morfismos

Definição. Sejam G_1, G_2 grupos. Uma aplicação $\psi : G_1 \longrightarrow G_2$ diz-se um *morfismo* ou *homomorfismo* se

$$(\forall x, y \in G_1) \qquad \psi(xy) = \psi(x)\,\psi(y)\,.$$

Um morfismo diz-se um *epimorfismo* se for uma aplicação sobrejetiva.
Um morfismo diz-se um *monomorfismo* se for uma aplicação injetiva.
Um morfismo diz-se um *isomorfismo* se for uma aplicação bijetiva. Neste caso, escreve-se $G_1 \cong G_2$ e diz-se que os dois grupos são *isomorfos.*
Um morfismo de um grupo nele mesmo diz-se um *endomorfismo.*
Um endomorfismo diz-se um *automorfismo* se for uma aplicação bijetiva.

Exemplo 29. Sejam G_1 e G_2 grupos e $\varphi : G_1 \to G_2$ definida por $\varphi(x) = 1_{G_2}$, para todo $x \in G_1$. Então, φ é um morfismo de grupos (conhecido por *morfismo nulo*).

De facto, dados $x, y \in G_1$, temos que $\varphi(xy) = 1_G = 1_G 1_G = \varphi(x)\varphi(y)$.

Exemplo 30. A aplicação $\varphi : \mathbb{R} \to \mathbb{R}\backslash\{0\}$, definida por $\varphi(x) = e^x$ para todo $x \in \mathbb{R}$, é um morfismo do grupo $(\mathbb{R}, +)$ no grupo $(\mathbb{R}\backslash\{0\}, \times)$.

A conclusão é imediata tendo em conta que, para todos os reais x e y, $e^{x+y} = e^x e^y$ e que $e^x \neq 0$.

Exemplo 31. A aplicação $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2$, definida por

$$\varphi([0]_4) = \varphi([2]_4) = [0]_2 \qquad \varphi([1]_4) = \varphi([3]_4) = [1]_2$$

é um morfismo de grupos.

Para provar esta afirmação, temos de verificar os 10 casos distintos possíveis (temos 16 somas possíveis, mas os dois grupos são comutativos):

$$\begin{aligned}
\varphi([0]_4 \oplus [0]_4) = \varphi([0]_4) = [0]_2 = [0]_2 \oplus [0]_2 = \varphi([0]_4) \oplus \varphi([0]_4)\\
\varphi([0]_4 \oplus [1]_4) = \varphi([1]_4) = [1]_2 = [0]_2 \oplus [1]_2 = \varphi([0]_4) \oplus \varphi([1]_4)\\
\varphi([0]_4 \oplus [2]_4) = \varphi([2]_4) = [0]_2 = [0]_2 \oplus [0]_2 = \varphi([0]_4) \oplus \varphi([2]_4)\\
\varphi([0]_4 \oplus [3]_4) = \varphi([3]_4) = [1]_2 = [0]_2 \oplus [1]_2 = \varphi([0]_4) \oplus \varphi([3]_4)\\
\varphi([1]_4 \oplus [1]_4) = \varphi([2]_4) = [0]_2 = [1]_2 \oplus [1]_2 = \varphi([1]_4) \oplus \varphi([1]_4)\\
\varphi([1]_4 \oplus [2]_4) = \varphi([3]_4) = [1]_2 = [1]_2 \oplus [0]_2 = \varphi([1]_4) \oplus \varphi([2]_4)\\
\varphi([1]_4 \oplus [3]_4) = \varphi([0]_4) = [0]_2 = [1]_2 \oplus [1]_2 = \varphi([1]_4) \oplus \varphi([3]_4)\\
\varphi([2]_4 \oplus [2]_4) = \varphi([0]_4) = [0]_2 = [0]_2 \oplus [0]_2 = \varphi([2]_4) \oplus \varphi([2]_4)\\
\varphi([2]_4 \oplus [3]_4) = \varphi([1]_4) = [1]_2 = [0]_2 \oplus [1]_2 = \varphi([2]_4) \oplus \varphi([3]_4)\\
\varphi([3]_4 \oplus [3]_4) = \varphi([2]_4) = [0]_2 = [1]_2 \oplus [1]_2 = \varphi([3]_4) \oplus \varphi([3]_4)
\end{aligned}$$

Este morfismo pode ser definido por $\varphi([x]_4) = [x]_2$, para todo $[x]_4 \in \mathbb{Z}_4$. Será que, dados $n, m \in \mathbb{N}$, a correspondência de $\mathbb{Z}_n$ para $\mathbb{Z}_m$, definida por $\varphi([x]_n) = [x]_m$ é um morfismo de grupos?

A resposta à pergunta do slide anterior é NÃO.

Se $n < m$, a correspondência nem sequer é uma aplicação, uma vez que $[m]_n = [m-n]_n$ e $\varphi([m]_n) = [0]_m \neq [-n]_m = \varphi([m-n]_n)$.

Se $n \geq m$, a correspondência é uma aplicação, mas não necessariamente um morfismo de grupos. Como contraexemplo, podemos considerar a aplicação $\varphi : \mathbb{Z}_5 \to \mathbb{Z}_6$, definida por $\varphi([x]_5) = [x]_6$. Temos

$$\varphi([2]_5 \oplus [4]_5) = \varphi([1]_5) = [1]_6 \neq [0]_6 = [2]_6 \oplus [4]_6 = \varphi([2]_5) \oplus \varphi([4]_5).$$

Prova-se que $\varphi : Z_n \to Z_m$, definida por $\varphi([x]_n) = [x]_m$ é um morfismo de grupos se e só se $m \mid n$.

Proposição. Sejam G_1 e G_2 dois grupos. Se $\psi : G_1 \longrightarrow G_2$ é um morfismo então $\psi(1_{G_1}) = 1_{G_2}$.

Demonstração. Temos que

$$1_{G_1} 1_{G_1} = 1_{G_1},$$

pelo que

$$\psi(1_{G_1})\,\psi(1_{G_1}) = \psi(1_{G_1} 1_{G_1}) = \psi(1_{G_1}).$$

Por outro lado, como $\psi(1_{G_1}) \in G_2$, temos que

$$\psi(1_{G_1})\,1_{G_2} = \psi(1_{G_1}).$$

Logo,

$$\psi(1_{G_1})\,\psi(1_{G_1}) = \psi(1_{G_1})\,1_{G_2},$$

pelo que, pela lei do corte,

$$\psi(1_{G_1}) = 1_{G_2}. \qquad \square$$

Proposição. Sejam G_1 e G_2 dois grupos e $\psi : G_1 \longrightarrow G_2$ um morfismo. Então $[\psi(x)]^{-1} = \psi\left(x^{-1}\right)$.

Demonstração. Seja $x \in G_1$. Então,

$$\psi(x)\,\psi\left(x^{-1}\right) = \psi\left(xx^{-1}\right) = \psi(1_{G_1}) = 1_{G_2}$$

e

$$\psi\left(x^{-1}\right)\psi(x) = \psi\left(x^{-1}x\right) = \psi(1_{G_1}) = 1_{G_2}.$$

Logo, pela própria definição de inverso, $[\psi(x)]^{-1} = \psi\left(x^{-1}\right)$. $\square$

Proposição. Sejam G_1 e G_2 dois grupos, $H \subseteq G_1$ e $\psi : G_1 \to G_2$ um morfismo. Então,

$$H < G_1 \Rightarrow \psi(H) < G_2.$$

Demonstração. Seja $H < G_1$. Então:

1. $\psi(H) \neq \emptyset$, pois
$$1_{G_1} \in H \Rightarrow \psi\left(1_{G_1}\right) \in \psi(H);$$
2. Sejam $a, b \in \psi(H)$. Então,
$$(\exists x, y \in H) \quad a = \psi(x) \quad \text{e} \quad b = \psi(y).$$
Assim,
$$(\exists x, y \in H) \quad ab = \psi(x)\,\psi(y) = \psi(xy),$$
pelo que $z = xy \in H$ é tal que $ab = \psi(z)$. Logo, $ab \in \psi(H)$;
3. Seja $a \in \psi(H)$. Então, existe $x \in H$ tal que $a = \psi(x)$. Como
$$a = \psi(x) \Rightarrow a^{-1} = [\psi(x)]^{-1} = \psi\left(x^{-1}\right)$$
e $x^{-1} \in H$, temos que $a^{-1} \in \psi(H)$.

Concluímos, assim, que $\psi(H) < G$. $\square$

Corolário. Seja $\psi : G_1 \longrightarrow G_2$ um morfismo de grupos. Se ψ é um monomorfismo então $G_1 \cong \psi(G_1)$. $\square$

Observação. Dois grupos finitos isomorfos têm a mesma ordem. Mas, dois grupos com a mesma ordem, não são necessariamente isomorfos. Como contraexemplo, basta pensar no grupo 4-Klein e no $\mathbb{Z}_4$.

