Teorema de Lagrange: Suponhamos $H \leq G$ então para quaisquer dois elementos $a, b \in G$ existe uma bijeção $aH \to bH$ onde:

$$aH = \{ah \mid h \in H\} \text{ e } bH = \{bH \mid h \in H\}$$

$$\psi : aH \to bH$$

Prova: $\psi : aH \to bH$

$$x = ah \to ba^{-1}x = ba^{-1}(ax) = bh$$

ψ é injetiva? ou é sobrejetiva?

"Ajuda a determinar quais subconjuntos de um determinado grupo são ou não subgrupos deste grupo!"

Teorema: Seja G um grupo e H um subgrupo de G. Então ordem de H divide ordem de G. Em particular, denotamos:

$$(G:H) = \frac{|G|}{|H|}$$ (Divisão de $|G| = n \in \mathbb{N}$ e $|H| = n_1 \in \mathbb{N}$

↳ índice de H em G.

Exemplo: Grupo Aditivo $\mathbb{Z}_{10}$.

$H_1 = \{0, 2, 4, 8\}$
$H_2 = \{0, 2, 4\}$
$H_3 = \{0, 8\}$
$H_4 = \{0, 5\}$
$H_5 = \{1, 2, 4, 8, 6\}$
$H_6 = \{0, 2, 4, 6, 8\}$

$\mathbb{Z}_{10} = \{0, 1, 2, \ldots\ldots, 8, 9\}$

Vamos usar o teorema de Lagrange p/ determinar qual dos subconjuntos H_i, não pode ser subgrupos de $\mathbb{Z}_{10}$.

i) $H_1 = \{0, 2, 4, 8\}$ possui ordem 4., e 4 não é divisor de 10.
$H_2 = \{0, 2, 4\}$ possui ordem 3., e 3 não é divisor de 10!

Temos que H_1 e H_2 não são subgrupos de $\mathbb{Z}_{10}$.

ii) Dado $\mathbb{Z}_{10} = \{0, 1, 2, \ldots\ldots, 8, 9\}$ e $H_3 = \{0, 8\}$
$|\mathbb{Z}_{10}| = 10$ $\qquad |H_3| = 2$

a) $|H_3| \,/\, |\mathbb{Z}_{10}|$ V.

b) Ambos deve possuir o mesmo elemento neutro, e $H_3 \neq \emptyset$.

$0 \in H_3$ e $0 \in \mathbb{Z}_{10}$. ✓

c) Todo elemento de $|H_3|$ deve possuir simetrico em $\mathbb{Z}_{10}$, "E também em H_3".

$0 \in H_3 \longrightarrow 0 \in \mathbb{Z}_{10}$ ✓
$8 \in H_3 \longrightarrow 8 = 2 - 10 = -8$. $2 \in \mathbb{Z}_{10}$, mas $2 \notin H_3$
↳ Caso: Temos que H_3 não é subgrupo de $\mathbb{Z}_{10}$.

ii) $\mathbb{Z}_{10} = \{0, 1, \ldots, 8, 9\}$ e $H_4 = \{0, 5\}$

a) $0 \in H_4$ e $0 \in \mathbb{Z}_{10}$, V (condição elemento neutro)

b) $|H_5| \mid |\mathbb{Z}_{10}| \longrightarrow 2 \mid 10$ V.

c) $5 \in H_4$ e $5 \in \mathbb{Z}_{10}$.

$5 = \bar{5} - 10 = -5$, logo H_4 e $\mathbb{Z}_{10}$ possuem o mesmo simétrico.

d) Falta verificar se a operação realizada em quaisquer elemento do conjunto, tem como resultado um elemento do conjunto, ou seja fechado no conjunto.

$0 + 0 = 0 \in H_4$ $\quad$ $5 + 0 = 5 \in H_4$

$0 + 5 = 5 \in H_4$ $\quad$ $5 + 5 = 10 = 0$ (modulo) $\in H_4$

Portanto H_4 é subgrupo de $\mathbb{Z}_{10}$.

