Teorema de Lagrange

José Antônio O. Freitas

MAT-UnB

$S_3 \ncong \mathbb{Z}_6$; $G \cong \mathbb{Z}_4$; $[a] \cong \mathbb{Z}_m$

Seja G um grupo finito.

$\to G = \bigcup_{x \in G} xH$; xH ; yH $\to xH = yH$ ou

$\to xH \cap yH = \emptyset$

Seja G um grupo finito. Se H é um subgrupo de G,

$x \sim y \Leftrightarrow xy^{-1} \in H$ É UMA RELAÇÃO DE EQUIVALÊNCIA EM G

$\to xH$; $x \in G$

Seja G um grupo finito. Se H é um subgrupo de G, então existirá uma quantidade finita de classes laterais módulo H

Seja G um grupo finito. Se H é um subgrupo de G, então existirá uma quantidade finita de classes laterais módulo H . Assim o conjunto

$$G/H = \{aH \mid a \in G\}$$

Seja G um grupo finito. Se H é um subgrupo de G, então existirá uma quantidade finita de classes laterais módulo H . Assim o conjunto

$$G/H = \{aH \mid a \in G\}$$

é finito.

Seja G um grupo finito. Se H é um subgrupo de G, então existirá uma quantidade finita de classes laterais módulo H . Assim o conjunto

$$G/H = \{aH \mid a \in G\}$$

é finito.
O número de elementos de G/H

Seja G um grupo finito. Se H é um subgrupo de G, então existirá uma quantidade finita de classes laterais módulo H . Assim o conjunto

$$G/H = \{aH \mid a \in G\}$$

é finito.
O número de elementos de G/H é chamado de **índice**

Seja G um grupo finito. Se H é um subgrupo de G, então existirá uma quantidade finita de classes laterais módulo H . Assim o conjunto

$$G/H = \{aH \mid a \in G\}$$

é finito.
O número de elementos de G/H é chamado de **índice** de H em G

Seja G um grupo finito. Se H é um subgrupo de G, então existirá uma quantidade finita de classes laterais módulo H . Assim o conjunto

$$G/H = \{aH \mid a \in G\}$$

é finito.

O número de elementos de G/H é chamado de **índice** de H em G e será denotado por

$$\boxed{[G:H]} = |G/H|. = (G:H)$$

Exemplos

(1) Seja $G = \{1, -1, i, -i\}$ *um grupo*

Exemplos

(1) Seja $G = \{1, -1, i, -i\}$ *um grupo e* $N = \{1, -1\}$

Exemplos

(1) Seja $G = \{1, -1, i, -i\}$ *um grupo e* $N = \{1, -1\}$ *um subgrupo de G.*

Exemplos

(1) Seja $G = \{1, -1, i, -i\}$ *um grupo e* $N = \{1, -1\}$ *um subgrupo de* G*. Já vimos que as classes laterais de* N *em* G *são*

Exemplos

(1) Seja $G = \{1, -1, i, -i\}$ *um grupo e* $N = \{1, -1\}$ *um subgrupo de* G*. Já vimos que as classes laterais de* N *em* G *são*

$$N \quad e \quad iN.$$

Exemplos

(1) *Seja* $G = \{1, -1, i, -i\}$ *um grupo e* $N = \{1, -1\}$ *um subgrupo de* G. *Já vimos que as classes laterais de* N *em* G *são*

$$N \quad e \quad iN.$$

Daí

$$G/N = \{N, iN\}$$

EXISTE H EM G T.Q

→ $|H| = 3$ É SUBGRUPO? NÃO

Exemplos

(1) *Seja* $G = \{1, -1, i, -i\}$ *um grupo e* $N = \{1, -1\}$ *um subgrupo de* G. *Já vimos que as classes laterais de* N *em* G *são*

$$N \quad e \quad iN.$$

Daí

$$G/N = \{N, iN\}$$

e assim $[G : H] = 2$.

Exemplos

(2) *Seja* $G = S_3$.

Exemplos

(2) Seja $G = S_3$*. Já vimos que se tomamos*

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

Exemplos

(2) Seja $G = S_3$. Já vimos que se tomamos

$$Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Exemplos

(2) Seja $G = S_3$. *Já vimos que se tomamos*

$$Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad e \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

então

$$S_3 = \{Id, f, f^2, g, gf, gf^2\}.$$

Exemplos

(2) Seja $G = S_3$. Já vimos que se tomamos

$$Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad e \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

então

$$S_3 = \{Id, f, f^2, g, gf, gf^2\}.$$

Considere o subgrupo $H = [\ g\ ]$

Exemplos

(2) Seja $G = S_3$*. Já vimos que se tomamos*

$$Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad e \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

então

$$S_3 = \{Id, f, f^2, g, gf, gf^2\}.$$

Considere o subgrupo $H = [\, g\,] = \{Id, g\}$*. Então* H *possui* 3 *classes laterais que são*

$$H, \ fH, \ f^2H.$$

Exemplos

(2) Seja $G = S_3$. *Já vimos que se tomamos*

$$Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad e \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

então

$$S_3 = \{Id, f, f^2, g, gf, gf^2\}.$$

Considere o subgrupo $H = [\ g\ ] = \{Id, g\}$. *Então* H *possui 3 classes laterais que são*

$$H, \ fH, \ f^2H.$$

Daí

$$\underline{G/H} = \{\underline{H, fH, f^2H}\}$$

$|S_n| = n!$; $|H| = 2$

Exemplos

(2) Seja $G = S_3$. Já vimos que se tomamos

$$Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad e \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

então

$$S_3 = \{Id, f, f^2, g, gf, gf^2\}.$$

Considere o subgrupo $H = [\, g \,] = \{Id, g\}$. Então H possui 3 classes laterais que são

$$H, \; fH, \; f^2H.$$

Daí

$$G/H = \{H, fH, f^2H\}$$

e então $[G : H] = 3$.

Teorema (Teorema de Lagrange)

Seja H um subgrupo

Teorema (Teorema de Lagrange)

Seja H um subgrupo de um grupo finito G.

Teorema (Teorema de Lagrange)

Seja H um subgrupo de um grupo finito G. Então $o(G) = o(H)[G : H]$

Teorema (Teorema de Lagrange)

Seja H um subgrupo de um grupo finito G. Então $o(G) = o(H)[G : H]$ e, portanto, $o(H)|o(G)$.

PROVA: SEJA $\boxed{H}$ UM SUBGRUPO DE UM GRUPO FINITO G. DENOTE $[G:H]=n$. ASSIM

$$G/H = \{a_1H, a_2H, \ldots, a_nH\}$$

Com

$\rightarrow a_i H \cap a_j H = \phi$

SEMPRE QUE $a_i \neq a_j$.

ALÉM DISSO,

$$\underline{G} = \underline{a_1 H} \cup \underline{a_2 H} \cup \dots \cup \underline{a_n}H.$$

E COMO TODAS AS CLASSES DE EQUIVALÊNCIA MÓDULO H POSSUEM A MESMA QUANTIDADE DE ELE- MENTOS E ESSA QUANTIDADE É

IGUAL À ORDEM H, $o(H)$, ENTÃO

$$o(G) = o(a_1H) + o(a_2H) + \dots + o(a_rH)$$

$$o(G) = \underbrace{o(H) + o(H) + \dots + o(H)}_{r \text{ PARCELAS}}$$

LOGO,

$$o(G) = \overset{[G:H]}{\overset{\shortparallel}{r}} \cdot o(H),$$

OU SEJA,

$$o(G) = [G:H]\, o(H)$$

PORTANTO, $\underline{o(H)} \mid \underline{o(G)}$. #

$\{1,2,3\ 4\}$

Observação:

No grupo S_4

Observação:

No grupo S_4 considere o seguinte subconjunto:

Observação:

No grupo S_4 considere o seguinte subconjunto:

$$L = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ \underline{1} & \underline{2} & \underline{3} & \underline{4} \end{pmatrix}, \right.$$

$4! = 24$

Observação:

No grupo S_4 considere o seguinte subconjunto:

$$L = \left\{ \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}}_{2}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \right\}.$$

Observação:

No grupo S_4 considere o seguinte subconjunto:

$$L = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \right\}.$$

Observe que o número de elementos de L

Observação:

No grupo S_4 considere o seguinte subconjunto:

$$L = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \right\}.$$

Observe que o número de elementos de $\underset{\substack{\| \\ 2}}{L}$ *divide* $\underline{|S_4|} = 4! = \underline{24}$

$L \neq \emptyset$, $x \in L \Rightarrow x^{-1} \in L$; $x, y \in L \Rightarrow xy \in L$

MAT-UnB

Observação:

No grupo S_4 considere o seguinte subconjunto:

$$L = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \right\}.$$

Observe que o número de elementos de L divide $|S_4| = 4! = 24$ mas L não é um subgrupo de S_4

Observação:

No grupo S_4 considere o seguinte subconjunto:

$$L = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \right\}.$$

Observe que o número de elementos de L divide $|S_4| = 4! = 24$ mas L não é um subgrupo de S_4 pois

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}^{-1}$$

Observação:

No grupo S_4 considere o seguinte subconjunto:

$$L = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \right\}.$$

Observe que o número de elementos de L divide $|S_4| = 4! = 24$ mas L não é um subgrupo de S_4 pois

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

Observação:

No grupo S_4 considere o seguinte subconjunto:

$$L = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \right\}.$$

Observe que o número de elementos de L divide $|S_4| = 4! = 24$ mas L não é um subgrupo de S_4 pois

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \notin L.$$

$x \mid o(G)$

Corolário

Seja G um grupo finito.

Corolário

Seja G um grupo finito. Então a ordem de um elemento $x \in G$

Corolário

Seja G um grupo finito. Então a ordem de um elemento $x \in G$ divide a ordem de G

Corolário

Seja G um grupo finito. Então a ordem de um elemento $x \in G$ divide a ordem de G e o quociente é $[G : H]$,

Corolário

Seja G um grupo finito. Então a ordem de um elemento $x \in G$ divide a ordem de G e o quociente é $[G : H]$, onde $H = [x]$.

PROVA: A ORDEM DE $x \in G$ É IGUAL À ORDEM DO SUBGRUPO $H = [x]$. ASSIM PELO TEOREMA DE LAGRANGE, $o(H) \mid o(G)$

E

$$o(G) = [G:H] \cdot \overset{o(x)}{\overset{\shortparallel}{o(H)}}$$

OU SEJA

$$o(\underset{-}{x}) \mid o(\underset{-}{G}).$$

#

S_4 : $\cancel{o(x) =} \underset{-}{5}$

Corolário

Sejam G um grupo finito

Corolário

Sejam G um grupo finito e $x \in G$.

Corolário

Sejam G um grupo finito e $x \in G$. Então

$$x^{o(G)}$$

Corolário

Sejam G um grupo finito e $x \in G$. Então

$$x^{o(G)} = e,$$

$$x^n = \underbrace{x * x * \cdots * x}_{n} \quad ; \quad \underbrace{x + x + \cdots + x}_{n}$$

Corolário

Sejam G um grupo finito e $x \in G$*. Então*

$$x^{o(G)} = e,$$

onde e denota o elemento neutro de G.

PROVA: SUPONHA QUE A ORDEM DE x É n. ASSIM n É O MENOR INTEIRO ESTRITAMENTE POSITIVO TAL QUE $x^n = e$.

ASSIM DO COROLÁRIO ANTERIOR PODEMOS ESCREVER

$$o(G) = [G:H] \cdot n$$

ONDE $H = [x]$.

Logo

$$x^{\underline{o(G)}} = x^{[G:H].H} = \left(x^{H}\right)^{[G:H]} = e^{[G:H]} = \underline{e}$$

Como queríamos. #

Corolário

Seja G um grupo finito

Corolário

Seja G um grupo finito cuja ordem é um número primo.

$G = [x]$

Corolário

Seja G um grupo finito cuja ordem é um número primo. Então G é um grupo cíclico

Corolário

Seja G um grupo finito cuja ordem é um número primo. Então G é um grupo cíclico e os únicos subgrupos de G

Corolário

Seja G um grupo finito cuja ordem é um número primo. Então G é um grupo cíclico e os únicos subgrupos de G são os triviais,

Corolário

Seja G um grupo finito cuja ordem é um número primo. Então G é um grupo cíclico e os únicos subgrupos de G são os triviais, ou seja, $\{e\}$ e G.

PROVA: SEJA $o(G) = p$, COM p PRIMO.

ASSIM $p > 1$ E DAÍ EXISTE $x \in G$

COM $x \neq e$. SEJA $H = [x]$.

DO TEOREMA DE LAGRANGE

SEGUE QUE

$$o(H) \mid p.$$

DAÍ $o(H) = 1$ OU $o(H) = p$.

ASSIM $H = \{e\}$ OU $H = G$. MAS

$H \neq \{e\}$ pois $x \neq e$. Logo

$$\underline{G} = H = [\underline{x}].$$

e assim G é cíclico.

Agora seja J um subgrupo

DE G. DAÍ PELO TEOREMA DE

LAGRANGE, SEGUE QUE

$$o(J) \mid o(G) = p$$

COM ISSO $o(J) = 1$ OU $o(J) = p$.

LOGO $J = \{e\}$ OU $J = G$,

COMO QUERÍAMOS. #