ÁLGEBRA A.

22/10/26 – AULA 11

CLASSE LATERAL DE H EM G, COM $H \lhd G$.

Como vimos na aula passada, se $H \lhd G$, então, $\forall a \in G$, $a \cdot H = H \cdot a$, ou seja, as classes laterais à esquerda e à direita são iguais.

Vamos definir o conjunto: para $a \in G$:

$$\bar{a} = aH = Ha \qquad (\text{pois } H \lhd G)$$

Assim, dados $a, b \in G$, definimos a operação:

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}. \qquad \text{(PRODUTO DE CLASSES)}$$

Precisamos verificar se esta operação está bem definida, ou seja, ela deve independer dos representantes da classe.

De fato, se $\bar{a} = \bar{a'}$ e $\bar{b} = \bar{b'}$, precisamos verificar se $\overline{a \cdot b} = \overline{a' \cdot b'}$

Note que:

$$\underline{\overline{a \cdot b}} = \bar{a} \cdot \bar{b} = \bar{a'} \cdot \bar{b'} = \underline{\overline{a' \cdot b'}}.$$

Logo, esta operação está bem definida.

Dados G um grupo e $H \lhd G$, definimos o conjunto de classes laterais G/H por:

$$G/H = \{ \underbrace{aH}_{=\bar{a}} : a \in G \} = \{ Ha : a \in G \}.$$

Note que $G/H \neq \emptyset$, pois, por exemplo:

$$\bar{e} = eH \text{ é tal que } e \in G.$$

Ou seja, $\bar{e} = eH \in G/H$.

PROPOSIÇÃO: Sejam G um grupo e $H \lhd G$. Então, o conjunto quociente G/H acima definido, com a operação $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$, é um grupo.

Além disso, se G for abeliano, então G/H o é.

DEMONSTR.:

Dados $\bar{a} = aH$; $\bar{b} = bH$ e $\bar{c} = cH$ elementos do conjunto G/H, temos:

$$\bar{a} \cdot (\bar{b} \cdot \bar{c}) = \bar{a} \cdot (bH \cdot cH) = \bar{a} \cdot (b(Hc)H) =$$

($H \lhd G$)

$$= \bar{a} \cdot (bc \cdot H) = (aH) \cdot (bcH) =$$

$$= a \cdot (H(bc)) \cdot H = a(bc) \cdot H \cdot H =$$

$\uparrow$ $H \lhd G$

$$= a \cdot (bc) \cdot H = (a \cdot b) \cdot cH = (ab) \cdot H \cdot cH$$

$$= ((aH) \cdot (bH)) \cdot cH = \underline{(\bar{a} \cdot \bar{b}) \cdot \bar{c}}$$

Logo, vale a associatividade.

obs.: Uma forma "mais limpa" de fazer seria:

$$\underline{\bar{a} \cdot (\bar{b} \cdot \bar{c})} = \bar{a} \cdot (\overline{b \cdot c}) = \overline{a \cdot (b \cdot c)} =$$

$$= \overline{(a \cdot b) \cdot c} = \overline{ab} \cdot \bar{c} = \underline{(\bar{a} \cdot \bar{b}) \cdot \bar{c}}$$

Existência do neutro:

Note que $\bar{e} = eH = H$, é tal que:

$$\underline{\bar{a} \cdot \bar{e}} = aH \cdot eH = a(He) \cdot H =$$

$$= a(eH) \cdot H = a \cdot H \cdot H = aH = \bar{a}$$

$$\Rightarrow \bar{a} \cdot \bar{e} = \bar{a}$$

Do mesmo modo tem-se:

$$\bar{e} \cdot \bar{a} = \bar{a}$$

Logo, $\bar{e} = H \lhd G$ é o neutro de G/H.

Resta encontrar o simétrico.

Dado $\bar{a} \in G/H$; afirmamos que $\overline{a^{-1}}$ é o simétrico de $\bar{a}$. De facto:

$$\bar{a} \cdot \overline{a^{-1}} = (aH)(a^{-1}H) = a(H a^{-1})H$$

$$= a \cdot (a^{-1} \cdot H) \cdot H = (a \cdot a^{-1}) \cdot H \cdot H$$

$= e$ (↑ $H \triangleleft G$.)

$$= e \cdot H = \bar{e} = H.$$

$$\Rightarrow \boxed{\bar{a} \cdot \overline{a^{-1}} = \bar{e}}.$$

Do mesmo modo tem-se que $\overline{a^{-1}} \cdot \bar{a} = \bar{e}$.