De facto, se o grupo 4-Klein $G = \{e, a, b, c\}$ fosse isomorfo ao grupo aditivo $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ e $f : G \to \mathbb{Z}_4$ fosse um isomorfismo de grupos, teríamos

$$\overline{0} = f(e) = f(xx) = f(x) \oplus f(x),$$

para todo $x \in G$. Sendo f bijetiva, concluíamos que todos os elementos de $\mathbb{Z}_4$ eram simétricos de si próprios, o que é uma contradição, pois, em $\mathbb{Z}_4$, apenas as classes $\overline{0}$ e $\overline{2}$ são inversas de si próprias.

Proposição. Sejam G_1 e G_2 dois grupos, $H \subseteq G_1$ e $\psi : G_1 \to G_2$ um epimorfismo. Então,

$$H \lhd G_1 \Rightarrow \psi(H) \lhd G_2.$$

Demonstração. Considerando a proposição anterior, como $H < G_1$, temos que $\psi(H) << \lhd G_2$. Assim, falta apenas provar que, para $g \in G_2$ e $a \in \psi(H)$, temos que $gag^{-1} \in \psi(H)$. De facto,

$$\begin{aligned} g \in G_2, a \in \psi(H) \quad &\Rightarrow (\exists x \in G_1, h \in H)\ g = \psi(x), \quad a = \psi(h) \\ &\Rightarrow (\exists x \in G_1, h \in H)\ gag^{-1} = \psi(x)\,\psi(h)\,[\psi(x)]^{-1} \\ &\Rightarrow gag^{-1} = \psi\left(xhx^{-1}\right) \text{ com } xhx^{-1} \in H \\ &\to gag^{-1} \in \psi(H), \end{aligned}$$

pelo que $\psi(H) \lhd G_2$. $\square$

Definição. Seja $\psi : G_1 \longrightarrow G_2$ um morfimo de grupos. Chama-se *núcleo (ou kernel)* de ψ, e representa-se por $\mathrm{Nuc}\psi$ ou $\ker \psi$, ao subconjunto de G_1

$$\mathrm{Nuc}\psi = \{x \in G_1 \mid \psi(x) = 1_{G_2}\}.$$

Exemplo 32. Se $\varphi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2$ é o morfismo definido no Exemplo 31., temos que

$$\mathrm{Nuc}\varphi = \{[0]_4, [2]_4\}.$$

Exemplo 33. Sejam G_1 e G_2 grupos e $\varphi : G_1 \rightarrow G_2$ o morfismo nulo. Então, $\mathrm{Nuc}\varphi = G_1$.

Proposição. Seja $\psi : G_1 \longrightarrow G_2$ um morfismo de grupos. Então, $\mathrm{Nuc}\psi \lhd \mathrm{G}_1$.

Demonstração. Começamos por provar que $\mathrm{Nuc}\psi$ é subgrupo de G_1.

1. Observemos, primeiro, que $1_{G_1} \in \mathrm{Nuc}\psi$. De facto, $1_{G_1} \in G_1$ e $\psi\left(1_{G_1}\right) = 1_{G_2}$;
2. Sejam $a, b \in G_1$. Como $a^{-1}b \in G_1$ e

$$\begin{aligned} a, b \in \mathrm{Nuc}\psi \quad & \Rightarrow \psi(a) = \psi(b) = 1_{G_2} \\ & \Rightarrow \psi\left(a^{-1}\right) = [\psi(a)]^{-1} = 1_{G_2}^{-1} = 1_{G_2} = \psi(b) \\ & \Rightarrow \psi\left(a^{-1}b\right) = \psi\left(a^{-1}\right)\psi(b) = 1_{G_2}1_{G_2} = 1_{G_2} \end{aligned}$$

temos que

$$a, b \in \mathrm{Nuc}\psi \Rightarrow a^{-1}b \in \mathrm{Nuc}\psi.$$

Assim, concluímos que este subconjunto de G_1 é, de facto, um seu subgrupo.
Sejam $g \in G_1$ e $b \in \mathrm{Nuc}\psi$. Então,

$$gbg^{-1} \in G_1$$

e

$$\begin{aligned} \psi\left(gbg^{-1}\right) &= \psi(g)\,\psi(b)\,\psi\left(g^{-1}\right) \\ &= \psi(g)\,1_{G_2}\,[\psi(g)]^{-1} \\ &= 1_{G_2}, \end{aligned}$$

pelo que $gbg^{-1} \in \mathrm{Nuc}\psi$. Logo, $\mathrm{Nuc}\psi \lhd G_1$. $\square$

O núcleo de um morfismo de grupos $\psi : G_1 \to G_2$ define uma relação de congruência, a saber

$$\begin{aligned} x \equiv y \,(\operatorname{mod} \operatorname{Nuc}\psi) \quad &\Leftrightarrow xy^{-1} \in \operatorname{Nuc}\psi \\ &\Leftrightarrow \psi\left(xy^{-1}\right) = 1_{G_2} \\ &\Leftrightarrow \psi(x)\,[\psi(y)]^{-1} = 1_{G_2} \\ &\Leftrightarrow \psi(x) = \psi(y)\,. \end{aligned}$$

Pelo que acabámos de ver, a demonstração da proposição seguinte é trivial.

