# Subgrupos

José Antônio O. Freitas

MAT-UnB

28 de outubro de 2020



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

1)  $(\mathbb{Z}_m,+)$  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

1)  $(\mathbb{Z}_m, +)$  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**.

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

- 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.



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**.

- 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.
- 3)  $(\mathbb{Z},+)$  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

3/11



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

3/11



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,  $y \in H$ .



1) Dado (G,\*) grupo,



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





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



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



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

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



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



- 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  $\mathbb{Z}$ .

- 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)  $G = U(\mathbb{Z}_8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}.$

- 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)  $G = U(\mathbb{Z}_8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ . Então  $(G, \odot)$  é um grupo

- 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)  $G = U(\mathbb{Z}_8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ . Então  $(G, \odot)$  é um grupo com |G| = 4.

- 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)  $G = U(\mathbb{Z}_8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ . Então  $(G, \odot)$  é um grupo com |G| = 4. Além disso,

- 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)  $G=U(\mathbb{Z}_8)=\{\overline{1},\overline{3},\overline{5},\overline{7}\}$ . Então  $(G,\odot)$  é um grupo com |G|=4. Além disso,

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

- 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)  $G = U(\mathbb{Z}_8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ . Então  $(G, \odot)$  é um grupo com |G| = 4. Além disso,

$$H_1 = \{\overline{1}, \overline{3}\}\$$
  
 $H_2 = \{\overline{1}, \overline{5}\}\$ 

- 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)  $G=U(\mathbb{Z}_8)=\{\overline{1},\overline{3},\overline{5},\overline{7}\}$ . Então  $(G,\odot)$  é um grupo com |G|=4. Além disso,

$$H_1 = \{\overline{1}, \overline{3}\}$$
  
 $H_2 = \{\overline{1}, \overline{5}\}$   
 $H_3 = \{\overline{1}, \overline{7}\}$ 

- 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)  $G=U(\mathbb{Z}_8)=\{\overline{1},\overline{3},\overline{5},\overline{7}\}$ . 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.



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



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



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

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



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

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

é 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,  $y \in G$ .

1) 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,  $y \in G$ .

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

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



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

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

- 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



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

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

- 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



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

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

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

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

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



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



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



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



1) 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



1) 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:



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



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



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



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



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



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



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



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

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



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

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



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  $\{e, a, a^2, b, ba, ba^2\}$ 



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



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,



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



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



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



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



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



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