Logo, G/H equipado com a operação

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b},$$

é um grupo.

Além disso, se G for abeliano, mostramos que G/H também é abeliano. De facto, basta observar que:

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b} = \overline{b \cdot a} = \bar{b} \cdot \bar{a}$$

(G é abeliano : $ab = ba$)

□

HOMOMORFISMOS DE GRUPOS:

Def.: Sejam $(G_1, *)$, $(G_2, \cdot)$ grupos. Dizemos que uma função $f: G_1 \to G_2$ é um homomorfismo de grupos se $\forall\, a, b \in G_1$, tivermos

$$f(a * b) = f(a) \cdot f(b).$$

Obs: Às vezes, escreve-se, sendo $f: G_1 \to G_2$ um homomorfismo:

$$f(a \cdot b) = f(a) \cdot f(b)$$

($a \cdot b$: operação em G_1; $f(a) \cdot f(b)$: operação em G_2.)

Ou seja, o símbolo "$\cdot$" costuma ser usado para G_1 e para G_2, mas observe-se que são, geralmente, operações diferentes.

Vejamos alguns exemplos de homomorfismos de grupos:

a) $f: (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$, dada por $f(x) = \ln x$.

($\mathbb{R}^+$: $(0, +\infty)$; $\cdot$: produto usual; $+$: soma usual.)

Esta função é um homomorfismo do grupo $(\mathbb{R}^+, \cdot)$ para o grupo $(\mathbb{R}, +)$, pois;

$\forall\, a, b \in \mathbb{R}^+$ tem-se que

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

---

02) Seja G um grupo. Fixe $g \in G$, e defina a função $\varphi_g : G \to G$ por

$$\varphi_g(x) = g x g^{-1}$$

Afirmamos que φ_g é um homomorfismo.

De fato, dados $x, y \in G$, temos que

$$\varphi_g(x.y) = g(xy)g^{-1} = g x g^{-1} \cdot g y \cdot g^{-1} =$$

$$= (g x g^{-1}) \cdot (g y g^{-1}) = \varphi_g(x) \cdot \varphi_g(y).$$

($g x g^{-1} = \varphi_g(x)$, $g y g^{-1} = \varphi_g(y)$)

---

03) Dados G um grupo e $H \lhd G$. Defina a aplicação

$$\pi : G \longrightarrow G/H$$

$$\pi(a) = \bar{a} = aH.$$

Esta função é chamada de aplicação canônica.

Afirmamos que π é um homomorfismo de grupos. De fato, dados $a, b \in G$, temos que

$$\pi(a \cdot b) = \overline{a \cdot b} = \bar{a} \cdot \bar{b} = \pi(a) \cdot \pi(b).$$

---

04) $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ dada por

$$f(a) = n \cdot a, \quad n \in \mathbb{Z} \text{ fixo}.$$

f é um homomorfismo de grupos pois, $\forall x, y \in \mathbb{Z}$, temos que

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

(DISTRIBUTIVIDADE EM $\mathbb{Z}$)

PROPOSIÇÃO: Seja $\varphi : G_1 \to G_2$ um homomorfismo de grupos. Então, valem as propriedades:

(01) $\varphi(e) = e'$ [e : neutro de G_1 ; e' : neutro de G_2]

(02) $\varphi(x^{-1}) = (\varphi(x))^{-1}$, $\forall x \in G_1$.

