subgrupos normais e grupos quociente

Definição. Sejam G um grupo e $H < G$. Diz-se que H é *subgrupo normal* ou *invariante* de G, e escreve-se $H \lhd G$, se

$$\forall x \in G,\ xH = Hx.$$

Exemplo 25.

$\circ$	ρ_1	ρ_2	ρ_3	θ_1	θ_2	θ_3
ρ_1	ρ_1	ρ_2	ρ_3	θ_1	θ_2	θ_3
ρ_2	ρ_2	ρ_3	ρ_1	θ_3	θ_1	θ_2
ρ_3	ρ_3	ρ_1	ρ_2	θ_2	θ_3	θ_1
θ_1	θ_1	θ_2	θ_3	ρ_1	ρ_2	ρ_3
θ_2	θ_2	θ_3	θ_1	ρ_3	ρ_1	ρ_2
θ_3	θ_3	θ_1	θ_2	ρ_2	ρ_3	ρ_1

Considere-se o grupo diedral do triângulo, D_3.

Então, o subgrupo $H = \{\rho_1, \theta_1\}$ não é normal pois, por exemplo,

$$\theta_2 H = \{\theta_2, \rho_3\} \neq \{\theta_2, \rho_2\} = H\theta_2.$$

No entanto, se considerarmos o subgrupo $K = \{\rho_1, \rho_2, \rho_3\}$, temos que $K \lhd D_3$, uma vez que

$$\rho_1 K = K\rho_1 = \rho_2 K = K\rho_2 = \rho_3 K = K\rho_3 = K = \{\rho_1, \rho_2, \rho_3\}$$

e

$$\theta_1 K = K\theta_1 = \theta_2 K = k\theta_2 = \theta_3 K = K\theta_3 = \{\theta_1, \theta_2, \theta_3\}.$$

Proposição. Dado um grupo G qualquer, o subgrupo trivial e o subgrupo impróprio são subgrupos normais de G. $\square$

Proposição. Seja G um grupo abeliano. Então, qualquer subgrupo H de G é normal em G. $\square$

Proposição. Seja G um grupo. Então, o centro de G, $Z(G) = \{x \in G : \forall a \in G, ax = xa\}$ é um subgrupo invariante G. $\square$

Proposição. Sejam G um grupo e $H < G$ tal que $[G : H] = 2$. Então, $H \triangleleft G$. $\square$

Vimos já que a comutatividade num grupo G implica a normalidade dos subgrupos. Assim, podemos afirmar que se H é um subgrupo de G tal que, para todos $a \in G$ e $h \in H$, $ah = ha$, então $H \lhd G$.

Reciprocamente, se H é um subgrupo normal de G o que podemos afirmar é que

$$\forall a \in G,\ \forall h_1 \in H,\ \exists h_2 \in H:\ \ ah_1 = h_2 a.$$

Teorema. Sejam G um grupo e $H < G$. Então,

$$H \lhd G \iff (\forall x \in G)\,(\forall h \in H) \quad xhx^{-1} \in H.$$

Demonstração. [$\Rightarrow$] Suponhamos que $H \lhd G$. Então, para todo $x \in G$,

$$xH = Hx.$$

Sejam $g \in G$ e $h \in H$. Temos que existe $h' \in H$

$$ghg^{-1} = (gh)\,g^{-1} = (h'g)\,g^{-1} = h'\left(gg^{-1}\right) = h',$$

pelo que $ghg^{-1} \in H$.

[$\Leftarrow$] Suponhamos que, para todos $x \in G$ e $h \in H$,

$$xhx^{-1} \in H.$$

Queremos provar que $H \lhd G$.

Seja $g \in G$. Então,

$$\begin{aligned} y \in gH \quad & \Leftrightarrow \quad (\exists h' \in H) \quad y = gh' \\ & \Leftrightarrow \quad (\exists h' \in H) \quad y = gh'\left(g^{-1}g\right) \\ & \Leftrightarrow \quad (\exists h' \in H) \quad y = \left(gh'g^{-1}\right)g \\ & \Rightarrow \quad y \in Hg \qquad \textit{por hipótese}, \end{aligned}$$

pelo que $gH \subseteq Hg$. De modo análogo, prova-se que $Hg \subseteq gH$ e, portanto, $Hg = gH$. $\square$

Proposição. Sejam G um grupo e H_1 e H_2 dois subgrupos normais de G. Então,

1. $H_1 \cap H_2 \lhd G$;
2. $H_1 H_2 \lhd G$.

