Teorema de Lagrange

No Contexto de Teoria de Grupos

Marco Busetti

UTFPR

8 de setembro de 2025

Roteiro

Tabela de Conteúdo

A pré-história do Teorema de Lagrange

Lagrange, em seus escritos de 1770/71, introduziu uma ideia importantíssima que, ao longo de um século, se desenvolveu no que hoje conhecemos como Teorema de Lagrange. Embora o teorema moderno conhecido em Teoria de Grupos — que afirma que a ordem de um subgrupo de um grupo finito sempre divide a ordem do grupo — não estivesse presente em seu trabalho original, sua percepção inicial foi o alicerce para essa descoberta fundamental.

Os m-valores para funções de n variáveis

Supondo f uma função bem definida de n entradas, definimos m como o número de diferentes funções obtidas em permutar as n variáveis de entrada. Isto é, os 'valores' de f.

Denotamos:

- $n \rightarrow$ um inteiro positivo;
- $x_1, x_2, x_3, \ldots, x_n \rightarrow n$ variáveis;
- $f(x_1, x_2, x_3, \ldots, x_n) \rightarrow$ uma função avaliada em n variáveis;
- $m \rightarrow$ o número de diferentes funções obtidas via permutação das variáveis $x_1, x_2, x_3, \ldots, x_n$.

Lagrange: Dado n, quais são os diferentes valores que m pode ter?

Valores possíveis para m e a conjectura de Lagrange

n	**m (valores possíveis para f)**
1	1
2	1, 2
3	1, 2, 3, 6
4	1, 2, 3, 4, 6, 8, 12, 24
5	E quanto a esta linha ??

- Na seção 97 de *Réflexions* de Lagrange, é conjecturado:

O número m de valores possíveis para f divide $n!$

Teorema de Lagrange: 1770 e 1870

Teorema de Lagrange 1770: o número m de valores possíveis de uma função de n varíaveis divide $n!$

Teorema de Lagrange 1870: Si le groupe H est contenu dans le groupe G, son ordre n est un diviseur de N, ordre de G.
[Camille Jordan, *Traité des Substitutions et des Équations Algébriques* (1870), p. 25— onde foi dada a origem do nome ao teorema que conhecemos hoje como Teorema de Lagrange.

A pergunta central: Como esses teoremas se conectam??

Tabela de Conteúdo

Operação Binária

Definição

Sejam G e E conjuntos não-vazios e $\oplus$ uma função tal que:

$$\oplus : \begin{array}{c} G \times G \to E \\ (a, b) \mapsto a \oplus b \end{array}$$

Definimos $\oplus$ como uma **operação binária** de dois elementos de G em E.

Operação Binária

Definição

Sejam G e E conjuntos não-vazios e $\oplus$ uma função tal que:

$$\oplus : \begin{array}{c} G \times G \to E \\ (a, b) \mapsto a \oplus b \end{array}$$

Definimos $\oplus$ como uma **operação binária** de dois elementos de G em E.

Definição

Dizemos que $\oplus$ é uma **lei de composição interna** em G se $E = G$.

Definição de Grupo

Definição

Seja G um conjunto não-vazio. Dizemos que $(G, \cdot)$ é um **grupo** se, e somente se, $\cdot$ é uma lei de composição interna em G tal que:

1. **Elemento neutro:** $\exists\, e \in G\ , \forall\, x \in G\ : x \cdot e = e \cdot x = x$
2. **Elemento inverso:** $\forall x \in G, \exists x^{-1} \in G :\ x \cdot x^{-1} = x^{-1} \cdot x = e$
3. **Associatividade:** $\forall\, x, y, z \in G : (x \cdot y) \cdot z = x \cdot (y \cdot z)$

Definição de Grupo

Definição

Seja G um conjunto não-vazio. Dizemos que $(G, \cdot)$ é um **grupo** se, e somente se, $\cdot$ é uma lei de composição interna em G tal que:

1. **Elemento neutro:** $\exists\, e \in G\ , \forall\, x \in G\ : x \cdot e = e \cdot x = x$
2. **Elemento inverso:** $\forall x \in G, \exists x^{-1} \in G :\ x \cdot x^{-1} = x^{-1} \cdot x = e$
3. **Associatividade:** $\forall\, x, y, z \in G : (x \cdot y) \cdot z = x \cdot (y \cdot z)$

Observação: Se $\forall\, (x, y) \in G \times G :\ x \cdot y = y \cdot x$, dizemos que G é um grupo *abeliano* (ou *comutativo*).