$H_4 < \mathbb{Z}_{10}$.

iii) $H_5 = \{1, 2, 4, 8, 6\}$ e $\mathbb{Z}_{10} = \{0, 1, \ldots, 8, 9\}$

a) Elemento neutro de $\mathbb{Z}_{10}$ precisa pertencer ao conjunto.

$0 \in \mathbb{Z}_{10}$ e $0 \notin H_5$.

Portanto H_5 não é subgrupo de $\mathbb{Z}_{10}$.

iv) $\mathbb{Z}_{10} = \{0, 1, \ldots, 8, 9\}$ $H_6 = \{0, 2, 4, 6, 8\}$

a) $|\mathbb{Z}_{10}| = 10$ e $|H_6| = 5$, $5 \mid 10$ V.

b) $H_6 = \{0,2,4,6,8\}$

$0 \in H_6$ e $0 \in \mathbb{Z}_{10}$ — Ambos possuem o elemento neutro

c) Elemento Simétrico

$0 \in H_6$; $0 = -0$
$2 \in H_6$; $2 = 8 = 8-10 = -2$
$4 \in H_6$; $4 = 6 = 6-10 = -4$
$6 \in H_6$; $6 = 4 = 4-10 = -6$
$8 \in H_6$; $8 = 2 = 2-10 = -8$

Todos os elementos de H_6 possui seu simétrico no próprio H_6.

d) fechado na operação:

$0-2 = -2$
$0-6 = -6$
$8-6 = 2$
$6-4 = 2$
$8-4 = 4$
$4-2 = 8$

Tem os resultados dentro do H_6.

Portanto H_6 é um subgrupo de $\mathbb{Z}_{10}$.

Além de facilitar determinar subgrupos, podemos também determinar a ordem de elementos de um grupo ou subgrupo.

Corolário: Se x é elemento de um grupo G, então a ordem de x divide a ordem de G. Em particular: $x^{|G|} = e$.

Ordem de elemento: Se x é elemento de um grupo G então ordem "$o(x)$" é o menor inteiro positivo k tal que $x^k = e$.

Exemplo: $\langle \mathbb{Z}_6, + \rangle$ $3 \in \mathbb{Z}_6$

$3^1 = 3$
$3^2 = 3+3 = 6 = 0$

$\left\{ \begin{array}{l} \text{Então } o(3) = 2 \\ 3^2 = 0 \pmod 6 \end{array} \right.$

Exemplo: Seja $G = \langle x \rangle$ um grupo de ordem 8. Temos então:

$G = \{x, x^2, x^3, x^4, \ldots, x^8\}$ e $x^8 = e$

É possível o grupo G ter um subgrupo de ordem 6?

Não, porque 6 não é divisor de 8.

É possível ter um subgrupo de ordem 4?

Sim, porque $4 | 8$.

Com isso, o grupo $G = \langle x \rangle$, de ordem 8, pode possuir subgrupos de ordem: 1, 2, 4, 8. Os mesmos valores são as possíveis ordem dos elementos de G.

Subgrupos de ordem 1 e 8: são os chamados triviais.
Subgrupos de ordem 2, 3, 4, 5, 6, 7: são os chamados próprios.

Exemplo: Considere um grupo de ordem 135. É possível o grupo ter um subgrupo de ordem: 5, 6, 11, 45, 9, 30, 27, 54?

$135 = 3^3 \cdot 5$ $\{5, 45, 27, 45,$

Grupo $|G| = 7!$, é possível G ter elementos por subgrupos cuja ordem seja 32, 100, 27, 16, 50?

$7.6.5.4.3.2.1$ • Subgrupos: 50, 16, 32, 100,

$100 = 2^4 . 5^2$
$32 = 2^5$
$27 = 3^3$
$16 = 4^2 = 2^3$
$50 = 2.5^2$

Homomorfismo de Grupos: Dada uma função f (função bijetora); seja uma aplicação $f: G \to J$.

Definição: Sejam $(G, \circ)$ e $(J, *)$ grupos quaisquer, um homomorfismo:

$f: G \to J$ é denominado isomorfismo se, e somente se, f é bijetiva.

