

# Subgrupos

José Antônio O. Freitas

MAT-UnB

28 de outubro de 2020

## Definição

Seja  $(G, *)$  um grupo.

## Definição

Seja  $(G, *)$  um grupo. Se  $\underline{G}$  é um conjunto com uma quantidade finita de elementos,

## Definição

Seja  $(G, *)$  um grupo. Se  $G$  é um conjunto com uma quantidade finita de elementos, dizemos que  $G$  é um grupo finito.

## Definição

Seja  $(G, *)$  um grupo. Se  $G$  é um conjunto com uma quantidade finita de elementos, dizemos que  $G$  é um **grupo finito**. Denotamos por  $|G|$

## Definição

Seja  $(G, *)$  um grupo. Se  $G$  é um conjunto com uma quantidade finita de elementos, dizemos que  $G$  é um **grupo finito**. Denotamos por  $|G|$  o número de elementos de  $G$

## Definição

Seja  $(G, *)$  um grupo. Se  $G$  é um conjunto com uma quantidade finita de elementos, dizemos que  $G$  é um **grupo finito**. Denotamos por  $|G|$  o número de elementos de  $G$  e que será chamado de ordem de  $G$

## Definição

Seja  $(G, *)$  um grupo. Se  $G$  é um conjunto com uma quantidade finita de elementos, dizemos que  $G$  é um **grupo finito**. Denotamos por  $|G|$  o número de elementos de  $G$  e que será chamado de **ordem** de  $G$  ou **cardinalidade** de  $G$ .

## Definição

Seja  $(G, *)$  um grupo. Se  $G$  é um conjunto com uma quantidade finita de elementos, dizemos que  $G$  é um **grupo finito**. Denotamos por  $|G|$  o número de elementos de  $G$  e que será chamado de **ordem** de  $G$  ou **cardinalidade** de  $G$ . Quando o conjunto  $G$  não é finito,

## Definição

Seja  $(G, *)$  um grupo. Se  $G$  é um conjunto com uma quantidade finita de elementos, dizemos que  $G$  é um **grupo finito**. Denotamos por  $|G|$  o número de elementos de  $G$  e que será chamado de **ordem** de  $G$  ou **cardinalidade** de  $G$ . Quando o conjunto  $G$  não é finito, dizemos que  $G$  é um **grupo infinito**.

## Definição

Seja  $(G, *)$  um grupo. Se  $G$  é um conjunto com uma quantidade finita de elementos, dizemos que  $G$  é um **grupo finito**. Denotamos por  $|G|$  o número de elementos de  $G$  e que será chamado de **ordem** de  $G$  ou **cardinalidade** de  $G$ . Quando o conjunto  $G$  não é finito, dizemos que  $G$  é um **grupo infinito**.

## Exemplos

1)  $(\underline{\mathbb{Z}_m}, \underline{+})$  é um grupo finito para todo  $m > 1$

## Definição

Seja  $(G, *)$  um grupo. Se  $G$  é um conjunto com uma quantidade finita de elementos, dizemos que  $G$  é um **grupo finito**. Denotamos por  $|G|$  o número de elementos de  $G$  e que será chamado de **ordem** de  $G$  ou **cardinalidade** de  $G$ . Quando o conjunto  $G$  não é finito, dizemos que  $G$  é um **grupo infinito**.

## Exemplos

1)  $(\mathbb{Z}_m, +)$  é um grupo finito para todo  $m > 1$  e  $|G| = \underline{m}$ .

## Definição

Seja  $(G, *)$  um grupo. Se  $G$  é um conjunto com uma quantidade finita de elementos, dizemos que  $G$  é um **grupo finito**. Denotamos por  $|G|$  o número de elementos de  $G$  e que será chamado de **ordem** de  $G$  ou **cardinalidade** de  $G$ . Quando o conjunto  $G$  não é finito, dizemos que  $G$  é um **grupo infinito**.

## Exemplos

- 1)  $(\mathbb{Z}_m, +)$  é um grupo finito para todo  $m > 1$  e  $|G| = m$ .
- 2)  $(S_m, \circ)$  é um grupo finito

$$\{\underline{1, 2, \dots, m}\} \sim !$$

## Definição

Seja  $(G, *)$  um grupo. Se  $G$  é um conjunto com uma quantidade finita de elementos, dizemos que  $G$  é um **grupo finito**. Denotamos por  $|G|$  o número de elementos de  $G$  e que será chamado de **ordem** de  $G$  ou **cardinalidade** de  $G$ . Quando o conjunto  $G$  não é finito, dizemos que  $G$  é um **grupo infinito**.

## Exemplos

- 1)  $(\mathbb{Z}_m, +)$  é um grupo finito para todo  $m > 1$  e  $|G| = m$ .
- 2)  $(S_n, \circ)$  é um grupo finito e  $|G| = n!$  elementos.

## Definição

Seja  $(G, *)$  um grupo. Se  $G$  é um conjunto com uma quantidade finita de elementos, dizemos que  $G$  é um **grupo finito**. Denotamos por  $|G|$  o número de elementos de  $G$  e que será chamado de **ordem** de  $G$  ou **cardinalidade** de  $G$ . Quando o conjunto  $G$  não é finito, dizemos que  $G$  é um **grupo infinito**.

## Exemplos

- 1)  $(\mathbb{Z}_m, +)$  é um grupo finito para todo  $m > 1$  e  $|G| = \underline{m}$ .
- 2)  $(S_n, \circ)$  é um grupo finito e  $|G| = n!$  elementos.
- 3)  $(\mathbb{Z}, +)$  é um grupo infinito.

## Definição

Seja  $(G, *)$  um grupo.

## Definição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio

## Definição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $\underline{H} \subseteq \underline{G}$

## Definição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é chamado de **subgrupo** de  $G$

## Definição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é chamado de **subgrupo** de  $G$  se, e somente se,  $(H, *)$

$x, y \in H \Rightarrow x * y \in H$ .

## Definição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é chamado de **subgrupo** de  $G$  se, e somente se,  $(H, *)$  é um grupo.

$(G, *)$  é GRUPO SE:

i) PARA TODOS  $x, y, z \in G$ ;  $(x * y) * z = x * (y * z)$

ii) EXISTE  $e \in G$  TAL QUE  $x * e = x = e * x$

PARA TODO  $x \in G$ .

iii) PARA CADA  $x \in G$ . EXISTE  $y \in G$  TAL QUE  $x * y = e = y * x$ .

## Definição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é chamado de **subgrupo** de  $G$  se, e somente se,  $(H, *)$  é um grupo.

## Proposição

Seja  $\underline{(G, *)}$  um grupo.

## Definição

*Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é chamado de **subgrupo** de  $G$  se, e somente se,  $(H, *)$  é um grupo.*

## Proposição

*Seja  $(G, *)$  um grupo. Um subconjunto não vazio*

## Definição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é chamado de **subgrupo** de  $G$  se, e somente se,  $(H, *)$  é um grupo.

## Proposição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é um subgrupo de  $G$

## Definição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é chamado de **subgrupo** de  $G$  se, e somente se,  $(H, *)$  é um grupo.

## Proposição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é um subgrupo de  $G$  se, e somente se

## Definição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é chamado de **subgrupo** de  $G$  se, e somente se,  $(H, *)$  é um grupo.

## Proposição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é um subgrupo de  $G$  se, e somente se

- i)  $x^{-1} \in H$ ,

## Definição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é chamado de **subgrupo** de  $G$  se, e somente se,  $(H, *)$  é um grupo.

## Proposição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é um subgrupo de  $G$  se, e somente se

- i)  $x^{-1} \in H$ , para todo  $x \in H$ ;
- ii)  $x * y \in H$ ,

## Definição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é chamado de **subgrupo** de  $G$  se, e somente se,  $(H, *)$  é um grupo.

## Proposição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é um subgrupo de  $G$  se, e somente se

- i)  $x^{-1} \in H$ , para todo  $x \in H$ ;
- ii)  $x * y \in H$ , para todos  $x, y \in H$ .

- X

## Definição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é chamado de **subgrupo** de  $G$  se, e somente se,  $(H, *)$  é um grupo.

## Proposição

Seja  $(G, *)$  um grupo. Um subconjunto não vazio  $H \subseteq G$  é um subgrupo de  $G$  se, e somente se

- i)  $x^{-1} \in H$ , para todo  $x \in H$ ;
- ii)  $x * y \in H$ , para todos  $x, y \in H$ .

$$\left\{ \begin{array}{l} i) x^{-1} \in H, \text{ para todo } x \in H; \\ ii) x * y \in H, \text{ para todos } x, y \in H. \end{array} \right.$$

**PARA TODO**  
 $x, y \in H$ .

PROVA: Precisamos mostrar que

1) Se  $H$  é subgrupos, então

i)  $x^{-1} \in H$ , para todos  $x \in H$

ii)  $x * y \in H$ , para todos  $x, y \in H$

$(H, *)$  é grupo.

2) SE  
 {  
   → i)  $\bar{x} \in H$ , PARA TODO  $x \in H$   
   ii)  $x, y \in H$ , PARA TODO  $x, y \in H$   
 ENTÃO  $(H, +)$  É GRUPO.

A PROVA DE (i) É SIMPLESMENTE UMA CONSEQUÊNCIA DA DEFINIÇÃO DE SUBGRUPO.

Vamos mostrar (2) então.

Da condição (ii) segue que a operação \* é uma operação binária em  $H$ .

Como  $(G, *)$  é grupo, então a operação \* é associativa em

$G$ ,  $\circ$  como  $H \subseteq G$ , ELA TAMBÉM  
É ASSOCIATIVA EM  $H$ .

