Homomorfismos de grupos

Os homomorfismos são as funções naturais a serem consideradas entre dois grupos. Mais precisamente, são as funções que respeitam as estruturas dos grupos envolvidos.

Dizemos que uma função $h\colon G \to G'$ é um *homomorfismo* entre dois grupos $(G, \cdot)$ e $(G', *)$ se preserva as operações dos grupos; isto é,

$$h(g_1 \cdot g_2) = h(g_1) * h(g_2).$$

Dizemos que o homomorfismo h é um *isomorfismo*, se ele for bijetor. Quando existir um isomorfismo entre dois grupos, dizemos que eles são *isomorfos*. Um isomorfismo de G nele próprio será chamado de *automorfismo*.

Denota-se o conjunto dos homomorfismos de G em G' por $\mathrm{Hom}(G, G')$, o conjunto dos isomorfismos de G em G' é denotado por $\mathrm{Iso}(G, G')$ e o conjunto dos automorfismos de G por $\mathrm{Aut}(G)$.

Recorde a definição de ordem de um elemento a de um grupo G: é o número natural, se existir,

$$o(a) = \min\{n \in \mathbb{N};\ a^n = e\}.$$

Caso contrário, define-se $o(a) = \infty$. Recorde também que se um inteiro N é tal que $a^N = e$, então $o(a)$ divide N.

O fato de um homomorfismo preservar as operações dos grupos, implica que ele preservará também elementos neutros e inversos. Além disso, o inverso de um isomorfismo é também um isomorfismo, como nos mostrará o próximo resultado.

Proposição Seja $h\colon G \to G'$ um homomorfismo de grupos. Sejam e e e', respectivamente, os elementos neutros de G e de G'. Tem-se que

i) $h(e) = e'$;

ii) $h(a^{-1}) = (h(a))^{-1},\ \forall\, a \in G$;

iii) Se h é um isomorfismo, então h^{-1} é também um homomorfismo de grupos.

iv) Se $a \in G$ com $o(a) < \infty$, então $o(h(a))$ divide $o(a)$.

Prova (i) Tem-se que

$$h(e) * e' = h(e) = h(e \cdot e) = h(e) * h(e),$$

logo cancelando $h(e)$ nos extremos das igualdades acima, obtemos $h(e) = e'$.

(ii) Tem-se que

$$h(a) * h(a^{-1}) = h(a \cdot a^{-1}) = h(e) = e'.$$

Do mesmo modo, mostra-se que $h(a^{-1}) * h(a) = e'$, o que nos diz que $h(a^{-1}) = (h(a))^{-1}$.

(iii) Suponha que h seja um isomorfismo e sejam $a', b' \in G'$. Considere $a, b \in G$ tais que $h(a) = a'$ e $h(b) = b'$, logo

$$h^{-1}(a' * b') = h^{-1}(h(a) * h(b)) = h^{-1}(h(a \cdot b)) = a \cdot b = h^{-1}(a') \cdot h^{-1}(b').$$

iv) Como $(h(a))^{o(a)} = h(a^{o(a)}) = h(e) = e'$, tem-se que $o(h(a))$ divide $o(a)$.

$\square$

Do ponto de vista abstrato, dois grupos isomorfos G e G' são considerados idênticos. Neste caso, escrevemos $G \cong G'$.

Exemplo Sejam G e G' grupos com elementos neutros e e e', respectivamente, a aplicação

$$\begin{array}{rcl} h\colon G & \to & G' \\ g & \mapsto & e' \end{array}$$

é um homomorfismo chamado *homomorfismo trivial*. Portanto $\mathrm{Hom}(G, G') \neq \emptyset$, sempre.

Exemplo Seja G um grupo e $a \in G$, a aplicação

$$\begin{array}{rcl} h_a\colon G & \to & G \\ g & \mapsto & aga^{-1} \end{array}$$

é um isomorfismo chamado de *automorfismo interno* associado a a.

O conjunto dos automorfismos internos de um grupo G será denotado por $\mathcal{I}(G)$.

Exemplo Não há nenhum homomorfismo não trivial de $\mathbb{Z}_3$ em $\mathbb{Z}_5$.

De fato, se $h\colon \mathbb{Z}_3 \to \mathbb{Z}_5$ é não trivial, tome $a \in \mathbb{Z}_3 \setminus \{0\}$ tal que $h(a) \in \mathbb{Z}_5 \setminus \{0\}$. Como $o(a) = 3$ e $o(h(a)) = 5$ e como , $5 \nmid 3$, temos um absurdo, pois $o(h(a))$ sempre divide $o(a)$. Assim, temos que $\mathrm{Hom}(\mathbb{Z}_3, \mathbb{Z}_5) = \{0\}$.

Proposição Se $h\colon G \to G'$ é um homomorfismo de grupos e H é um subgrupo de G, então $h(H)$ é um subgrupo de G'.

Prova Sejam $y, w \in h(H)$, logo existem $x, v \in H$ tais que $h(x) = y$ e $h(v) = w$. Como $xv^{-1} \in H$ por H ser um subgrupo de G, tem-se que

$$yw^{-1} = h(x)h(v)^{-1} = h(x)h(v^{-1}) = h(xv^{-1}) \in h(H),$$

o que mostra que $h(H)$ é um subgrupo de G'.

$\square$

Dado um homomorfismo $h \in \mathrm{Hom}(G, G')$, definimos o *núcleo* de h como sendo

$$\mathrm{N}(h)\colon = h^{-1}(e') = \{x \in G;\ h(x) = e'\}.$$

O conjunto $\mathrm{N}(h)$ é um subgrupo de G, como mostra o resultado a seguir quando particularizado para o subgrupo $H' = \{e'\}$ de G'.

Proposição Seja $h \in \mathrm{Hom}(G, G')$ e seja H' um subgrupo de G', então $h^{-1}(H')$ é um subgrupo de G que contém $\mathrm{N}(h)$.

Prova Inicialmente, observe que $h^{-1}(H')$ é não vazio, pois contém e. Agora sejam $x, v \in h^{-1}(H')$ e ponhamos $y = h(x)$ e $w = h(v)$, que por definição são elementos de H', logo

$$h(xv^{-1}) = h(x) * h(v^{-1}) = h(x) * (h(v))^{-1} = y * w^{-1} \in H',$$

consequentemente, $xv^{-1} \in h^{-1}(H')$, o que mostra que $h^{-1}(H')$ é um subgrupo de G. Por outro lado, tem-se claramente que $\mathrm{N}(h) = h^{-1}(e') \subset h^{-1}(H')$, já que $\{e'\} \subset H'$.

$\square$

Núcleos de homorfismos têm as seguintes propriedades notáveis:

Proposição Seja $h\colon G \to G'$ um homomorfismo de grupos. Tem-se que

i) para todo $a \in G$, $h^{-1}(h(a)) = aN(h) = N(h)a$.

ii) h é injetor se, e somente se, $N(h) = \{e\}$.

Prova (i) $h^{-1}(h(a)) = \{x \in G;\ h(x) = h(a)\}$. Mas,

$$h(x) = h(a) \Leftrightarrow \begin{cases} h(xa^{-1}) = e' \ \Leftrightarrow \ xa^{-1} \in \mathrm{N}(H) \ \Leftrightarrow \ x \in \mathrm{N}(h)a; \\ h(a^{-1}x) = e' \ \Leftrightarrow \ a^{-1}x \in \mathrm{N}(H) \ \Leftrightarrow \ x \in a\,\mathrm{N}(h); \end{cases}$$

donde segue o resultado.

ii) Se h é injetora, temos que $\{e\} = h^{-1}(h(e)) = N(h)$, logo $N(h) = \{e\}$. Se $N(h) = \{e\}$ e $h(a) = h(b)$, então $h(ab^{-1}) \in \mathrm{N}(h) = \{e\}$, logo $ab^{-1} = e$ e, portanto, $a = b$.

$\square$

A propriedade do núcleo dada no item (i) da proposição acima que diz que $aN(h) = N(h)a$, para todo $a \in G$, não é compartilhada em geral pelos subgrupos de um grupo, como poderemos constatar no próximo exemplo.

Exemplo Sejam $\sigma = (1\,2\,3)$ e $\tau = (1\,2)$ em S_3. Considere o grupo $H = \langle \tau \rangle = \{e, \tau\}$, logo

$$\sigma H = \{\sigma, \sigma\tau\} \neq \{\sigma, \tau\sigma\} = H\sigma.$$

Os únicos subgrupos de S_3 que possuem tal propriedade são $\{e\}$, $\langle \sigma \rangle$ e S_3.

Subgrupos de um grupo que possuem a propriedade dos núcleos acima descrita desempenham papel importante e merecem um nome. Diremos que um subgrupo H de um grupo G é um *subgrupo normal* de G se para todo $a \in G$ se tenha $aH = Ha$.

Exemplo Um subgrupo H de índice 2 em um grupo G é sempre normal em G. De fato, as classes laterais à esquerda de H em G são apenas duas: $eH = H$ e aH, onde a é um elemento qualquer de $G \setminus H$. O mesmo ocorre para as classes laterais à direita, essas são: He e Ha. Como $aH \cap H = \emptyset$ e $aH \cup H = G$, o mesmo ocorrendo para as classes laterais à direita, segue-se que $aH = Ha$ para todo $a \in G$.