Para mostrar que f é isomorfismo é necessário mostrar que:

i) f é homomorfismo
ii) f é injetivo
iii) f é sobrejetivo

Exemplo: Mostre que $f: \mathbb{Z} \to 2\mathbb{Z}$ dada por $f(n) = 2n$, $\forall n \in \mathbb{Z}$, é um isomorfismo do grupo aditivo $\mathbb{Z}$ no grupo aditivo $2\mathbb{Z}$.

i) Homomorfismo: Sejam $m, n \in \mathbb{Z}$, então:

$$f(m+n) = 2(m+n)$$
$$= 2m + 2n$$
$$= f(m) + f(n)$$

Portanto, f é um homomorfismo.

ii) Injetividade: Temos $f: \mathbb{Z} \to 2\mathbb{Z}$ dada por $f(n) = 2n$, $\forall n \in \mathbb{Z}$.

$Nuc(f) = \{n \in \mathbb{Z} \mid f(n) = 0\}$. Mas:

$f(n) = 0 \to 2n = 0 \to n = 0 \to Nuc(f) = \{0\}$

Portanto, f é injetivo.

iii) Sobrejetividade: Seja $y \in 2\mathbb{Z}$. Então $\exists x \in \mathbb{Z}$ tal que $y = 2x \to x = y/2 \in \mathbb{Z}$

Logo: $f(x) = f(y/2) = \cancel{2} \frac{y}{\cancel{2}} = y$

Então, f é sobrejetivo.

Sendo assim, f é um homomorfismo bijetivo, e portanto, um isomorfismo!

Observação 1: Quando existe um isomorfismo $f: G \to J$ dizemos que G e J são isomorfos.

Observação 2: A forma como um isomorfismo $f: G \to J$ é definido garante uma correspondência biunívoca entre seus elementos, respeitando as operações de cada grupo!

Na prática, do ponto de vista algébrico (na teoria dos grupos) os grupos G e J possuem as mesmas propriedades e, portanto, podem ser considerados indistintos (salvo pelas representações dos elementos).

Homomorfismo de grupos: Sejam $(G, \cdot)$ e $(J, *)$ dois grupos. Uma aplicação $f: G \to J$ é um homomorfismo se ela é compatível com as estruturas dos grupos, i.é, se

$$f(a \cdot b) = f(a) * f(b), \ \forall a, b \in G$$

Exemplo: Mostre que considerando os grupos $(\mathbb{Z}, +)$ e $(\mathbb{C}^*, \cdot)$ a função definida por:

$$f: \mathbb{Z} \to \mathbb{C}^* \qquad \text{é um homomorfismo}$$
$$n \to i^n \qquad \text{de grupos.}$$

Demonstração: Sejam $m, n \in \mathbb{Z}$. Logo:

$$f(m+n) = i^{m+n} = i^m \cdot i^n$$

$\therefore f(m+n) = f(m) \cdot f(n), \ \forall m, n \in \mathbb{Z}$.

Então pela definição, temos que f é um homomorfismo de grupos.

Exemplo: Considerando um grupo $(G, \cdot)$, a aplicação Id de G em G, definida por:

$$Id: G \to G \qquad \text{É um homomorfismo denominado}$$
$$g \to g \qquad \text{identidade.}$$

Demonstração: De fato: $\forall a, b \in G$ segue que:

$$I_d(a.b) = a.b$$
$$= Id(a).Id(b)$$

Portanto, Id é um homomorfismo.

Exemplo: Sendo $(G, \circ)$ um grupo, a aplicação f de G em G, definida por:

$$f: G \rightarrow G$$
$$g \rightarrow e$$

é um homomorfismo (denominado trivial)

De fato: $\forall a, b \in G$ segue que $f(a.b) = e$
$$= e.e$$
$$= f(a).f(b)$$

Portanto, f é um homomorfismo.

Propriedades elementares dos homomorfismos:

Seja $f: G \rightarrow J$ um homomorfismo do grupo $(G, \cdot)$ no grupo $(J, *)$. Então:

1) Se e_G e e_J são os neutros de G e J respectivamente, vale que $f(e_G) = e_J$.