COMO  $H \neq \emptyset$ , SEJA  $x \in H$ .  
AGORA, DE (ii) SEGUÉ  $a \in$

$$x * x^{-1} \in H$$

Pois  $x^{-1} \in H$ . Assim

$$c = x * \overset{\sim}{x} \in H$$

ISTO É,  $e \in H$ .

PONTAVÍDO,  $(H, *)$  É GRUPO,

DU SEJA,  $H$  É UM SUBGRUPO  
DE  $G$ . #

## Exemplos

1) Dado  $(G, *)$  grupo,

## Exemplos

1) Dado  $(G, *)$  grupo,  $H = \{e\}$

## Exemplos

1) Dado  $(G, *)$  grupo,  $H = \{e\}$  e  $\underline{H = G}$

## Exemplos

1) Dado  $(G, *)$  grupo,  $H = \{e\}$  e  $H = G$  são subgrupos de  $G$ ,

## Exemplos

- 1) Dado  $(G, *)$  grupo,  $H = \{e\}$  e  $H = G$  são subgrupos de  $G$ , chamados de subgrupos triviais.

## Exemplos

- 1) Dado  $(G, *)$  grupo,  $H = \{e\}$  e  $H = G$  são subgrupos de  $G$ , chamados de **subgrupos triviais**.
- 2) Seja  $(\mathbb{Z}, +)$  um grupo.

## Exemplos

1) Dado  $(G, *)$  grupo,  $H = \{e\}$  e  $H = G$  são subgrupos de  $G$ , chamados de **subgrupos triviais**.

2) Seja  $(\mathbb{Z}, +)$  um grupo. Tomando  $\underline{H} = \underline{\underline{m\mathbb{Z}}}$ ,

$$\left\{ \underline{\underline{m n}} \mid n \in \mathbb{Z} \right\}$$

## Exemplos

- 1) Dado  $(G, *)$  grupo,  $H = \{e\}$  e  $H = G$  são subgrupos de  $G$ , chamados de **subgrupos triviais**.
- 2) Seja  $(\mathbb{Z}, \underline{+})$  um grupo. Tomando  $H = \underline{m\mathbb{Z}}$ , onde  $\underline{m > 1}$ , então  $H$  é subgrupo de  $\mathbb{Z}$ .

2) COMO  $0 = m \cdot 0$ , ENTAJ $\bar{e}$   $0 \in \mathbb{H}$ .

DADO  $x \in m\mathbb{Z}$ . ENTAJ $\bar{e}$  EXISTE  
 $h \in \mathbb{Z}$  TAL QUE  
 $x = mh$ .

AGORA,

$$-x = - (mh) = m(-h) \in m\mathbb{Z}$$

DA' -  $x \in \mathbb{Z}$ , PRA TUDO  $x \in \mathbb{Z}$ .

FINALMENTE, SEJA  $n, x, y \in \mathbb{Z}$ ,  
ASSIM EXISTEM  $n, l \in \mathbb{Z}$  TAIS QUE

$$x = m n$$

$$y = m l$$

DA'

$$x+y = mn + ml = m(n+l) \in m\mathbb{Z}.$$

PORTANTO,  $H = m\mathbb{Z}$  é um SUBGRUPO  
DE  $\mathbb{Z}$ .

## Exemplos

- 1) Dado  $(G, *)$  grupo,  $H = \{e\}$  e  $H = G$  são subgrupos de  $G$ , chamados de **subgrupos triviais**.
- 2) Seja  $(\mathbb{Z}, +)$  um grupo. Tomando  $H = m\mathbb{Z}$ , onde  $m > 1$ , então  $H$  é subgrupo de  $\mathbb{Z}$ .
- 3)  $G = U(\mathbb{Z}_8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ .

## Exemplos

- 1) Dado  $(G, *)$  grupo,  $H = \{e\}$  e  $H = G$  são subgrupos de  $G$ , chamados de **subgrupos triviais**.
- 2) Seja  $(\mathbb{Z}, +)$  um grupo. Tomando  $H = m\mathbb{Z}$ , onde  $m > 1$ , então  $H$  é subgrupo de  $\mathbb{Z}$ .
- 3)  $G = U(\mathbb{Z}_8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ . Então  $(G, \odot)$  é um grupo

## Exemplos

- 1) Dado  $(G, *)$  grupo,  $H = \{e\}$  e  $H = G$  são subgrupos de  $G$ , chamados de **subgrupos triviais**.
- 2) Seja  $(\mathbb{Z}, +)$  um grupo. Tomando  $H = m\mathbb{Z}$ , onde  $m > 1$ , então  $H$  é subgrupo de  $\mathbb{Z}$ .
- 3)  $G = U(\mathbb{Z}_8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ . Então  $(G, \odot)$  é um grupo com  $|G| = 4$ .