Exemplos de Grupos

- $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ - grupos abelianos

Exemplos de Grupos

- $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ - grupos abelianos
- $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$ - grupos abelianos

Exemplos de Grupos

- $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ - grupos abelianos
- $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$ - grupos abelianos
- $(GL_n(\mathbb{K}), \times)$ - grupo das matrizes $n \times n$ invertíveis

Exemplos de Grupos

- $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ - grupos abelianos
- $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$ - grupos abelianos
- $(GL_n(\mathbb{K}), \times)$ - grupo das matrizes $n \times n$ invertíveis
- $(\mathbb{Z}/n\mathbb{Z}, +)$ - grupos cíclicos finitos

Exemplos de Grupos

- $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ - grupos abelianos
- $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$ - grupos abelianos
- $(GL_n(\mathbb{K}), \times)$ - grupo das matrizes $n \times n$ invertíveis
- $(\mathbb{Z}/n\mathbb{Z}, +)$ - grupos cíclicos finitos
- $(\mathbb{Z}_p^*, \odot)$ - grupo multiplicativo módulo p primo

Exemplos de Grupos

- $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ - grupos abelianos
- $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$ - grupos abelianos
- $(GL_n(\mathbb{K}), \times)$ - grupo das matrizes $n \times n$ invertíveis
- $(\mathbb{Z}/n\mathbb{Z}, +)$ - grupos cíclicos finitos
- $(\mathbb{Z}_p^*, \odot)$ - grupo multiplicativo módulo p primo
- S_n - grupo simétrico (permutações de n elementos)

Tabela de Conteúdo

Definição de Subgrupo

Definição

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

Definição de Subgrupo

Definição

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

Teorema

Seja $H \subseteq G$ tal que $H \neq \emptyset$ e $(G, \cdot)$ é um grupo. Então $H \leq G$ se, e somente se:

1. $h_1 \cdot h_2 \in H$, $\forall (h_1, h_2) \in H \times H$
2. $h^{-1} \in H$, $\forall h \in H$

Exemplos de Subgrupos

- G e $\{e\}$ são subgrupos **triviais** de G

Exemplos de Subgrupos

- G e $\{e\}$ são subgrupos **triviais** de G
- $(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$ para todo $n \in \mathbb{Z}$

Exemplos de Subgrupos

- G e $\{e\}$ são subgrupos **triviais** de G
- $(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$ para todo $n \in \mathbb{Z}$
- $SL_n(\mathbb{K}) = \{A \in GL_n(\mathbb{K}) : \det(A) = 1\} \leq GL_n(\mathbb{K})$

Exemplos de Subgrupos

- G e $\{e\}$ são subgrupos **triviais** de G
- $(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$ para todo $n \in \mathbb{Z}$
- $SL_n(\mathbb{K}) = \{A \in GL_n(\mathbb{K}) : \det(A) = 1\} \leq GL_n(\mathbb{K})$
- Centro do grupo: $Z(G) = \{x \in G : xg = gx,\ \forall g \in G\}$

Subgrupo Gerado

Definição

Seja $(G, \cdot)$ um grupo e $X \subseteq G$ não-vazio. O **subgrupo gerado por** X é:

$$\langle X \rangle = \bigcap \{H : H \leq G \text{ e } X \subseteq H\}$$

Subgrupo Gerado

Definição

Seja $(G, \cdot)$ um grupo e $X \subseteq G$ não-vazio. O **subgrupo gerado por** X é:

$$\langle X \rangle = \bigcap \{H : H \leq G \text{ e } X \subseteq H\}$$

Proposição

$$\langle X \rangle = \{x_1 x_2 \dots x_n : x_i \in X \cup X^{-1},\ n \geq 1\}$$

Subgrupo Gerado

Definição

Seja $(G, \cdot)$ um grupo e $X \subseteq G$ não-vazio. O **subgrupo gerado por** X é:

$$\langle X \rangle = \bigcap \{H : H \leq G \text{ e } X \subseteq H\}$$

Proposição

$$\langle X \rangle = \{x_1 x_2 \dots x_n : x_i \in X \cup X^{-1},\ n \geq 1\}$$

Para um único elemento: $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$

Grupos Cíclicos

Definição

Um grupo G é chamado de **cíclico** quando pode ser gerado por um único elemento $a \in G$, isto é, $G = \langle a \rangle$.

Grupos Cíclicos

Definição

Um grupo G é chamado de **cíclico** quando pode ser gerado por um único elemento $a \in G$, isto é, $G = \langle a \rangle$.

Proposição

Se G é um grupo cíclico, então G é abeliano.

Grupos Cíclicos

Definição

Um grupo G é chamado de **cíclico** quando pode ser gerado por um único elemento $a \in G$, isto é, $G = \langle a \rangle$.

Proposição

Se G é um grupo cíclico, então G é abeliano.

Exemplos:

- $\mathbb{Z} = \langle 1 \rangle$
- $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle$

Ordem de Elementos

Definição

Seja $(G, \cdot)$ um grupo.

- A **ordem do grupo** G é $|G|$ (número de elementos)
- A **ordem de um elemento** $\alpha \in G$ é $\mathcal{O}(\alpha) = |\langle \alpha \rangle|$

Ordem de Elementos

Definição

Seja $(G, \cdot)$ um grupo.

- A **ordem do grupo** G é $|G|$ (número de elementos)
- A **ordem de um elemento** $\alpha \in G$ é $\mathcal{O}(\alpha) = |\langle \alpha \rangle|$

Proposição

Seja G um grupo e $\alpha \in G$. São equivalentes:

1. $\mathcal{O}(\alpha) < \infty$
2. $\exists t \in \mathbb{Z}_+^* : \alpha^t = e$ (onde t é minimal)

Tabela de Conteúdo

Classes Laterais

Definição

Seja G um grupo, $H \leq G$ e $x \in G$.

- **Classe lateral à esquerda:** $xH = \{xh : h \in H\}$
- **Classe lateral à direita:** $Hx = \{hx : h \in H\}$

Classes Laterais

Definição

Seja G um grupo, $H \leq G$ e $x \in G$.

- **Classe lateral à esquerda:** $xH = \{xh : h \in H\}$
- **Classe lateral à direita:** $Hx = \{hx : h \in H\}$

Definição

O **índice de H em G** é o número de classes laterais distintas:

$$[G : H] = |\{\text{classes laterais à esquerda de } H\}|$$

Classes Laterais

Definição

Seja G um grupo, $H \leq G$ e $x \in G$.

- **Classe lateral à esquerda:** $xH = \{xh : h \in H\}$
- **Classe lateral à direita:** $Hx = \{hx : h \in H\}$

Definição

O **índice de H em G** é o número de classes laterais distintas:

$$[G : H] = |\{\text{classes laterais à esquerda de } H\}|$$

Propriedade importante: O número de classes laterais à esquerda é igual ao número de classes laterais à direita.

Propriedades das Classes Laterais

Proposição

Seja G um grupo, $H \leq G$ e $x, y \in G$. Então:

1. $x \in xH$ (todo elemento está em sua classe lateral)

Propriedades das Classes Laterais

Proposição

Seja G um grupo, $H \leq G$ e $x, y \in G$. Então:

1. $x \in xH$ (todo elemento está em sua classe lateral)
2. $xH = yH$ se, e somente se, $x^{-1}y \in H$

Propriedades das Classes Laterais

Proposição

Seja G um grupo, $H \leq G$ e $x, y \in G$. Então:

1. $x \in xH$ (todo elemento está em sua classe lateral)
2. $xH = yH$ se, e somente se, $x^{-1}y \in H$
3. Ou $xH = yH$ ou $xH \cap yH = \emptyset$

Propriedades das Classes Laterais

Proposição

Seja G um grupo, $H \leq G$ e $x, y \in G$. Então:

1. $x \in xH$ (todo elemento está em sua classe lateral)
2. $xH = yH$ se, e somente se, $x^{-1}y \in H$
3. Ou $xH = yH$ ou $xH \cap yH = \emptyset$
4. $|xH| = |H|$ para todo $x \in G$

Propriedades das Classes Laterais

Proposição

Seja G um grupo, $H \leq G$ e $x, y \in G$. Então:

1. $x \in xH$ (todo elemento está em sua classe lateral)
2. $xH = yH$ se, e somente se, $x^{-1}y \in H$
3. Ou $xH = yH$ ou $xH \cap yH = \emptyset$
4. $|xH| = |H|$ para todo $x \in G$

Conclusão: As classes laterais formam uma **partição** de G.

Tabela de Conteúdo

Teorema de Lagrange

Teorema de Lagrange

Seja G um grupo finito e H um subgrupo de G.
Então $|H|$ divide $|G|$.
Mais precisamente: $|G| = |H| \cdot [G : H]$

Teorema de Lagrange

Teorema de Lagrange

Seja G um grupo finito e H um subgrupo de G.
Então $|H|$ divide $|G|$.
Mais precisamente: $|G| = |H| \cdot [G : H]$

Ideia da Demonstração:

- As classes laterais de H particionam G
- Cada classe lateral tem cardinalidade $|H|$
- Existem $[G : H]$ classes laterais distintas
- Logo: $|G| = |H| \cdot [G : H]$

Consequências do Teorema de Lagrange

Corolário

Se G é um grupo finito e $\alpha \in G$, então $\mathcal{O}(\alpha)$ divide $|G|$.

Consequências do Teorema de Lagrange

Corolário

Se G é um grupo finito e $\alpha \in G$, então $\mathcal{O}(\alpha)$ divide $|G|$.

Corolário

Se G é um grupo finito de ordem p primo, então G é cíclico.

Consequências do Teorema de Lagrange

Corolário

Se G é um grupo finito e $\alpha \in G$, então $\mathcal{O}(\alpha)$ divide $|G|$.

Corolário

Se G é um grupo finito de ordem p primo, então G é cíclico.

Teorema de Euler

Seja G um grupo finito com $|G| = n$. Então:

$$\forall g \in G, \quad g^n = e$$

Pequeno Teorema de Fermat

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Então:

$$a^{p-1} \equiv 1 \pmod{p}$$

Pequeno Teorema de Fermat

Pequeno Teorema de Fermat

Seja p um número primo e $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Então:

$$a^{p-1} \equiv 1 \pmod{p}$$

Demonstração: Aplicação direta do Teorema de Euler ao grupo $(\mathbb{Z}_p^*, \odot)$, que tem ordem $p - 1$.

Multiplicatividade do Índice

Proposição

Seja G um grupo e sejam $K \leq H \leq G$. Então:

$$[G : K] = [G : H] \cdot [H : K]$$

Multiplicatividade do Índice

Proposição

Seja G um grupo e sejam $K \leq H \leq G$. Então:

$$[G : K] = [G : H] \cdot [H : K]$$

Demonstração: Aplicação sucessiva do Teorema de Lagrange:

$$|G| = |H| \cdot [G : H] \tag{1}$$
$$|H| = |K| \cdot [H : K] \tag{2}$$
$$|G| = |K| \cdot [G : K] \tag{3}$$

Tabela de Conteúdo

Teorema de Lagrange (1770): O número m de valores de uma função f de n variáveis divide n!

Seja $G = S_n$ o grupo de todas as permutações dos elementos em $\{x_1, x_2, \ldots, x_n\}$.
Seja f^g a função obtida ao aplicar a permutação $g \in G$ nas variáveis em f.
Tomemos H como a família de todas as permutações $h \in G$ tais que $f^h = f$.
Logo, H é subgrupo de G e 2 'valores' de f, f^{g_1} e f^{g_2} são iguais se e somente se g_1 e g_2 estão na mesma classe lateral de H.
Portanto, o número de 'valores' de f é o número de classes laterais de H em G e, logo, divide $n!$

□

Tabela de Conteúdo

Obrigado!

Dúvidas?

Referências

- https://m-a.org.uk/resources/downloads/3H-Peter-Neumann-Lagrange-Theorem.pdf
- https://github.com/MARCOVB5/grupos
- GARCIA, Arnaldo; LEQUAIN, Yves. *Elementos de Álgebra*. Rio de Janeiro: IMPA, 2003.