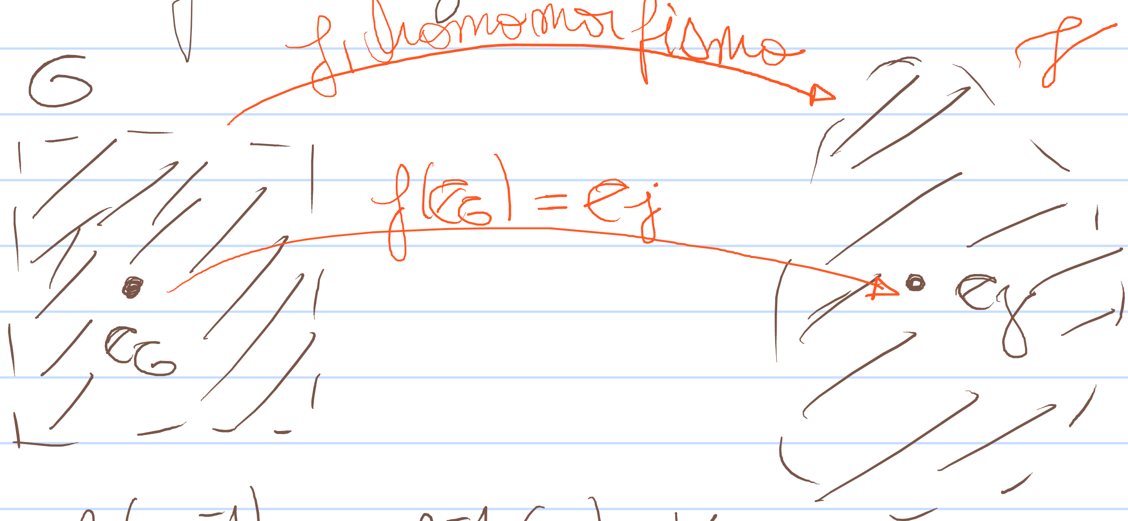
Dem: É claro que $f(e_G) \in J$, logo,

$$f(e_G) * e_J = f(e_G)$$

Mas $f(e_G) = f(e_G \cdot e_G)$. Então,

$$f(e_G) * e_J = f(e_G \cdot e_G)$$
$$= f(e_G) * f(e_G) \rightarrow \cancel{f(e_G)} * e_J = \cancel{f(e_G)} * f(e_G)$$
$$e_J = f(e_G)$$

Isto quer dizer:



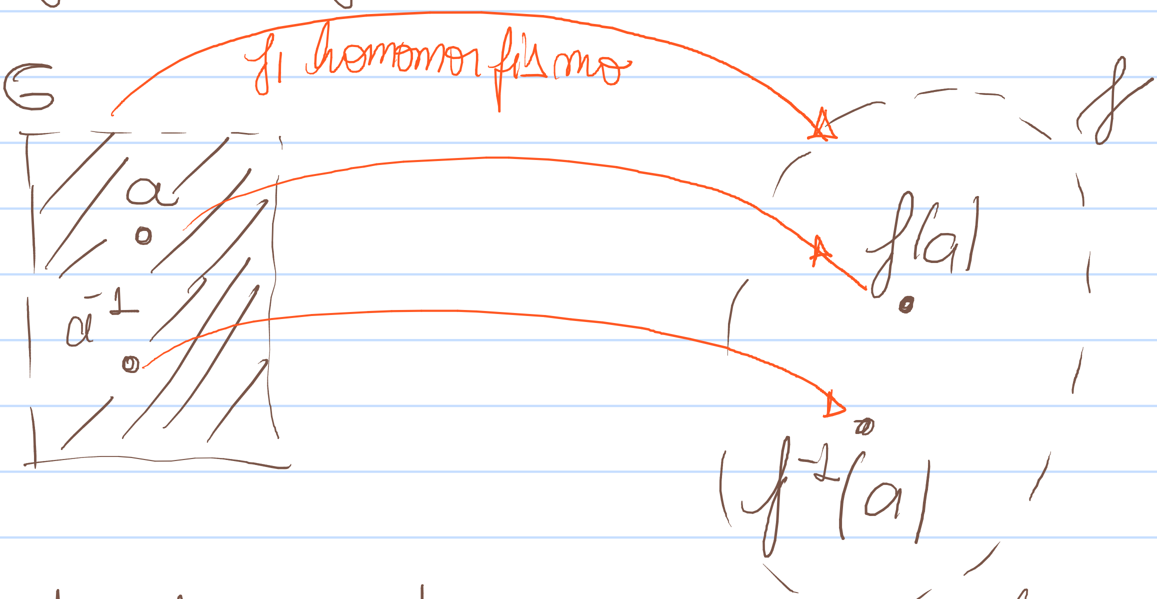
2) $f(a^{-1}) = f^{-1}(a), \forall a \in G$