## Exemplos

- 1) Dado  $(G, *)$  grupo,  $H = \{e\}$  e  $H = G$  são subgrupos de  $G$ , chamados de **subgrupos triviais**.
- 2) Seja  $(\mathbb{Z}, +)$  um grupo. Tomando  $H = m\mathbb{Z}$ , onde  $m > 1$ , então  $H$  é subgrupo de  $\mathbb{Z}$ .
- 3)  $G = U(\mathbb{Z}_8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ . Então  $(G, \odot)$  é um grupo com  $|G| = 4$ . Além disso,

## Exemplos

- 1) Dado  $(G, *)$  grupo,  $H = \{e\}$  e  $H = G$  são subgrupos de  $G$ , chamados de **subgrupos triviais**.
- 2) Seja  $(\mathbb{Z}, +)$  um grupo. Tomando  $H = m\mathbb{Z}$ , onde  $m > 1$ , então  $H$  é subgrupo de  $\mathbb{Z}$ .
- 3)  $G = U(\mathbb{Z}_8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ . Então  $(G, \odot)$  é um grupo com  $|G| = 4$ . Além disso,

$$H_1 = \{\bar{1}, \bar{3}\} \quad (\text{c}), (\text{c})$$

## Exemplos

- 1) Dado  $(G, *)$  grupo,  $H = \{e\}$  e  $H = G$  são subgrupos de  $G$ , chamados de **subgrupos triviais**.
- 2) Seja  $(\mathbb{Z}, +)$  um grupo. Tomando  $H = m\mathbb{Z}$ , onde  $m > 1$ , então  $H$  é subgrupo de  $\mathbb{Z}$ .
- 3)  $G = U(\mathbb{Z}_8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ . Então  $(G, \odot)$  é um grupo com  $|G| = 4$ . Além disso,

$$\begin{aligned}H_1 &= \{\bar{1}, \bar{3}\} \\H_2 &= \{\bar{1}, \bar{5}\}\end{aligned}$$

## Exemplos

- 1) Dado  $(G, *)$  grupo,  $H = \{e\}$  e  $H = G$  são subgrupos de  $G$ , chamados de **subgrupos triviais**.
- 2) Seja  $(\mathbb{Z}, +)$  um grupo. Tomando  $H = m\mathbb{Z}$ , onde  $m > 1$ , então  $H$  é subgrupo de  $\mathbb{Z}$ .
- 3)  $G = U(\mathbb{Z}_8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ . Então  $(G, \odot)$  é um grupo com  $|G| = 4$ . Além disso,

$$\left\{ \begin{array}{l} H_1 = \{\bar{1}, \bar{3}\} \\ H_2 = \{\bar{1}, \bar{5}\} \\ H_3 = \{\bar{1}, \bar{7}\} \end{array} \right.$$

## Exemplos

- 1) Dado  $(G, *)$  grupo,  $H = \{e\}$  e  $H = G$  são subgrupos de  $G$ , chamados de **subgrupos triviais**.
- 2) Seja  $(\mathbb{Z}, +)$  um grupo. Tomando  $H = m\mathbb{Z}$ , onde  $m > 1$ , então  $H$  é subgrupo de  $\mathbb{Z}$ .
- 3)  $G = U(\mathbb{Z}_8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ . Então  $(G, \odot)$  é um grupo com  $|G| = 4$ . Além disso,

$$\begin{array}{ll} H_1 = \{\bar{1}, \bar{3}\} & \rightarrow H \subseteq G \\ H_2 = \{\bar{1}, \bar{5}\} & \\ H_3 = \{\bar{1}, \bar{7}\} & |H| = 3 \end{array}$$

São subgrupos de  $G$ .

## Exemplos

4) Considere o grupo aditivo  $M_2(\mathbb{R})$ .

## Exemplos

4) Considere o grupo aditivo  $M_2(\mathbb{R})$ . Mostre que o conjunto

## Exemplos

4) Considere o grupo aditivo  $M_2(\mathbb{R})$ . Mostre que o conjunto

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}) \mid a + d = 0 \right\}$$

## Exemplos

4) Considere o grupo aditivo  $M_2(\mathbb{R})$ . Mostre que o conjunto

$\cancel{\emptyset} \neq H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}) \mid a + d = 0 \right\}$

é um subgrupo de  $M_2(\mathbb{R})$ .

Painéis,  $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in H$ , Pois  $0+0=0$ .

LOGO,  $A \neq \emptyset$ .

SEJA  $A \in H$ . LOGO

$$-A = \begin{pmatrix} -x & -y \\ -z & -t \end{pmatrix} \text{ com } -(x+t) = 0.$$

AGORA

$$-A = \begin{pmatrix} -x & -y \\ -y & -t \end{pmatrix}$$

E DA:  $-x - t = -(x + t) = 0$ . com

ISSO  $-A \in H$ .

POIS ULTIMO SEJA M  $A, B \in H$ .

DA:

$$A = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \text{ com } x+t=0$$

$$B = \begin{pmatrix} \alpha & \beta \\ r & s \end{pmatrix} \text{ com } \alpha+s=0.$$

LG,

$$A + B = \begin{pmatrix} x+\alpha & y+\beta \\ z+\gamma & t+\delta \end{pmatrix}$$

$$\begin{aligned} \bar{t} \\ (x+\alpha) + (t+\delta) &= (x+t) + (\alpha+\delta) \\ &= 0+0=0 \end{aligned}$$

LJO,  $A + B \in H$ .

PONTANEO.  $H$  é SUBGRUPO

DE  $M_2(\mathbb{R})$ .

Seja  $(G, *)$  um grupo.

Seja  $(G, \underline{*})$  um grupo. Para simplificar a notação

Seja  $(G, *)$  um grupo. Para simplificar a notação vamos adotar uma notação multiplicativa

Seja  $(G, *)$  um grupo. Para simplificar a notação vamos adotar uma notação multiplicativa e escrever  $(\underline{G}, \underline{*}) =$

Seja  $(G, *)$  um grupo. Para simplificar a notação vamos adotar uma notação multiplicativa e escrever  $(G, *) = (G, \cdot)$ .

Seja  $(G, *)$  um grupo. Para simplificar a notação vamos adotar uma notação multiplicativa e escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

Seja  $(G, *)$  um grupo. Para simplificar a notação vamos adotar uma notação multiplicativa e escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

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

Seja  $(G, *)$  um grupo. Para simplificar a notação vamos adotar uma notação multiplicativa e escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

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

Seja  $(G, *)$  um grupo. Para simplificar a notação vamos adotar uma notação multiplicativa e escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

$$\textcolor{red}{x * y} = x \cdot y = \textcolor{red}{\cancel{x}} \textcolor{red}{y}$$

$$\textcolor{red}{f \circ g} = fg$$

Seja  $(G, *)$  um grupo. Para simplificar a notação vamos adotar uma notação multiplicativa e escrever  $(G, *) = (G, \cdot)$ . Assim, dados  $x, y \in G$  vamos denotar

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

Nesse caso vamos dizer simplesmente que  $\boxed{G}$  é um grupo.

## Proposição

*Seja  $G$  um grupo.*

## Proposição

Seja  $G$  um grupo. Dado  $H \subset G$  um subgrupo

## Proposição

*Seja  $G$  um grupo. Dado  $H \subset G$  um subgrupo defina*

## Proposição

Seja  $G$  um grupo. Dado  $H \subset G$  um subgrupo defina

$$\underline{x \sim y}$$

## Proposição

*Seja  $G$  um grupo. Dado  $H \subset G$  um subgrupo defina*

*$x \sim y$  se, e somente se,*

## Proposição

Seja  $G$  um grupo. Dado  $H \subset G$  um subgrupo defina

$x \sim y$  se, e somente se,  $\underline{x^{-1}y} \in \underline{H}$

## Proposição

Seja  $G$  um grupo. Dado  $H \subset G$  um subgrupo defina

$\cancel{x \sim y \text{ se, e somente se, }} \underbrace{x^{-1}y \in H}_{\cancel{\text{}}}$

para todos  $x, y \in G$ .

## Proposição

Seja  $G$  um grupo. Dado  $H \subset G$  um subgrupo defina

$$x \sim y \text{ se, e somente se, } x^{-1}y \in H$$

para todos  $x, y \in G$ .

- 1) A relação  $\sim$

## Proposição

Seja  $G$  um grupo. Dado  $H \subset G$  um subgrupo defina

$$x \sim y \text{ se, e somente se, } x^{-1}y \in H$$

para todos  $x, y \in G$ .

- 1) A relação  $\sim$  sobre  $G$  definida acima é uma relação de equivalência.

## Proposição

Seja  $G$  um grupo. Dado  $H \subset G$  um subgrupo defina

$$x \sim y \text{ se, e somente se, } x^{-1}y \in H$$

para todos  $x, y \in G$ .

- 1) A relação  $\sim$  sobre  $G$  definida acima é uma relação de equivalência.
- 2) Se  $a \in G$ ,

## Proposição

Seja  $G$  um grupo. Dado  $H \subset G$  um subgrupo defina

$$x \sim y \text{ se, e somente se, } x^{-1}y \in H$$

para todos  $x, y \in G$ .

- 1) A relação  $\sim$  sobre  $G$  definida acima é uma relação de equivalência.
- 2) Se  $a \in G$ , então a classe de equivalência determinada por  $a$

## Proposição

Seja  $G$  um grupo. Dado  $H \subset G$  um subgrupo defina

$$x \sim y \text{ se, e somente se, } x^{-1}y \in H$$

para todos  $x, y \in G$ .