DEMONSTR.:

(01) Basta notar que:

$$\varphi(e) = \varphi(e \cdot e) = \varphi(e) \cdot \varphi(e)$$

(φ é homomorfismo)

$$\Rightarrow \varphi(e) = \varphi(e) \cdot \varphi(e)$$

Multiplicando por $(\varphi(e))^{-1}$:

$$e' = \underbrace{\varphi(e)}_{\in G_2} \cdot \underbrace{(\varphi(e))^{-1}}_{\in G_2} = \varphi(e) \cdot \underbrace{\varphi(e) \cdot (\varphi(e))^{-1}}_{e'} = \varphi(e) \cdot e'$$

$$\Rightarrow e' = \varphi(e) \cdot e' = \varphi(e) \quad ; \text{ provando (01).}$$

(02) $\varphi(x^{-1}) = (\varphi(x))^{-1}$, $\forall x \in G_1$.

Note que; $\forall x \in G$:

$$\varphi(x^{-1}) \cdot \varphi(x) = \varphi(x^{-1} \cdot x) = \varphi(e) = e'$$

(φ é homomorfismo; por (01))

$$\Rightarrow \underbrace{\varphi(x^{-1})}_{\in G_2} \cdot \underbrace{\varphi(x)}_{\in G_2} = e'$$

Multiplicando por $(\varphi(x))^{-1}$, vem:

$$\varphi(x^{-1}) \cdot \underbrace{\left(\varphi(x) \cdot (\varphi(x))^{-1}\right)}_{= e'} = e' \cdot (\varphi(x))^{-1}$$

$$\Rightarrow \varphi(x^{-1}) \cdot e' = e' \cdot (\varphi(x))^{-1}$$

$$\varphi(x^{-1}) = (\varphi(x))^{-1}$$

□

NÚCLEO DE UM HOMOMORFISMO:

MOTIVAÇÃO: Do estudo de transformações lineares de Álgebra linear; dada $T: V \to W$ uma transf. linear do espaço vetorial V para o espaço vetorial W, (lembre que $T(\vec{u}+\vec{v}) = T(\vec{u}) + T(\vec{v})$ e

$T(\alpha \vec{u}) = \alpha \cdot T(\vec{u})$; e então, olhando para a adição, T é um homomorfismo), vimos o conceito de núcleo de uma transf. linear:

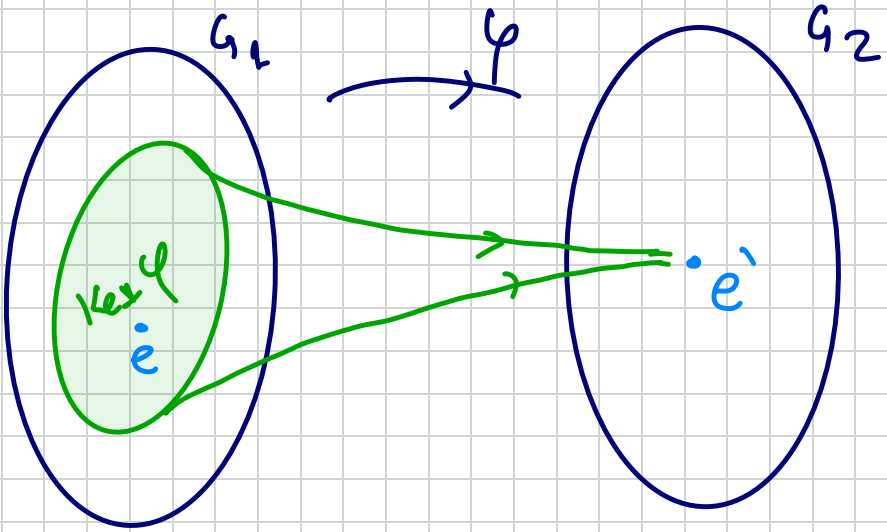
$$\ker(T) = \{\vec{v} \in V : T(\vec{v}) = \vec{0}_W\}.$$

Este conceito é exatamente o mesmo para o estudo de homomorfismos de grupos.

Def: Seja $\varphi: G_1 \to G_2$ um homomorfismo de grupos. Definimos o núcleo de φ por

$$\ker \varphi = \{x \in G_1 : \varphi(x) = e'\}.$$

onde e' é o neutro em G_2.



Note que $\ker\varphi \neq \emptyset$, pois pela proposição anterior $\varphi(e) = e'$. Logo, $e \in \ker\varphi$.

Na Álgebra linear, o núcleo de uma transformação linear é um subespaço vetorial do espaço vetorial do domínio. Este resultado se espelha na Álgebra no seguinte:

TEOREMA: Seja $\varphi : G_1 \to G_2$ um homomorfismo de grupos. Então, $\ker\varphi \lhd G_1$.

DEMONSTR.: Dado $\varphi : G_1 \to G_2$ homomorfismo.

Vamos mostrar que:

(01) $\ker\varphi < G_1$;

(02) $\ker\varphi \lhd G_1$.

AF 01: $\ker\varphi < G_1$. Dados $\alpha, \beta \in \ker\varphi$, temos

mostrar que:

(i) $\alpha.\beta \in \ker\varphi$;

(ii) $\alpha^{-1} \in \ker\varphi$.

(i) $\varphi(\alpha.\beta) = \varphi(\alpha)\cdot\varphi(\beta) = e'\cdot e' = e'$

(φ é homomorf.) ; (pois $\alpha, \beta \in \ker\varphi$)

$\Rightarrow \varphi(\alpha.\beta) = e'$. Logo, $\boxed{\alpha.\beta \in \ker\varphi}$;

provando (i).

(ii) $\varphi(\alpha^{-1}) = (\varphi(\alpha))^{-1} = (e')^{-1} = e'$

(PROP. ANTERIOR) ; ($\alpha \in \ker\varphi$)

$\Rightarrow \varphi(\alpha^{-1}) = e' \Rightarrow \boxed{\alpha^{-1} \in \ker\varphi}$;

provando (ii).

De (i) e (ii) segue que $\ker\varphi < G_1$.

Resta provar a normalidade.

AF-02: $\ker\varphi \lhd G_1$:

Dados $g \in G_1$ e $\alpha \in \ker\varphi$, precisamos mostrar que $g\alpha g^{-1} \in \ker\varphi$. De fato:

$\varphi(g\alpha g^{-1}) = \varphi(g)\cdot\varphi(\alpha)\cdot\varphi(g^{-1}) =$

(φ é homomorf.) ; $= e'$ pois $\alpha \in \ker\varphi$

$$= \varphi(g) \cdot e' \cdot \varphi(g^{-1}) = \varphi(g) \cdot \varphi(g^{-1}) =$$

(φ é homomorfismo)

$$= \varphi(g \cdot g^{-1}) = \varphi(e) = e'$$

($g \cdot g^{-1} = e$; $\varphi(e) = e'$ pela Prop.)

$$\Rightarrow \varphi(g \alpha g^{-1}) = e' \Rightarrow g \alpha g^{-1} \in \ker \varphi$$

Portanto, $\ker \varphi \lhd G$.

□

Def.: Dizemos que um homomorfismo $\varphi: G_1 \to G_2$ é injetivo se $\forall\, x, y \in G_1$:

$$\varphi(x) = \varphi(y) \Rightarrow x = y.$$

Um homomorfismo injetivo é chamado de ENDOMORFISMO.

Ex.: $f: (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ dada por

$$f(x) = n \cdot x \qquad (n \in \mathbb{Z}, n \neq 0).$$

Já vimos que f é um homomorfismo, pois:

$$f(x+y) = n \cdot (x+y) = n \cdot x + n \cdot y = f(x) + f(y).$$

Afirmamos que f é injetiva. De fato:

$$f(x) = f(y) \Rightarrow nx = ny \Rightarrow x = y.$$

PROPOSIÇÃO: Seja $\varphi: G_1 \to G_2$ um homomorfismo de grupos. Então, φ é injetivo se, e somente se, $\ker \varphi = \{e\}$.

DEMONSTR.: Seja $\varphi: G_1 \to G_2$ um homomorfismo de grupos.

($\Rightarrow$) Suponha que φ é injetiva. A mostrar:

$$\ker \varphi = \{e\}.$$

Por absurdo, suponha que $\ker \varphi \neq \{e\}$.

Então, $\exists\, x \in \ker \varphi$, $x \neq e$ tal que $\varphi(x) = e$. Mas disso, segue que:

$$\varphi(x) = e = \varphi(e),$$ mas $x \neq e$, um absurdo, pois supomos φ injetiva!

Logo, $\ker \varphi = \{e\}$.

($\Leftarrow$) Reciprocamente, suponha que $\ker \varphi = \{e\}$.

A mostrar: φ é injetiva. Sejam $x, y \in G_1$ tais que $\varphi(x) = \varphi(y)$. Então, multiplicando à direita por $(\varphi(y))^{-1}$, obtemos:

$$\varphi(x).(\varphi(y))^{-1} = \varphi(y).(\varphi(y))^{-1} = e'$$

$$\Rightarrow \varphi(x).(\varphi(y))^{-1} = e'$$

$\Rightarrow \quad \varphi(x) \cdot \varphi(y^{-1}) = e' \quad \Rightarrow \quad \varphi(x \cdot y^{-1}) = e'$

↑ PROPRIEDADE DO HOMOMORFISMO

↑ φ é' homomorf.

Logo, $x \cdot y^{-1} \in \ker \varphi = \{e\}$

↑ POR HIPÓTESE

Então,

$$x \cdot y^{-1} = e .$$

Multiplicando à direita por y ;

$$x \cdot \underbrace{y^{-1} \cdot y}_{e} = e \cdot y = y$$

$$\Rightarrow x = y .$$

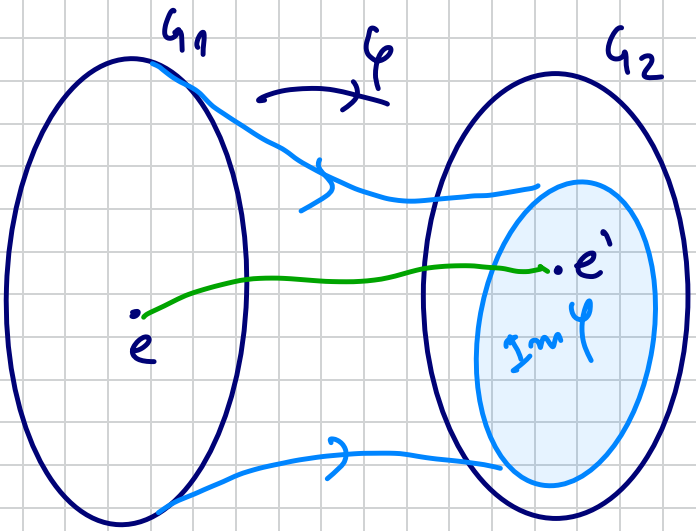
Ou seja, mostramos que, se $\varphi(x) = \varphi(y)$, então, $x = y$, isto é', φ é' injetiva.

□

IMAGEM DE UM HOMOMORFISMO:

Def: Seja $\varphi: G_1 \to G_2$ um homomorfismo de grupos. Definimos a imagem de φ por:

$$\operatorname{Im}\varphi = \varphi(G_1) = \{ y \in G_2 : \exists\, x \in G_1 \text{ tal que } \varphi(x) = y \}.$$



$\operatorname{Im}\varphi \neq \emptyset$, pois $\varphi(e) = e'$.

PROPOSIÇÃO: A imagem de um homomorfismo é um subgrupo do grupo G_2.

DEMONSTR.: Seja $\varphi: G_1 \to G_2$ um homomorfismo de grupos. A mostrar:

$$\operatorname{Im}\varphi < G_2.$$

De facto, dados $x, y \in \operatorname{Im}\varphi$, precisamos mostrar que:

(i) $x.y \in \operatorname{Im}\varphi$

(ii) $x^{-1} \in \operatorname{Im}\varphi$.

Como $x, y \in \operatorname{Im}\varphi$, então $\exists\, \alpha, \beta \in G_1$ tais que

$\varphi(\alpha) = x$ e $\varphi(\beta) = y$. Assim:

- $x \cdot y = \varphi(\alpha) \cdot \varphi(\beta) = \varphi(\alpha \cdot \beta) \in \operatorname{Im}\varphi$; ($\alpha \cdot \beta \in G_1$)

(φ é homomorf. — provando (i).)

- $x^{-1} = (\varphi(\alpha))^{-1} = \varphi(\alpha^{-1}) \in \operatorname{Im}\varphi$; provando (ii)

De (i) e (ii) segue que $\operatorname{Im}\varphi < G_2$.

□