Observação. É óbvio que, se um grupo G admite um subgrupo normal H, as relações $\equiv^e \pmod{H}$ e $\equiv^d \pmod{H}$ são uma e uma só relação de congruência. De facto,

$$\begin{aligned} x \equiv^e y \pmod{H} \quad &\Leftrightarrow x^{-1}y \in H \Leftrightarrow y \in xH = Hx \\ &\Leftrightarrow yx^{-1} \in H \Leftrightarrow x \equiv^d y \pmod{H}. \end{aligned}$$

Assim, fala-se de uma única relação $\equiv \pmod{H}$, que, por sua vez, define um único conjunto quociente, que se representa por G/H. Logo,

$$G/H = \{xH \mid x \in G\} = \{Hx \mid x \in G\}.$$

Proposição. Sejam G um grupo e $H \lhd G$. Então, G/H é grupo, se considerarmos o produto de subconjuntos de G.

Demonstração. Sejam $x, y \in G$. Então,

$$xHyH = xyHH = xyH,$$

pelo que G/H é fechado para o produto.

Mais ainda, a operação é associativa, H é o seu elemento neutro e cada classe xH admite a classe $x^{-1}H$ como elemento inverso. □

Definição. Sejam G um grupo e $H \lhd G$. Ao grupo G/H chama-se *grupo quociente*.

Exemplo 26. Considere-se o subgrupo $3\mathbb{Z} = \{3k : k \in \mathbb{Z}\}$ do grupo (aditivo) $\mathbb{Z}$. Como a adição usual de inteiros é comutativa, concluímos que $3\mathbb{Z} \lhd \mathbb{Z}$. Como estamos a trabalhar com a linguagem aditiva, temos que, dados $x, y \in \mathbb{Z}$,

$$x \equiv y \pmod{3\mathbb{Z}} \Leftrightarrow x-(-y) \in 3\mathbb{Z} \Leftrightarrow x-y = 3k, \text{ para algum } k \in \mathbb{Z} \Leftrightarrow x \equiv y \pmod 3.$$

Assim, temos que

$$\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\} = \mathbb{Z}_3.$$

Proposição. Sejam G um grupo e θ uma relação de congruência definida em G. Então, a classe de congruência do elemento identidade, $[1_G]_\theta$, é um subgrupo normal de G. Mais ainda, para $x, y \in G$,

$$x\,\theta\,y \Longleftrightarrow x^{-1}y \in [1_G]_\theta\,.$$

Observação. Com o que vimos até agora, é claro que existe uma relação biunívoca entre o conjunto das congruências possíveis de definir num grupo e o conjunto dos subgrupos normais nesse mesmo grupo: Cada subgrupo normal H de um grupo G define uma relação de congruência em G (relação mod H) e cada relação de congruência em G origina um subgrupo normal de G (a classe do elemento identidade).

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 27. 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 $\varphi(xy) = 1_{G_2} = 1_{G_2}1_{G_2} = \varphi(x)\varphi(y)$.

Exemplo 28. 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 29. 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):

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

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 $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_5$, definida por $\varphi([x]_6) = [x]_5$. Temos

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

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

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

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

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

$\square$

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,

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

$\square$

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

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

Exemplo 31. Sejam G_1 e G_2 grupos e $\varphi : G_1 \to G_2$ o morfismo nulo. Então, $\mathrm{Nuc}\varphi = G_1$.

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

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

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

Proposição. Seja $\psi : G_1 \to G_2$ um morfismo de grupos. Então, ψ é um monomorfismo se e só se $\mathrm{Nuc}\psi = \{1_{\mathrm{G}_1}\}$. $\square$

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

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

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,

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

teorema fundamental do homomorfismo

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,

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

$\square$

Lema. Sejam $\psi : G \to G'$ um morfismo de grupos e $K < G$. Então,

$$\mathrm{Nuc}\psi \subseteq K \Rightarrow \psi^{-1}(\psi(K)) = K.$$

1º Teorema do Isomorfismo. Sejam G e G' dois grupos e $\psi : G \longrightarrow G'$ um epimorfismo. Seja $K \lhd G$ tal que $\mathrm{Nuc}\psi \subseteq K$. Então,

$$G/_K \cong G'/_{\psi(K)}.$$

$$\begin{tikzcd}
G \arrow[r, "\psi"] \arrow[d, "\pi"] & G' \arrow[d, "\pi'"] \\
G/K \arrow[r, "\theta"] & G'/\psi(K)
\end{tikzcd}$$

Lema. Sejam G um grupo e $H < G$ e $H' \lhd G$. Então, $HH' < G$. $\square$

Lema. Sejam G um grupo e $H < G$ e $H' \lhd G$. Então, se $H' \subseteq H$, então, $H' \lhd H$. $\square$

2º Teorema do Isomorfismo. Sejam G um grupo e $H, T < G$ tal que $T \lhd G$. Então,

$$(HT)/_{T} \cong H/_{(H \cap T)}.$$