- 1) A relação  $\sim$  sobre  $G$  definida acima é uma relação de equivalência.
- 2) Se  $a \in G$ , então a classe de equivalência determinada por  $a$  é o conjunto

## Proposição

Seja  $G$  um grupo. Dado  $H \subset G$  um subgrupo defina

$$x \sim y \text{ se, e somente se, } x^{-1}y \in H$$

para todos  $x, y \in G$ .

- 1) A relação  $\sim$  sobre  $G$  definida acima é uma relação de equivalência.
- 2) Se  $\underline{a} \in G$ , então a classe de equivalência determinada por  $a$  é o conjunto

$$\underline{\underline{aH}} =$$

## Proposição

Seja  $G$  um grupo. Dado  $H \subset G$  um subgrupo defina

$$x \sim y \text{ se, e somente se, } x^{-1}y \in H$$

para todos  $x, y \in G$ .

- 1) A relação  $\sim$  sobre  $G$  definida acima é uma relação de equivalência.
- 2) Se  $a \in G$ , então a classe de equivalência determinada por  $a$  é o conjunto

$$\underline{aH} = \{ah\}$$

## Proposição

Seja  $G$  um grupo. Dado  $H \subset G$  um subgrupo defina

$x \sim y$  se, e somente se,  $\underline{x^{-1}y} \in H$

para todos  $x, y \in G$ .

$$\underline{y} \xrightarrow{x^{-1}} \underline{Hx}$$

- 1) A relação  $\sim$  sobre  $G$  definida acima é uma relação de equivalência.
- 2) Se  $a \in G$ , então a classe de equivalência determinada por  $a$  é o conjunto

$$\rightarrow aH = \{ah \mid h \in H\}.$$

$aH$  É CLASSE LATERAL 'A' DIREITA  
nórdulo  $H$ .

$e = \bar{x}x \in H?$

$\bar{y}x \in H?$

PROVA: 1)  $x \sim x, \forall x \in G$

SE  $x \sim y$ , ENTÃO  $y \sim x$ .

SE  $x \sim y \wedge y \sim z$ , ENTÃO  $x \sim z$ .

Primeiro, DADO  $x \in G$ . como  $\bar{x}x \in H$

$H$  é SUBGRUPO, ENTÃO  $e \in H \in$

$$H \ni e = \bar{x}x$$

LOGO,  $x \sim x$ .

$$y^{-1}x \rightarrow l \in H$$

AGORA SUPONHA QUE  $x \sim y$ . DA:

$$x^{-1}y \in H$$

ISTO É,

$$x^{-1}y = l$$

ONDE  $\underline{l} \in H$ ! ASSIM  $\underline{l}^{-1} \in H$  E

$$H \ni \underline{l} = (\overset{\rightarrow}{x} \overset{\rightarrow}{y}) = \overset{\rightarrow}{y} (\overset{\rightarrow}{x}^{-1})^{-1} =$$

$$= \underline{y^{-1}x}$$

ESTO E,  $\underline{y^{-1}x} \in H$ . LOGO,  $y \sim x$ .

SUPONHA QUE  $x \sim y \in y \sim j$ . DI

$$\underline{x^{-1}y \in H} \quad \underline{y^{-1}j \in H}.$$

ASSim

$$(x^{-1}y)(y^{-1}z) \in H$$

$$x^{-1} \underbrace{(y y^{-1})}_e z \in H$$

$$x^{-1}z \in H.$$

$E$  ént̄o  $x \sim j$ .

PONTANT<sup>9</sup>, A RELAÇÃO  $\sim$  É

DE FATO UMA RELAÇÃO DE

EQUIVALÊNCIA EM  $G$ .

v) SEJA  $a \in G$ . Daí,

$$\bar{a} = \{x \in G \mid x \sim a\} \stackrel{\subseteq}{=} aH$$

SEJA  $x \in \bar{a}$ . Daí  $x \sim a$ , ISTO  
é,  $x^{-1}a \in H$ . LOGO, EXISTE  $\underline{l} \in H$   
TAL QUAI

$$x^{-1}a = l$$

$$x = \underline{q} \underline{l}^{-1}$$

com ISSO,  $x \in \underline{a} H$ .

AGORA SETA  $y \in \underline{a} H$ . LOGO

EXISTE  $t \in H$  TAL QUE

$$y = \underline{q} t$$

DA:

$$\bar{a}^{-1}y = t \in H$$

ISTO É,  $a \sim y$ . ASSIM  $y \in \bar{a}$ .

POR TANTO,  $\bar{a} = aH$ . #

## Proposição

Seja  $H$  um subgrupo de um grupo  $G$ .

