Subgrupos

José Antônio O. Freitas

MAT-UnB



Seja (G, *) um grupo.



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



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



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|



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



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



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.



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,



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**.



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

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

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

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

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**.

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

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**.

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

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**.

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



Seja (G, *) um grupo.



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



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



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





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.



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.



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



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 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 chamado de **subgrupo** de G se, e somente se, (H,*) é um grupo.

Proposição

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

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

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

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

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

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

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



i) Dado (G,*) grupo,





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



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



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



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

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

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

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

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

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

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

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

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

$$H_1=\{\overline{1},\overline{3}\}$$

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

$$H_1 = \{\overline{1}, \overline{3}\}$$

$$H_2 = \{\overline{1}, \overline{5}\}$$

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

$$H_1 = \{\overline{1}, \overline{3}\}\$$

 $H_2 = \{\overline{1}, \overline{5}\}\$
 $H_3 = \{\overline{1}, \overline{7}\}\$

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

$$H_1 = \{\overline{1}, \overline{3}\}$$

 $H_2 = \{\overline{1}, \overline{5}\}$
 $H_3 = \{\overline{1}, \overline{7}\}$

São subgrupos de G.



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



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

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

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

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

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

 \acute{e} um subgrupo de $M_2(\mathbb{R})$.



Seja (G, *) um grupo.



Seja (G,*) 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 (G,*) =



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





$$x * y =$$



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



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



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

Nesse caso vamos dizer simplesmente que G é um grupo.



Seja G um grupo.





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



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



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

 $x \sim y$



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

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



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

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



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

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



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

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

para todos x, $y \in G$.

i) A relação \sim



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

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

para todos $x, y \in G$.

i) A relação \sim sobre G definida acima é uma relação de equivalência.



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

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

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



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

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

- i) A relação \sim sobre G definida acima é uma relação de equivalência.
- ii) Se a ∈ G, então a classe de equivalência determinada por a



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

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

- i) A relação \sim sobre G definida acima é uma relação de equivalência.
- ii) Se a ∈ G, então a classe de equivalência determinada por a é o conjunto



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

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

- i) A relação \sim sobre G definida acima é uma relação de equivalência.
- ii) Se a ∈ G, então a classe de equivalência determinada por a é o conjunto

$$aH =$$



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

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

para todos $x, y \in G$.

- i) A relação ~ sobre G definida acima é uma relação de equivalência.
- ii) Se a ∈ G, então a classe de equivalência determinada por a é o conjunto

$$aH = \{ah$$



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

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

para todos x, $y \in G$.

- i) A relação \sim sobre G definida acima é uma relação de equivalência.
- ii) Se a ∈ G, então a classe de equivalência determinada por a é o conjunto

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



Seja H um subgrupo de um grupo G.



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



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



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



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.



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.



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



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

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



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



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



ii) Considere o grupo multiplicativo \mathbb{R}^*



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



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



ii) 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}^*



ii) 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}^* e as classes laterais serão:



iii) Considere agora o grupo simétrico $G = S_3$.



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



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

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



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

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



iii) 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 $\{e, a, a^2, b, ba, ba^2\}$ =

iii) 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 $\{e, a, a^2, b, ba, ba^2\} = S_3$.

iii) 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,

iii) 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, $a^2 = a \circ a$,

iii) 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

iii) 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 $ba^2=b\circ (a\circ a)$.

iii) 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 $H = \{e, a, a^2\}$.

iii) 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 $H = \{e, a, a^2\}$. Então H é subgrupo de S_3

iii) 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 $H = \{e, a, a^2\}$. Então H é subgrupo de S_3 e as classes laterais serão: