ÁLGEBRA A -

29/10/26 - AULA 12

Na aula passada iniciamos o estudo de homomorfismo de grupos. Dizemos que $\varphi: (G_1, *) \to (G_2, \cdot)$ é um homomorfismo de grupo se, e só se $\forall a, b \in G_1$;

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b)$$

Estudamos propriedades e conceitos de núcleo e imagem de um homomorfismo.

ERRATA: Um homomorfismo $f: G_1 \to G_2$ injetivo chama-se MONOMORFISMO, e não ENDOMORFISMO, como escrito na aula passada. Um homomorfismo $f: G_1 \to G_2$ injetivo chama-se ENDOMORFISMO somente quando $G_1 = G_2$. (ou seja, um homomorfismo injetivo de um grupo em si mesmo)

Def.: Dados $f: G_1 \to G_2$ e $g: G_2 \to G_3$ homomorfismos de grupos, definimos a composição:

$$g \circ f: G_1 \to G_3 \quad \text{por:} \quad \forall x \in G_1$$

$$(g \circ f)(x) = g(f(x)) \quad ;$$

uma composição de funções como estudada em cálculo.

PROPOSIÇÃO: A composição de homomorfismos é um homomorfismo.

DEMONSTR.: Sejam $f: G_1 \to G_2$ e $g: G_2 \to G_3$ homomorfismos de grupos. A mostrar:

$g \circ f: G_1 \to G_3$ é um homomorfismo de grupos.

Dados $x, y \in G_1$, precisamos mostrar que

$$(g \circ f)(x \cdot y) = (g \circ f)(x) \cdot (g \circ f)(y).$$

De fato, note que:

$$(g \circ f)(x \cdot y) = g(f(x \cdot y)) = g(f(x) \cdot f(y)) =$$

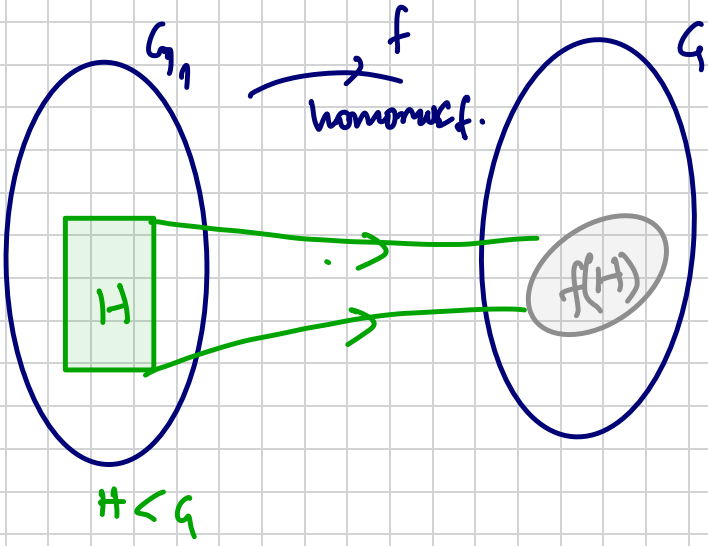
(f é homomorf.) (g é homomorf.)

$$= g(f(x)) \cdot g(f(y)) = (g \circ f)(x) \cdot (g \circ f)(y).$$

□

PROPOSIÇÃO: Sejam $f: G_1 \to G_2$ um homomorfismo de grupos e $H < G_1$. Então,

$$f(H) < G_2.$$



$f(H) < G_2$

DEMONSTR: Seja $f: G_1 \to G_2$ um homomorfismo de grupos e $H < G_1$.

Define o conjunto $f(H)$ por:

A mostrar: $f(H) < G_2$.

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

Note que $f(H)$ está bem definido, ou seja, $f(H) \neq \emptyset$; pois $f(e) = e'$

Dados $\alpha, \beta \in f(H)$, vamos mostrar que:

(i) $\alpha \cdot \beta \in f(H)$;

(ii) $\alpha^{-1} \in f(H)$.

Como $\alpha, \beta \in f(H)$, então $\exists\, h_1, h_2 \in H$ tais que

$$f(h_1) = \alpha \quad \text{e} \quad f(h_2) = \beta.$$

Disso, segue que:

(i) $\alpha.\beta = f(h_1).f(h_2) = f(h_1.h_2) \in f(H)$

$h_1.h_2 \in H < G_1$

f é homomorf.

$\Rightarrow \alpha.\beta \in f(H)$.

(ii) $\alpha^{-1} = (f(h_1))^{-1} = f(h_1^{-1}) \in f(H)$

$h_1^{-1} \in H < G_1$

PROPRIEDADE DA AULA PASSADA

$\Rightarrow \alpha^{-1} \in f(H)$.

Portanto, de (i) e (ii) segue que $f(H) < G_2$.

□

PROPOSIÇÃO: Sejam $f: G_1 \to G_2$ um homomorfismo de grupos e $H < G$. Então

$$f^{-1}(f(H)) = H.\ker f.$$

DEMONSTR.: Precisamos provar uma igualdade de conjuntos, e isto é feito mostrando duas afirmações:

AF-01: $H.\ker f \subset f^{-1}(f(H))$:

Dado $\alpha \in H.\ker f$, mostremos que $\alpha \in f^{-1}(f(H))$.

Como $\alpha \in H.\ker f$, então, $\exists\, h \in H$, $\exists\, x \in \ker f$

tal que

$$\alpha = h \cdot x.$$

Aplicando o homomorfismo f, teremos:

$$f(\alpha) = f(h \cdot x) = f(h) \cdot \underbrace{f(x)}_{e', \text{ pois } x \in \ker f} = f(h) \cdot e' = f(h)$$

(f é homomorf.)

$$\Rightarrow f(\alpha) = f(h) \in f(H)$$

$$\Rightarrow f(\alpha) \in f(H) \Rightarrow \alpha \in f^{-1}(f(H)).$$

Isso prova a AF·01.

AF·02: $f^{-1}(f(H)) \subset H \cdot \ker f$.

Dado $w \in f^{-1}(f(H))$, logo, $f(w) \in f(H)$

Assim, $\exists h \in H$ tal que $f(w) = f(h)$ (*)

Vamos analisar $f(w \cdot h^{-1})$:

$$f(w h^{-1}) = f(w) \cdot f(h^{-1}) = f(w) \cdot (f(h))^{-2} =$$

(f é homomorf.)

($= f(h)$ por (*); PROPRIEDADE DOS HOMOMORFISMOS)

$$= f(h) \cdot (f(h))^{-1} = e'$$

$$\Rightarrow f(w h^{-1}) = e'$$

$$\Rightarrow w \cdot h^{-2} \in \ker f$$

$$\Rightarrow w \in h.\ker f \subset H.\ker f;$$

o que prova a AF·02.

Pelas afirmações 01 e 02 segue o resultado.

□

Def.: Dizemos que um homomorfismo $f: G_1 \to G_2$ é um:

(a) **monomorfismo** quando f for injetivo;

(b) **epimorfismo** quando f for sobrejetivo;

(c) **isomorfismo** quando f for bijetivo.

Quando $f: G_1 \to G_2$ é um isomorfismo, dizemos que os grupos G_1 e G_2 são ISOMORFOS, e escrevemos

$$G_1 \cong G_2.$$

Ex.: $f: ((0,+\infty), \cdot) \to (\mathbb{R}, +)$ dada por

$$f(x) = \log_2 x.$$

Afirmamos que $((0,+\infty), \cdot) \cong (\mathbb{R}, +)$.

Para mostrar isto precisamos provar que:

(i) $f : (0, +\infty) \to \mathbb{R}$, $f(x) = \log_2 x$ é um homomorfismo;

(ii) f é injetiva e sobrejetiva. (e, portanto, bijetiva)

AF-01: f é um homomorfismo de grupos:
Dados $x, y \in (0, +\infty)$, temos:

$$f(x \cdot y) = \log_2 (x \cdot y) = \log_2 x + \log_2 y =$$

(PROPRIEDADE DOS LOGARITMOS)

$$= f(x) + f(y).$$

Logo, vale a AF-01.

AF-02: f é injetiva: basta mostrar que

$$f(x) = f(y) \Rightarrow x = y \; ; \text{ ou}$$

mostrar que $\ker f = \{1\}$ → neutro em $((0, +\infty), \cdot)$

$$\ker f = \{ x \in (0, +\infty) : f(x) = 0 = e \}$$

$$= \{ x \in (0, +\infty) : \log_2 x = 0 \} = \{1\}$$

↳ $\log_2 x = 0 \Leftrightarrow 2^0 = x$

$x = 1$

Logo, $\ker f = \{1\}$; ou seja f é injetiva.

AF·03: f é sobrejetiva:

$$f: (0, +\infty) \to \mathbb{R} \quad ; \quad f(x) = \log_2 x .$$

Dado $z \in \mathbb{R}$, precisamos encontrar $x \in (0, +\infty)$ tal que $f(x) = z$. De fato, basta tomar $x = 2^z$, pois neste caso, teremos:

$$f(x) = f(2^z) = \log_2 2^z = z$$

Logo, f é sobrejetiva.

"RASCUNHO":

$f(x) = z$

$\log_2 x = z$

$2^z = x$

Assim, f é um ~~homomorfismo~~ bijetivo, ou seja, um isomorfismo; mostrando que

$$((0, +\infty), \cdot) \simeq (\mathbb{R}, +) .$$

PROP.: Seja $f: G_1 \to G_2$ um homomorfismo de grupos. Então, f é um isomorfismo se, e somente se, $\exists\, g: G_2 \to G_1$ homomorfismo tal que

$$f \circ g = id_{G_2} \quad \text{e} \quad g \circ f = id_{G_1}.$$

DEMONSTR.: Suponha $f: G_1 \to G_2$ isomorfismo

A mostrar: $\exists\, g: G_2 \to G_1$ homomorfismo tal que

$$(f \circ g)(y) = y, \quad \forall y \in G_2 \quad \text{e}$$

$$(g \circ f)(x) = x, \quad \forall x \in G_1.$$

Para isso, basta tomar $g = f^{-1}: G_2 \to G_1$, visto que f^{-1} existe, pois sendo f isomorfismo, em particular é bijetiva, logo, inversível.

Assim, da def. de função inversa, segue que

$$(f \circ g)(y) = (f \circ f^{-1})(y) = y = id_{G_2};$$

e

$$(g \circ f)(x) = (f^{-1} \circ f)(x) = x = id_{G_1}.$$

Além disso, $g: G_2 \to G_1$ é um homomorfismo, pois

$\forall\, z_1, z_2 \in G_2$, $\exists\, x_1, x_2 \in G_1$ tais que

$$g(z_1) = x_1 \quad \text{e} \quad g(z_2) = x_2.$$

Logo, $f(x_1) = z_1$ e $f(x_2) = z_2$, pois g é inversa de f. Então:

$$g(z_1 \cdot z_2) = g(f(x_1) \cdot f(x_2)) = g(f(x_1 \cdot x_2)) =$$

(f é homomorf.)

$$= x_1 \cdot x_2 = g(z_1) \cdot g(z_2).$$

($g \circ f = id$.)

($\Leftarrow$) Reciprocamente, dada $f: G_1 \to G_2$ homomorf., suponha que $\exists\, g: G_2 \to G_1$ homomorfismo tal que

$$f \circ g = id_{G_2} \quad \text{e} \quad g \circ f = id_{G_1}. \qquad (*)$$

Temos que provar que f é isomorfismo.

Como f é homomorfismo, resta mostrar que é bijetiva.

Mas as igualdades em $(*)$ já nos mostram que o é.

Isso conclui a demonstração. □