Subgrupos normais-Propriedades

Dada a importância do conceito de subgrupo normal, daremos no próximo resultado algumas formulações a ele equivalentes, cuja prova deixamos como exercício.

Proposição Seja H um subgrupo de um grupo G. São equivalentes:

i) Para todo $a \in G$, $aH = Ha$;

ii) Para todo $a \in G$, $aHa^{-1} = H$;

iii) Para todo $a \in G$, $aHa^{-1} \subset H$;

iv) Para todos $a, b \in G$, $(aH)(bH) = (ab)H$.

$\square$

A proposição acima, entre outras coisas, nos diz que um subgrupo de G é normal se, e somente se, ele é deixado invariante por todo automorfismo interno de G.

Dado um grupo G, existe um subgrupo normal de G que se distingue, é o seu *centro*:

$$Z(G) = \{g \in G;\ gh = hg, \forall\, h \in G\},$$

ou seja, o conjunto dos elementos de G que possuem a propriedade de comutar com todos os elementos de G.
O centro possui as seguintes propriedades simples de serem verificadas

a) $Z(G)$ é um subgrupo abeliano de G.

b) $Z(G)$ é um subgrupo normal de G.

c) G é abeliano se e somente se $Z(G) = G$.

O centro de um grupo pode ser trivial como mostra o exemplo a seguir.

Na Lista 7, é proposto como exercício mostrar que $Z(S_n)$ é trivial. Mais precisamente, que $Z(S_2) = S_2$ e que $Z(S_n) = \{e\}$, se $n \geq 3$.

Dados um grupo G e um seu subgrupo H, vamos definir G/H como sendo o conjunto das classes laterais à esquerda de H em G, isto é

$$G/H = \{gH;\ g \in G\}.$$

Quando não houver risco de confundir qual é o subgrupo H em consideração, denotaremos o elemento gH de G/H por $\overline{g}$ e o denominaremos também *classe residual* de g módulo H.

Analogamente, para as classes laterais à direita, definimos

$$H \backslash G = \{Hg;\ g \in G\}.$$

Temos que $|G/H| = |H \backslash G| = (G : H)$.

Quando H é sugrupo normal de G, podemos definir a operação $(aH)(bH) = (ab)H$ em G/H.

O conjunto G/H com essa operação forma um grupo. De fato, a operação é associativa, o elemento neutro é $eH = H$ e o inverso de aH é $a^{-1}H$.

Esse grupo será chamado de grupo quociente de G pelo subgrupo normal H. Esse grupo vem acompanhado do homomorfismo sobrejetor *natural*

$$\begin{aligned} \varphi\colon G &\to G/H \\ g &\mapsto \overline{g} \end{aligned}$$

tal que $\mathrm{N}(\varphi) = H$.

De modo análogo, sendo H um subgrupo normal de G, segue da Proposição anterior (iv) que $(Ha)(Hb) = H(ab)$, logo temos também uma estrutura de grupo sobre $H \backslash G$.

Como um subgrupo qualquer H de um grupo abeliano G é normal, tem-se que G/H é um grupo que também é abeliano.

Teoremas dos homomorfismos

Ao tentar resolver um determinado problema em um dado grupo, pode ser interessante transferir o problema para um outro ambiente onde a questão seja mais fácil de ser respondida. Isso na prática será feito através da noção de homomorfismo. Por isso é interessante saber a relação existente entre os subgrupos de um grupo e os subgrupos do grupo a ele relacionado através de um homomorfismo. Esse será o objetivo dessa seção.

Proposição Seja $h\colon G \to G'$ um homomorfismo de grupos e sejam H um subgrupo de G e H' um subgrupo de G'. Tem-se que

i) $h^{-1}(h(H)) = H\,\mathrm{N}(h) = \mathrm{N}(h)H$.

ii) $h(h^{-1}(H')) = H' \cap h(G)$.

Prova i)Temos que.

$$
\begin{aligned}
x \in h^{-1}(h(H)) \iff & \; h(x) \in h(H) \iff h(x) = h(a), \text{ para algum } a \in H \\
\iff & \; h(a^{-1}x) = e', \text{ para algum } a \in H \\
\iff & \; a^{-1}x \in \mathrm{N}(h), \text{ para algum } a \in H \\
\iff & \; x \in a\,\mathrm{N}(h), \text{ para algum } a \in H \\
\iff & \; x \in H\,\mathrm{N}\,h.
\end{aligned}
$$

Do mesmo modo prova-se que $h^{-1}(h(H)) = \mathrm{N}(h)H$.
ii) Temos que

$$
\begin{aligned}
y \in h(h^{-1}(H')) \iff & \; y = h(x) \text{ e } x \in h^{-1}(H'), \text{ para algum } x \in G \\
\iff & \; y = h(x) \text{ e } y = h(x) \in H', \text{ para algum } x \in G \\
\iff & \; y \in h(G) \cap H'.
\end{aligned}
$$