$f(e_G) = e_J = f(a \cdot a^{-1}) = f(a) * f(a^{-1}) \longrightarrow$

$f(a) * f(a^{-1}) = f(e_G)$

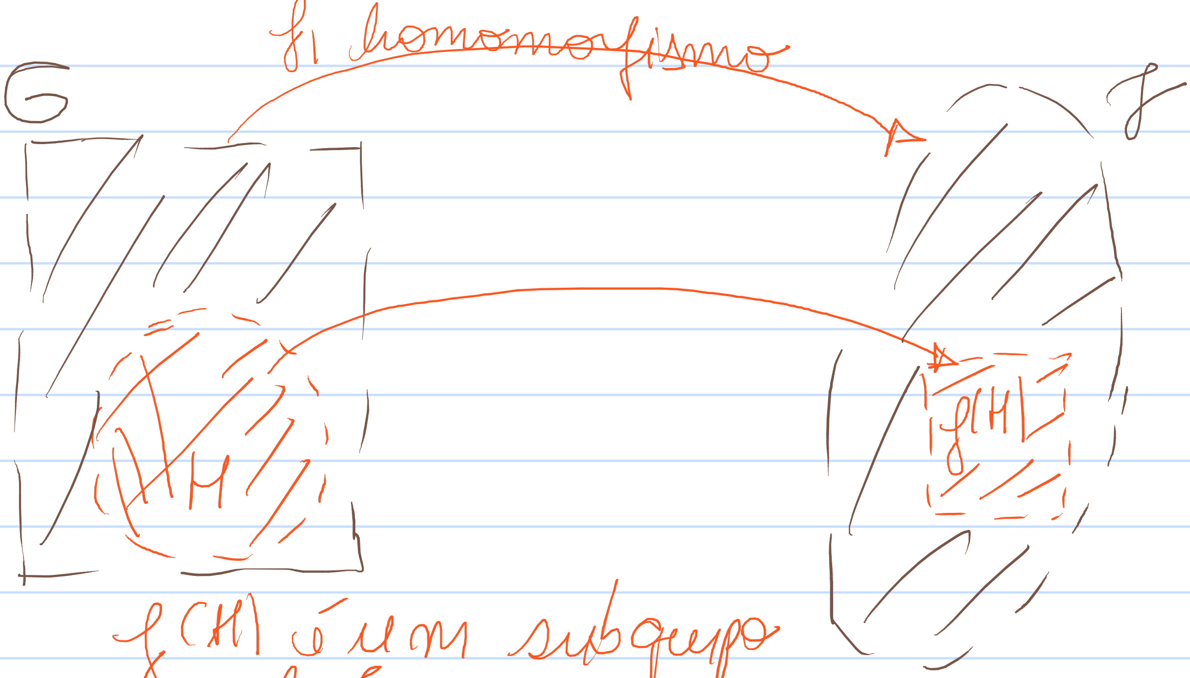
$\longrightarrow f^{-1}(a) * f(a) * f(a^{-1}) = f^{-1}(a) * f(e_G)$

$f(a^{-1}) = f^{-1}(a)$



3) Se $H < G$, então $f(H) < J$, sendo que:

$f(H) = \{f(h); h \in H\}$.



f(H) é um subgrupo de J.

4) Se G, H e J são grupos e $f: G \to H$ e $g: H \to J$ são homomorfismos de grupos, então (a composição de funções):

$$g \circ f: G \to J$$

Também é um homomorfismo de grupos.

$$\begin{tikzcd} G \arrow[r, bend left, "f"] \arrow[rr, bend right, "g \circ f"'] & H \arrow[r, bend left, "g"] & J \end{tikzcd}$$

<u>Propriedades</u> <u>Isomórficas</u>: dada uma função $f: G \to H$ deve manter estas propriedades:

i) Elementos distintos de G geram elementos distintos em H: se $r \neq r'$ em G, então $f(r) \neq f(r')$ em H.