Proposição. Seja $\psi : G_1 \to G_2$ um morfismo de grupos. Então, ψ é um monomorfismo se e só se $\operatorname{Nuc}\psi = \{1_{G_1}\}$. □

Proposição. Sejam G um grupo e $H \lhd G$. Então,

$$\begin{aligned} \pi : G &\longrightarrow G/H \\ x &\longmapsto xH \end{aligned}$$

é um epimorfismo (ao qual se chama *epimorfismo canónico*) tal que $\mathrm{Nuc}\pi = H$.

Demonstração. Sejam G um grupo e $H \lhd G$.

Então, para $x, y \in G$,

$$\psi(xy) = (xy)H = xHyH = \psi(x)\psi(y),$$

pelo que π é um morfismo. Além disso, ψ é obviamente sobrejetiva (cada classe é imagem por π do seu representante). Por fim,

$$\begin{aligned} x \in \mathrm{Nuc}\pi &\Leftrightarrow \pi(x) = H \\ &\Leftrightarrow xH = H \Leftrightarrow x \in H. \qquad \square \end{aligned}$$

Os resultados que estudámos no final da secção anterior dizem-nos que:

(i) Dado um morfismo qualquer entre dois grupos, o seu núcleo é um subgrupo normal do domínio;

(ii) Dado um subgrupo normal de um grupo, existe um morfismo cujo núcleo é aquele subgrupo.

Considerando as duas situações em simultâneo, temos que:
se $\psi : G \to G'$ é um morfismo de grupos, então, por (i),

$$\mathrm{Nuc}\psi \lhd G.$$

Logo, por (ii), $\pi : G \to G/_{\mathrm{Nuc}\psi}$ é um epimorfismo tal que

$$\mathrm{Nuc}\pi = \mathrm{Nuc}\psi.$$

Teorema Fundamental do Homomorfismo. Seja $\theta : G \longrightarrow G'$ um morfismo de grupos. Então,

$$\mathrm{Im}\,\theta \cong G/_{\mathrm{Nuc}\,\theta}.$$

Demonstração. Sejam $K = \mathrm{Nuc}\,\theta$ e $\phi : G/_K \longrightarrow G'$ tal que

$$\phi\,(xK) = \theta\,(x)\,, \qquad \forall x \in G.$$

$$\begin{tikzcd}
G \arrow[r, "\theta"] \arrow[d, "\pi"'] & G' \\
G/\mathrm{Nuc}\,\theta \arrow[ur, "\phi"'] &
\end{tikzcd}$$

Estará a função ϕ bem definida, i.e., se $xK = yK$ será que $\theta(x) = \theta(y)$? SIM. De facto,

$$\begin{aligned} xK = yK \quad &\Leftrightarrow x^{-1}y \in K \,(= \mathrm{Nuc}\,\theta) \\ &\Leftrightarrow \theta\left(x^{-1}y\right) = 1_{G'} \\ &\Leftrightarrow \theta(x) = \theta(y)\,. \end{aligned}$$

Além disso, demonstrámos ainda que $\theta(x) = \theta(y) \Rightarrow xK = yK$, i.e., que

$$\phi(xK) = \phi(yK) \Rightarrow xK = yK,$$

pelo que ϕ é injectiva.

Mais ainda,

$$\begin{aligned} \mathrm{Im}\,\phi \quad &= \{\phi(xK) \mid x \in G\} \\ &= \{\theta(x) \mid x \in G\} \\ &= \mathrm{Im}\,\theta. \end{aligned}$$

Observamos, por último, que ϕ é um morfismo, já que

$$\phi(xKyK) = \phi(xyK) = \theta(xy) = \theta(x)\,\theta(y) = \phi(xK)\,\phi(yK)\,.$$

Concluímos, então, que ϕ é um monomorfismo cujo conjunto imagem (que é isomorfo ao seu domínio) é igual a $\mathrm{Im}\theta$.

Logo,

$$\mathrm{Im}\,\theta \cong G/_{K} = G/_{\mathrm{Nuc}\,\theta}.$$

$\square$