$\square$

Teorema(Teorema dos homomorfismos) Seja $h\colon G \to G'$ um homomorfismo de grupos.

i) A aplicação

$$\begin{array}{rcl} \overline{h}\colon G/\operatorname{N}(h) & \to & h(G) \\ \overline{g} & \mapsto & h(g) \end{array}$$

é um isomorfismo de grupos.

ii) Existe uma bijeção dada por

$$\begin{array}{ccc} \{\text{subgrupos de } G \text{ contendo } \operatorname{N}(h)\} & \longleftrightarrow & \{\text{subgrupos de } h(G)\} \\ H & \longrightarrow & h(H) \\ h^{-1}(H') & \longleftarrow & H' \end{array}$$

Essa bijeção faz corresponder entre si os subgrupos normais de G que contém $\operatorname{N}(h)$ e os subgrupos normais de $h(G)$.

Prova Isto é um exercício fácil, usando a proposição anterior.

$\square$

Em particular, temos que $G/\{e\} \cong G$ e $G/G \cong \{e\}$ (verifique).

Teorema Seja G um grupo cíclico.
(i) Se G é infinito, então G é isomorfo a $(\mathbb{Z}, +)$.
(ii) Se G é finito de ordem n, então G é isomorfo a $(\mathbb{Z}_n, +)$.

Prova Suponhamos que $G = \langle a \rangle$. Temos o homomorfismo sobrejetor do grupo aditivo $(\mathbb{Z}, +)$ em G,

$$\begin{array}{rccc} h\colon & \mathbb{Z} & \to & G \\ & m & \mapsto & a^m. \end{array}$$

(i) Se G é infinito, temos que $\mathrm{N}(h) = \{0\}$, pois caso contrário a teria ordem finita implicando que G é finito, logo pelo Teorema do Homomorfismo temos que

$$\mathbb{Z} \cong \mathbb{Z}/\{0\} \cong h(\mathbb{Z}) = G.$$

(ii) Se $|G| = n$, então como $o(a) = n$, segue-se que $\mathrm{N}(h) = n\mathbb{Z}$. Logo o resultado segue novamente do Teorema do Homomorfismo.

$\square$

Portanto só há, a menos de isomorfismos, um único grupo cíclico infinito, que é $\mathbb{Z}$, e para cada $n \in \mathbb{N}$, só há um único grupo cíclico de ordem n, que é $\mathbb{Z}_n$.

Produtos de grupos Dados dois grupos G_1 e G_2, o produto cartesiano $G_1 \times G_2$ tem uma estrutura natural de grupo dada pela operação

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2'), \quad \forall\, g_1, g_1' \in G_1,\ \forall\, g_2, g_2' \in G_2,$$

de tal modo que se G_1 e G_2 são abelianos, então $G_1 \times G_2$ é abeliano.

Dados dois subgrupos H e K de um grupo G, o conjunto

$$HK = \{hk;\ h \in H \text{ e } k \in K\}$$

não é necessariamente um subgrupo de G.

Por exemplo, dados os subgrupos $H = \{e, (1\ 2)\}$ e $K = \{e, (1\ 3)\}$ de S_3, o conjunto $HK = \{e, (1\ 2), (1\ 3), (1\ 3\ 2)\}$ não é obviamente um subgrupo de S_3.

O próximo resultado nos dirá quando HK é um subgrupo de G.

Proposição Sejam H e K subgrupos de G. Então HK é um subgrupo de G se, e somente se, $HK = KH$.

Prova Suponhamos que HK seja um subgrupo de G, logo dado $hk \in HK$, existe $h'k' \in HK$ tal que $hk(h'k') = e$, portanto, $hk = k'^{-1}h'^{-1} \in KH$. Assim, $HK \subset KH$. A outra inclusão se mostra de modo análogo.

Recipocamente, Suponha que $HK = KH$. Para provarmos que HK é um subgrupo de G, note que $e \in HK$, logo $HK \neq \emptyset$. Por outro lado se $hk, h'k' \in HK$, então

$$hk(h'k')^{-1} = hkk'^{-1}h'^{-1} = h(kk'^{-1})h'^{-1} = hh''k'' = (hh'')k'' \in HK,$$

onde $h''k''$ é a escrita de $(kk'^{-1})h'^{-1} \in KH$ como elemento de HK.

$\square$

Note que se H é um subgrupo normal em G, então $Hk = kH$, para todo $k \in G$ e, portanto, para todo $k \in K$. Logo, $HK = KH$, e, consequentemente, HK é um subgrupo de G.