2) Cada elemento de H esta para algum elemento de G^*.

Para cada $h \in H$, existe um $r \in G$ sendo que $f(r) = h$.

As propriedades (1) e (2) diz que a função f deve manter injetiva e sobrejetiva, isto é f é bijetiva.

Assim: $a * b = c$ em $G \to f(a) * f(b) = f(c)$ em H

$a * b = c \to f(a*b) = f(c) = f(a) * f(b)$ em H. Logo:

$$f(a*b) = f(a) * f(b)$$

<u>Definição</u>: Temos G e H sendo grupos com a operação denotada por $*$. G é isomorfo para um grupo H (simbologia, $G \cong H$) se existe uma função $f: G \to H$ sendo que:

i) f é injetiva ii) f é sobjetiva

iii) $f(a*b) = f(a) * f(b)$ $\forall a,b \in G$

Neste caso, a função f é chamada um isomorfismo. Temos que $G \cong H$ se e somente se $H \cong G$.

Exemplo: Um grupo multiplicativo $U_8 = \{1, 3, 5, 7\}$ de unidades em $\mathbb{Z}_8$ é isomorfo para um grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$. Temos: $f: U_8 \to \mathbb{Z}_2 \times \mathbb{Z}_2$.

$$\left.\begin{array}{l} f(1) = (0,0) \\ f(3) = (1,0) \\ f(5) = (0,1) \\ f(7) = (1,1) \end{array}\right\}$$

Temos uma bijeção:

$f(ab) = f(a) + f(b) \ \forall a,b \in U_8$

Trocando cada $a \in U_8$ por um elemento $f(a) \in \mathbb{Z}_2 \times \mathbb{Z}_2$.

Exemplo: E é um grupo aditivos de inteiros.

$f: \mathbb{Z} \to E$, dado por $f(a) = 2a$ é um isomorfismo.

1) injetivo: Supondo que $a, b \in \mathbb{Z}$ e $f(a) = f(b)$ em E, então:

$$f(a) = f(b)$$
$$2a = 2b$$
$$a = b$$

Temos que f é injetiva.

2) subjetiva: Agora supomos $N \in E$, desde que N é um inteiro, $N = 2k$ para cada inteiro k. Dado que:

$$f(k) = 2k = N$$ é f é subjetiva.

Finalmente, para todos $a, b \in \mathbb{Z}$:

$$f(a+b) = 2(a+b) = 2a + 2b = f(a) + f(b)$$

f é um isomorfismo de grupos aditivos

"Se G é abeliano e H não é abeliano, então G e H não são isomorfismo."

"Se f é um isomorfismo, então a e $f(a)$ tem a mesma ordem."

Se G é um grupo, então um isomorfismo $G \to G$ é chamado um autoisomorfismo do grupo G.

Exemplo: Um grupo aditivo $\mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ cada um tem ordem 4 mas não é isomorfo, porque cada elemento diferente zero de $\mathbb{Z}_2 \times \mathbb{Z}_2$ tem ordem 2. E em $\mathbb{Z}_4$ tem 2 elementos de ordem 4.

Exemplo: Se G é um grupo, então a identidade mapa: $\iota_G : G \to G$ dada por:

$\iota_G(x) = x$, é um automorfismo de G

Isto é claramente que ι_G é bijetivo, e para qualquer $a, b \in G$,

$$\iota_G(a * b) = a * b = \iota_G(a) * \iota_G(b)$$

O próximo teorema completamente caracterizado para grupos cíclicos.

Teorema: Temos G sendo um grupo cíclico:

1) Se G é infinito, então G é isomorfismo para um grupo aditivo $\mathbb{Z}$.

2) Se G é finito de ordem n, então G é isomorfo para um grupo aditivo $\mathbb{Z}_n$.

Homomorfismo:

Definição: Temos G e H sendo grupos com a operação $*$. Uma função $f: G \to H$ é dita ser homomorfo se:

$$f(a*b) = f(a) * f(b) \ \forall a,b \in G$$

Cada isomorfismo é um homomorfismo, mas um homomorfismo não precisa ser um isomorfismo.