## Proposição

*Seja  $H$  um subgrupo de um grupo  $G$ . Então duas classes laterais quaisquer*

## Proposição

*Seja  $H$  um subgrupo de um grupo  $G$ . Então duas classes laterais quaisquer módulo  $H$*

## Proposição

*Seja  $H$  um subgrupo de um grupo  $G$ . Então duas classes laterais quaisquer módulo  $H$  são subconjuntos de  $G$  que possuem a mesma cardinalidade,*

$$\underline{aH}, \underline{bH}$$

$$f: \underline{aH} \rightarrow \underline{bH}$$

$\downarrow$

## Proposição

Seja  $H$  um subgrupo de um grupo  $G$ . Então duas classes laterais quaisquer módulo  $H$  são subconjuntos de  $G$  que possuem a mesma cardinalidade, isto é, a mesma quantidade de elementos.

$$\underline{aH}, \underline{eH} = \{ \underline{el} \mid l \in H \} = \boxed{\underline{H}}$$

$|H|$

$$aH = \{al \mid l \in H\}$$

$$bH = \{bl \mid l \in H\}$$

PROVA: DADA'S DUAS CLASSE QUAISquer  
 $aH \in bH$ , VAMOS MOSTRAR QUE SEM-  
PRE É POSSÍVEL DEFINIR UM A  
FUNÇÃO  $f: aH \rightarrow bH$  QUE É BIJETORA.



PARA ISSO, DEFINA  $f: aH \rightarrow bH$  POR  
 $f(al) = bl$ ;  $l \in H$ .

Se  $\forall$   $a$   $l_1 = l_2$   $\epsilon aH$  TAis  $\Theta$   $\cup E$

$$f(l_1) = f(l_2)$$

$\Delta i$

$$\alpha(b^{-1}) bl_1 = bl_2$$

$$b^{-1} b l_1 = b^{-1} bl_2$$

$$\underline{l_1} = \underline{l_2}$$

$$x \in \mathbb{H} : f(x) = bt$$
$$at = x = al \quad ; \quad f(al) = bt \Leftrightarrow bl = bt \Leftrightarrow l = t$$

Então  $al_1 = al_2$ . Isso é,  $f$

é INJETORA.

AGORA, SEJA  $bt \in b\mathbb{H}$ . TOME  
 $at \in a\mathbb{H}$  É ASSIM

$$f(at) = bt$$

Logo,  $f$  é sobrejetora.

Pontanto,  $f$  é bijetora e

com isso os conjuntos A e  
B possuem exatamente a  
mesma quantidade de elemen-

TOS E ESSA QANTIDADE É 11).

#

## Exemplos

1) No grupo multiplicativo  $G = \{1, -1, i, -i\}$ ,

## Exemplos

1) No grupo multiplicativo  $G = \{1, -1, i, -i\}$ , onde  $i^2 = -1$ .

## Exemplos

1) No grupo multiplicativo  $G = \{1, -1, i, -i\}$ , onde  $i^2 = -1$ . Considere o conjunto  $H = \{1, \underline{-1}\}$ .

## Exemplos

1) No grupo multiplicativo  $G = \{1, -1, i, -i\}$ , onde  $i^2 = -1$ . Considere o conjunto  $H = \{1, -1\}$ . Então  $H$  é um subgrupo de  $G$

$$aH \cap bH = \emptyset \text{ ou } \underline{aH = bH}$$

$$\Rightarrow aH = Ha \text{ se } G \text{ é comutativo.}$$

## Exemplos

1) No grupo multiplicativo  $G = \{1, -1, i, -i\}$ , onde  $i^2 = -1$ . Considere o conjunto  $H = \{1, -1\}$ . Então  $H$  é um subgrupo de  $G$  e as classes laterais serão:

$$1H = H = \{1, -1\}$$

$$iH = \{il \mid l \in H\} = \{i, -i\}$$

EXISTEM DUAS CLASSES LATERAIS  
que são:  $H + iH$

$aH : Ha$

$$IH = H \cdot L$$

$$Hi = \{li \mid l \in H\} = \{i, -i\} = iH$$

## Exemplos

2) Considero o grupo multiplicativo  $\mathbb{R}^*$

## Exemplos

2) Considere o grupo multiplicativo  $\mathbb{R}^*$  e  $H = \{x \in \mathbb{R}^* \mid x > 0\}$

## Exemplos

2) Considere o grupo multiplicativo  $\mathbb{R}^*$  e  $H = \{x \in \mathbb{R}^* \mid x > 0\} \subset \mathbb{R}^*$ .

## Exemplos

2) Considere o grupo multiplicativo  $\mathbb{R}^*$  e  $H = \{x \in \mathbb{R}^* \mid x > 0\} \subset \mathbb{R}^*$ .  
 Então  $H$  é subgrupo de  $\mathbb{R}^*$

$$z \in H.$$

$$x \in H; \text{ Daí } x > 0 \in z > 0, \text{ logo } \frac{z}{x} \in H.$$

$$x, y \in H, \text{ Daí } x > 0 \in y > 0, \text{ logo } xy > 0 \in xy \in H.$$

$$H^+ = H \cap \{x \in \mathbb{R}^* \mid x > 0\}$$

$$a \in \mathbb{R}^* ; aH = \left\{ \underbrace{al}_{\in H} \mid l \in H \right\}$$

Se  $a > 0$ , also  $a > 0$ . PAMA TOOS  $l \in H$   
EST DAI  $al \in H$ . LOGO

$$aH = H, a > 0.$$

SE  $a < 0$ ,  $a \neq 0$ , PATA TOSO

$\{x \in \mathbb{R}^* \mid x < 0\}$

$$aH = \{x \in \mathbb{R}^* \mid x < 0\}; a \neq 0.$$

LOGO EXISTEM DUAS CLASSES

(ATENÇÃO:  $H \in aH$ , com  $a < 0$ .

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

## Exemplos

3) Considere agora o grupo simétrico  $\underline{G = S_3}$ .

## Exemplos

3) Considere agora o grupo simétrico  $G = S_3$ . Denote por

## Exemplos

3) Considere agora o grupo simétrico  $G = S_3$ . Denote por

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

## Exemplos

3) Considere agora o grupo simétrico  $G = S_3$ . Denote por

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

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

## Exemplos

3) Considere agora o grupo simétrico  $G = S_3$ . Denote por

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

Fica como exercício verificar que  $\{\underline{e}, \underline{a}, \underline{a^2}, \underline{b}, \underline{ba}, \underline{ba^2}\} =$

## Exemplos

3) Considere agora o grupo simétrico  $G = S_3$ . Denote por

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

Fica como exercício verificar que  $\{e, a, a^2, b, ba, ba^2\} = \underline{S_3}$ .

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

## Exemplos

3) Considere agora o grupo simétrico  $G = S_3$ . Denote por

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

Fica como exercício verificar que  $\{\text{id}, a, a^2, b, ba, ba^2\} = S_3$ . Aqui e é a função identidade,

## Exemplos

3) Considere agora o grupo simétrico  $G = S_3$ . Denote por

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

Fica como exercício verificar que  $\{e, a, a^2, b, ba, ba^2\} = S_3$ . Aqui  $e$  é a função identidade,  $a^2 = \underline{a \circ a}$ ,

## Exemplos

3) Considere agora o grupo simétrico  $G = S_3$ . Denote por

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

Fica como exercício verificar que  $\{e, a, a^2, b, ba, ba^2\} = S_3$ . Aqui  $e$  é a função identidade,  $a^2 = a \circ a$ ,  $ba = b \circ a$  e

## Exemplos

3) Considere agora o grupo simétrico  $G = S_3$ . Denote por

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

Fica como exercício verificar que  $\{e, a, a^2, b, ba, ba^2\} = S_3$ . Aqui  $e$  é a função identidade,  $a^2 = a \circ a$ ,  $ba = b \circ a$  e  $ba^2 = \underline{b} \circ (\underline{a} \circ a)$ .

## Exemplos

3) Considere agora o grupo simétrico  $G = S_3$ . Denote por

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

Fica como exercício verificar que  $\{e, a, a^2, b, ba, ba^2\} = S_3$ . Aqui  $e$  é a função identidade,  $a^2 = a \circ a$ ,  $ba = b \circ a$  e  $ba^2 = b \circ (a \circ a)$ . Seja  $H = \{e, a, a^2\}$ .

## Exemplos

3) Considere agora o grupo simétrico  $G = S_3$ . Denote por

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

Fica como exercício verificar que  $\{e, a, a^2, b, ba, ba^2\} = S_3$ . Aqui  $e$  é a função identidade,  $a^2 = a \circ a$ ,  $ba = b \circ a$  e  $ba^2 = b \circ (a \circ a)$ . Seja  $H = \{e, \underline{a}, \underline{a^2}\}$ . Então  $H$  é subgrupo de  $S_3$

## Exemplos

3) Considere agora o grupo simétrico  $G = S_3$ . Denote por

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

Fica como exercício verificar que  $\{e, a, a^2, b, ba, ba^2\} = S_3$ . Aqui  $e$  é a função identidade,  $a^2 = a \circ a$ ,  $ba = b \circ a$  e  $ba^2 = b \circ (a \circ a)$ . Seja  
→  $H = \{\underline{e}, \underline{a}, \underline{a^2}\}$ . Então  $H$  é subgrupo de  $S_3$  e as classes laterais serão:

$$\underline{a}^2 \cdot \underline{a} = (\underline{a}^2 \cdot a) \cdot a = e \cdot a = a$$

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

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

$\overset{c}{\underset{n}{\text{?}}}$

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

AS CLASSES LATÉNAIS SÃO:

$$eH = H^e$$

$$bH = \{ bl \mid l \in H \} = \{ be, ba, ba^2 \}$$

$$b^*H = \{ b, \cancel{ba}, \cancel{ba^2} \}$$

$$Hb = \{ b, \cancel{ab}, \cancel{a^2b} \}$$

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

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

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

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