

1 Subgrupos normais, grupos quocientes e homomorfismos

Nesta seção discutiremos noções importantes para a continuidade dos nossos estudos em teoria de grupos. Já discutimos sobre subgrupos, veremos agora uma subclasse importante deles.

Definição 1. Sejam G um grupo. um subgrupo H de G é dito **normal** se para todo $x \in G$ temos $xHx^{-1} \subset H$. Denotamos $H \triangleleft G$.

Não é fácil em geral decidir se um subgrupo de um dado grupo é normal ou não. O seguinte lema é útil para abordar problemas concretos nessa direção.

Lema 1. *Sejam G um grupo e $H \leq G$. As seguintes condições são equivalentes:*

1. $H \triangleleft G$.
2. Para todo $x \in G$ temos $xHx^{-1} = H$.
3. Para todo $x \in G$ temos $xH = Hx$.

Demonstração. 1) $\Rightarrow$ 2): Se H é normal em G , então $xHx^{-1} \subset H$, para todo $x \in G$. Resta provar que para todo $x \in G$, temos $H \subseteq xHx^{-1}$. De fato, sejam $h \in H$ e $x \in G$. Temos

$$h = g(g^{-1}hg)g^{-1} \in g(g^{-1}Hg)g^{-1} \stackrel{1)}{\subseteq} gHg^{-1}$$

. 1) $\Rightarrow$ 2) e 3) $\Rightarrow$ 1) são imediatos. □

Exemplo 1. Seja G um grupo. Então $Z(G) \triangleleft G$ e $[G, G] \triangleleft G$.

Exemplo 2. O grupo $D(n)$ das matrizes diagonais quadradas de ordem n é um subgrupo normal de $GL(n)$

O seguinte lema é bastante útil para demonstrar que um dado subgrupo de um grupo é normal.

Lema 2. Se G é um grupo e $H < G$ tal que $(G : H) = 2$ então $H \triangleleft G$

Demonstração. Exercício! □

Subgrupos normais são particularmente importantes pois é graças a eles que podemos definir grupos quocientes. Note que dado G um grupo e $H < G$, podemos definir o conjunto $G/H := \{xH ; x \in G\}$ das classes laterais a direita de H em G . Não é verdade em geral que se munirmos G/H da operação induzida de G , que G/H é um grupo, mas se H for um subgrupo normal isso sempre será verdade como veremos a seguir.

Teorema 1. Sejam G um grupo e $H \triangleleft G$. O conjunto $G/H := \{xH ; x \in G\}$ das classes laterais a direita de H em G , é um grupo, com a operação definida por

$$\begin{aligned} \psi : G/H \times G/H &\rightarrow G/H \\ (xH, yH) &\mapsto xyH. \end{aligned}$$

Demonstração. A prova é uma mera checagem da validade dos axiomas de grupo.

G1) Sejam $x, y, z \in G$, e considere $(xHyH)zH = (xyH)zH = (xy)zH = x(yz)H = xH(yzH) = xH(yHzH)$.

G2) O elemento neutro de G/H é a classe lateral de H . De fato, seja $x \in G$, então $(xH)H = xH = Hx = HHx$, pois H é normal.

G3) Seja $x \in G$, então $x^{-1} \in G$ e $xHx^{-1} = xx^{-1}H = H$.

Portanto G/H é um grupo. □

O grupo das classes laterais do Teorema 1 anterior é dito **grupo quociente** de G por H .

Observação. Nas condições do Teorema 1, observe que G/H é formado pelas classes laterais tanto à direita quanto à esquerda, e não há diferença entre elas, uma vez que $xH = Hx$ para todo $x \in G$.

Exemplo 3. Seja $\mathbb{Z}$ o grupo aditivo dos inteiros. Considere o grupo cíclico gerado pelo inteiro n , isto é $\langle n \rangle := \{0, n, 2n, \dots\}$, o grupo quociente $\mathbb{Z}_n := \mathbb{Z}/\langle n \rangle$, é o grupo das classes dos restos da divisão por n .

Veremos a seguir como podemos relacionar diferentes grupos, através de operações que respeitem suas estruturas.

Definição 2. Sejam $(G_1, *_1)$ e $(G_2, *_2)$ dois grupos. Um **homomorfismo (de grupos)** é uma função $f : G_1 \rightarrow G_2$ satisfazendo $f(x *_1 y) = f(x) *_2 f(y)$ para quaisquer $x, y \in G_1$.

Exemplo 4. Seja $G_1 = \text{GL}(n, \mathbb{R})$ o grupo geral linear e $G_2 = (\mathbb{R} \setminus \{0\}, *)$ o grupo multiplicativo real. A função determinante $\det : G_1 \rightarrow G_2$, é um homomorfismo de grupos.

Definição 3. Um homomorfismo $f : G_1 \rightarrow G_2$ um é dito:

1. **monomorfismo**, se f é injetora.
2. **epimorfismo**, se f é sobrejetora.
3. **isomorfismo**, se f é bijetora. Neste caso dizemos que G_1 e G_2 são **isomorfos** e denotamos por $G_1 \simeq G_2$.

Um isomorfismo f é um **automorfismo** se $G_1 = G_2$.

Exemplo 5. 1. Sejam G um grupo e $x \in G$. A aplicação $f : \mathbb{Z} \rightarrow G$, definida por $f(n) = x^n$ é um homomorfismo.

2. Seja G um grupo comutativo. A aplicação $f : G \rightarrow G$, definida por $f(x) = x^{-1}$ é um automorfismo de G .

3. Sejam G um grupo e $y \in G$. A aplicação $\gamma_y : G \rightarrow G$, definida por $\gamma_y(x) = yxy^{-1}$ é um automorfismo de G , chamado **conjugação** por y .

Proposição 1. Sejam $f : G_1 \rightarrow G_2$ e $g : G_2 \rightarrow G_3$ um homomorfismo. Então:

1. $g \circ f$ é um homomorfismo.
2. Se f é isomorfismo, então f^{-1} é um isomorfismo.

Definição 4. Sejam $f : G_1 \rightarrow G_2$ um homomorfismo e e_2 o elemento neutro de G_2 .

1. O subconjunto

$$\ker(f) = \{x \in G_1 ; f(x) = e_2\}$$

é dito **núcleo** de f .

2. O subconjunto

$$\text{Im}(f) = \{f(x) \in G_2 ; x \in G_1\}$$

é dito **imagem** de f .

Exemplo 6. Retomando o exemplo em que consideramos o homomorfismo dado pela função determinante, vemos que $\ker \det = \text{SL}(n, \mathbb{R})$

A seguinte Proposição nos será útil, e é de fácil verificação, por isso será deixada como exercício ao leitor.

Proposição 2. *Seja $f : G_1 \rightarrow G_2$ um homomorfismo de grupos e $x \in G_1$.*

1. *Se e_1 e e_2 são os elementos neutros de G_1 e G_2 , respectivamente, então $f(e_1) = e_2$.*
2. *Para qualquer $x \in G_1$, temos $f(x^{-1}) = (f(x))^{-1}$.*
3. *f é monomorfismo se, e somente se, $\ker(f) = e_1$.*
4. *Se $o(x) < \infty$, então $o(f(x))$ divide $o(x)$.*

Também é imediato verificar que:

Proposição 3. *Sejam G um grupo, $H \triangleleft G$ e G/H o grupo quociente. A função*

$$\begin{aligned} \pi : G &\rightarrow G/H \\ x &\mapsto xH \end{aligned}$$

é um homomorfismo e seu núcleo é precisamente H .

Chamamos o homomorfismo π do Corolário 1 de **homomorfismo canônico** de G no grupo quociente G/H .

Teorema 2 (do Isomorfismo I). *Seja $f : G_1 \rightarrow G_2$ um homomorfismo. Então:*

1. $K := \ker(f)$ é um subgrupo normal de G_1 .
2. Existe um único isomorfismo $\hat{f} : G_1/K \rightarrow \text{Im}(f)$ tal que $\hat{f} \circ \pi = f$, onde $\pi : G \rightarrow G/K$ é o homomorfismo canônico.

Demonstração. 1. Seja $g \in G_1$. Vamos mostrar que $gKg^{-1} \subseteq K$. Para todo $k \in K$, temos

$$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)e_{G_2}f(g)^{-1} = e_{G_2}.$$

Logo, $gkg^{-1} \in K$ e portanto $K \triangleleft G_1$.

2. Primeiramente vamos demonstrar a existência do isomorfismo.

Seja $I := \text{Im}(f)$. Considere a função $\hat{f} : G/K \rightarrow I$, definida por $\hat{f}(gK) = f(g)$, vamos mostrar que $\hat{f}$ é isomorfismo.

- (a) $\hat{f}$ está bem definida, ou seja, $\hat{f}$ não depende do representante escolhido.

Dadas $g_1K, g_2K \in G/K$ com $g_1K = g_2K$ (i.e. $(g_2)^{-1}g_1 \in K$), $\hat{f}(g_1K) = f(g_1)$ e $\hat{f}(g_2K) = f(g_2)$. Segue que

$$(f(g_2))^{-1}f(g_1) = f((g_2)^{-1})f(g_1) = f((g_2)^{-1}g_1) = e_{G_2}.$$

Logo $f(g_1) = f(g_2)$.

- (b) $\hat{f}$ é homomorfismo.

Dados $g_1K, g_2K \in G/K$, temos

$$\hat{f}(g_1Kg_2K) = \hat{f}(g_1g_2K) = f(g_1g_2) = f(g_1)f(g_2) = \hat{f}(g_1K)\hat{f}(g_2K).$$

- (c) $\hat{f}$ é isomorfismo.

De fato, dado $gK \in G/K$ se $\hat{f}(gK) = e_{G_2}$, temos $f(g) = e_{G_2}$, ou seja, $g \in K$. Logo $gK = K$ e $\hat{f}$ é monomorfismo.

E por fim, dado $g' \in I$, existe $g \in G_1$ tal que $f(g) = g'$. Considere a classe $gK \in G/K$, segue que $\hat{f}(gK) = f(g) = g'$, logo $\hat{f}$ é sobrejetora.

(d) $\hat{f} \circ \pi = f$.

De fato, dado $g \in G_1$, temos

$$\hat{f} \circ \pi(g) = \hat{f}(\pi(g)) = \hat{f}(gK) = f(g).$$

Agora vamos demonstrar a unicidade. Suponha que exista outro isomorfismo $\tilde{f} : G/K \rightarrow I$ tal que $\tilde{f} \circ \pi = f$. Logo $\tilde{f} \circ \pi = \hat{f} \circ \pi$ e como π é sobrejetor temos $\tilde{f} = \hat{f}$.

□

Temos a seguinte importante caracterização de subgrupos normais.

Corolário 1. *Sejam G um grupo, $H < G$ então G/H é um grupo se, e somente se, $H \triangleleft G$.*

Demonstração. Se H é subgrupo normal, temos por definição que G/H é grupo. Por outro lado, suponha que G/H , e considere a projeção canônica $\pi G \rightarrow G/H$. É claro que π é um homomorfismo de onde segue que $\ker \pi = H$, e portanto, pelo Primeiro Teorema do isomorfismo temos que H é normal. □

Exemplo 7. Segue do Exemplo 6, que $\text{SL}(n, \mathbb{R})$ é um subgrupo normal de $\text{GL}(n, \mathbb{R})$.

Teorema 3 (do Isomorfismo II). *Sejam H e K subgrupos de G , com $H \triangleleft G$. Então:*

1. $H \cap K \triangleleft H$
2. $K/(H \cap K) \simeq KH/H$

Teorema 4 (do Isomorfismo III). *Sejam H e K subgrupos normais de G , com $K \subseteq H \subseteq G$. Então:*

$$(G/K)/(H/K) \simeq G/H.$$

Teorema 5 (da Correspondência). *Sejam $f : G_1 \rightarrow G_2$ um homomorfismo sobrejetivo, com $K := \ker(f)$. Então:*

1. Se $H \leq G_1$, então $H' := f(H) = \{f(h) ; h \in H\} \leq G_2$. Mais ainda, se $H \triangleleft G_1$, então $H' \triangleleft G_2$.
2. Se $H' \leq G_2$, então $\exists! H \supseteq K$, $H \leq G_1$ tal que $f(H) = H'$. Mais ainda, se $H' \triangleleft G_2$, então $H \triangleleft G_1$.

Demonstração. 1. Como $f(e_{G_1}) = e_{G_2}$, temos $H' \neq \emptyset$. E mais, sejam $h'_1 = f(h_1), h'_2 = f(h_2) \in H'$, temos

$$h'_1 h'_2 = f(h_1) f(h_2) = f(h_1 h_2).$$

Logo, $h'_1 h'_2 \in H'$. E mais,

$$(h'_1)^{-1} = f(h_1)^{-1} = f(h_1^{-1}).$$

Logo $(h'_1)^{-1} \in H'$. portanto, $H' \leq G_2$.

Por fim, se $H_1 \triangleleft G_1$, como f é sobrejetivo, dado $y \in G_2$ existe $x \in G_1$ tal que $f(x) = y$. Logo, dado $h'_1 = f(h_1) \in H'$, temos

$$y h'_1 y^{-1} = f(x) f(h_1) f(x^{-1}) = f(x h_1 x^{-1}),$$

mas como $H_1 \triangleleft G_1$, temos $x h_1 x^{-1} = h_2 \in H$. E portanto $H' \triangleleft G_2$.

2. Considere o conjunto $H = \{h \in G_1 ; f(h) \in H'\}$. Como $e_{G_2} \in H'$, temos $K \subset H$. E mais, dados $h_1, h_2 \in H$, com $f(h_1) = h'_1$ e $f(h_2) = h'_2$, temos

$$f(h_1 h_2) = f(h_1) f(h_2) = h'_1 h'_2 \in H',$$

$$f(h_1^{-1}) = f(h_1)^{-1} = (h'_1)^{-1} \in H',$$

logo $h_1 h_2, h_1^{-1} \in H$ e portanto $H \leq G_1$.

Por fim, dados $x \in G_1$ e $h_1 \in H$, com $f(x) = y$ e $f(h_1) = h'_1$, temos

$$f(x h_1 x^{-1}) = f(x) f(h_1) f(x^{-1}) = f(x) f(h_1) f(x)^{-1} = y h'_1 y^{-1} \in H',$$

pois $H' \triangleleft G_2$. Portanto $H \triangleleft G_1$.

□

Muitas vezes o resultado acima é enunciado da seguinte (importantíssima!!) maneira.

Teorema 6 (da Correspondência-BIS). *Sejam G um grupo, e $H \triangleleft G$. Então existe uma correspondência biunívoca entre:*

$$\{\text{Subgrupos normais de } G/H\} \leftrightarrow \{\text{Subgrupos normais de } G \text{ que contém } H\}$$

Demonstração. Considere a projeção canônica $\pi : G \rightarrow G/H$. Já vimos que $\ker \pi = H$, logo aplicando o Teorema 5, temos o resultado. $\square$

Exercícios

1. Prove que se G é um grupo e $H < G$ tal que $(G : H) = 2$ então $H \triangleleft G$.
2. Dê exemplo de um grupo G e um subgrupo H de modo que a operação induzida de G em G/H **NÃO** define um grupo (Sugestão: Olhe para subgrupos de S_3).
3. Prove a Proposição 1
4. Seja G um grupo. Definimos como $G' := \{[x, y]; x, y \in G\}$, o grupo gerado pelos comutadores dos elementos de G , e dizemos que G' é o **grupo derivado** de G . Prove que G/G' é abeliano.
5. Prove que se G e H são grupos cíclicos de mesma ordem, então G e H são isomorfos.
6. Prove que todo grupo de ordem menor ou igual a 5 é abeliano.
7. Prove que todo grupo de ordem 9 é abeliano(*).
8. Mostre que, apesar dos exercícios 7 e 6, nem todo grupo de ordem menor que 9 é abeliano.
9. Seja $\varphi : G_1 \rightarrow G_2$ um homomorfismo de grupos finitos e $H < G_1$. Prove que $|\varphi(H)|$ divide $|H|$.

10. Quantos homomorfismos de grupos existem entre $\mathbb{Z}_{20}$ e $\mathbb{Z}_{10}$
11. Quantos homomorfismos de grupos existem entre $\mathbb{Z}_m$ e $\mathbb{Z}_n$ (*)
12. Suponha que G é um grupo abeliano finito e que um número primo p divide a ordem de G , prove que a equação $x^p = e$ admite solução em G . (*)
13. Seja G um grupo finito abeliano e p um número primo tal que p^n divide $|G|$ e p^{n+1} não divide $|G|$, então G possui um subgrupo de ordem p . Este problema é conhecido como Teorema de Sylow para grupos abelianos. (*)