Exemplo: A função $f: \mathbb{R}^* \to \mathbb{R}^*$ dada por $f(x) = x^2$ é um homomorfismo de grupos multiplicativos, porque:

$$f(ab) = (ab)^2 = a^2b^2 = f(a) \cdot f(b)$$

Contudo, f não é injetivo porque:

$$f(1) = f(-1)$$

Também não é sobrejetivo porque:

$$f(x) = x^2 \geq 0 \ \forall x$$

Então é uma imagem n negativa sob f.

Exemplo: A função $f: \mathbb{Z} \to \mathbb{Z}_5$ dada por $f(a) = [a]$ é um grupo homomorfo aditivo, porque:

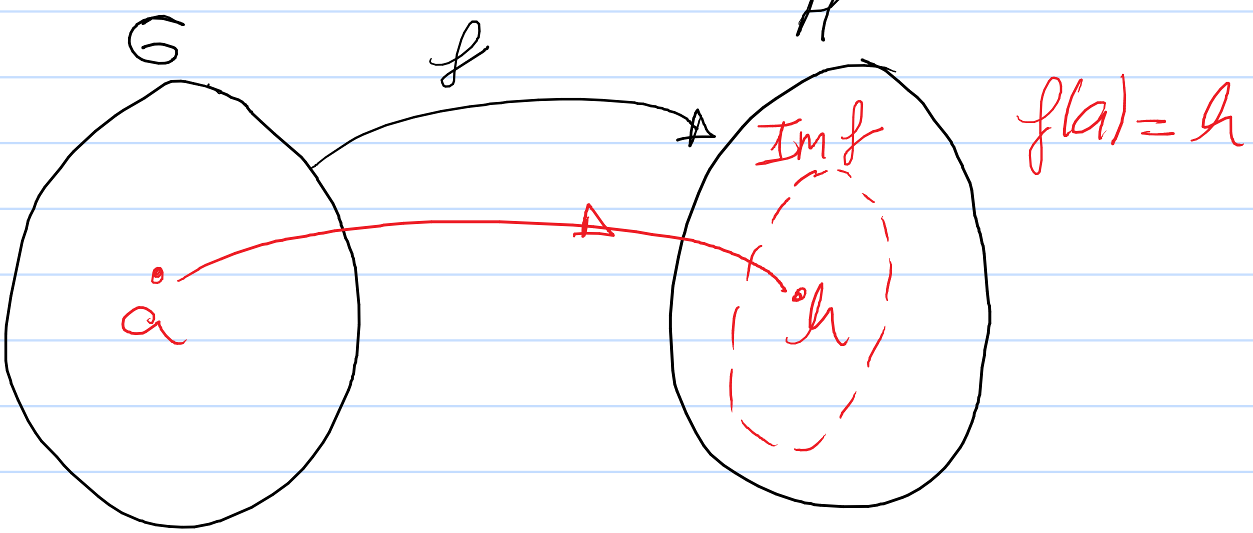
$$f(a+b) = [a+b] = [a] + [b] = f(a) + f(b)$$

É homomorfo, f é sobjetivo mas não é injetivo.

Lembramos que a imagem de uma função $f: G \to H$ é um subconjunto de H, temos que:

$$\operatorname{Im} f = \{ h \in H / h = f(a) \ \forall a \in G \}$$

A função f pode ser considerada como um mapa sobrejetivo de G para $\operatorname{Im} f$.



Teorema: Temos G e H sendo grupos com elementos identidade e_G e e_H respectivamente. Se $f: G \to H$ é um homomorfismo, então:

1) $f(e_G) = e_H$
2) $f(a^{-1}) = f(a)^{-1}$ para cada $a \in G$
3) $\operatorname{Im} f$ é um subgrupo de H
4) Se f é injetivo, então $G \cong \operatorname{Im} f$.

Teorema de Cayley: Cada grupo G é isomorfo para um grupo de permutações.

Corolário: Cada grupo finito de ordem n é isomorfo para um subgrupo de simetria de grupos S_n.