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

Proposição

- i) O subconjunto [x] é um subgrupo de G.
- ii) Se H é um subgrupo de G tal que $x \in H$,



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

Proposição

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



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.



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



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



ii) No grupo S_3 ,



ii) 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



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



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

i)
$$x^h = e$$



<u>Definição</u>

- i) $x^h = e$
- ii) $x^r \neq e$



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



- *i*) $x^{h} = e$
- ii) $x^r \neq e$ qualquer que seja o inteiro r tal que 0 < r < h



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



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



- *i*) $x^{h} = e$
- ii) $x^r \neq e$ qualquer que seja o inteiro r tal que 0 < r < h diremos que a **ordem** ou **período** de x é h.



- *i*) $x^{h} = e$
- ii) $x^r \neq e$ 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



- *i*) $x^{h} = e$
- ii) $x^r \neq e$ 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

- *i*) $x^{h} = e$
- ii) $x^r \neq e$ 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

- *i*) $x^{h} = e$
- ii) $x^r \neq e$ 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

- i) $x^h = e$
- ii) $x^r \neq e$ 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

- i) $x^h = e$
- ii) $x^r \neq e$ 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**.



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



ii) Em S₃ temos:



iii) Em \mathbb{Z}_5 temos:



iv) Em \mathbb{Z}



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



iv) 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 $x^m = e$



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