

Subgrupos normais

Definição

Um subgrupo H de um grupo G diz-se um subgrupo normal de G se $aH = Ha$, para todo o $a \in G$. Usa-se a notação $H \trianglelefteq G$.

Proposição

Um subgrupo H de um grupo G é normal em G se e só se $xHx^{-1} \subseteq H$, qualquer que seja $x \in G$.

Demonstração. Se H é normal em G , então, para quaisquer $x \in G$ e $h \in H$, existe $h' \in H$ tal que $xh = h'x$. Logo $xhx^{-1} = h'$ e, portanto, $xHx^{-1} \subseteq H$.

Reciprocamente, se $xHx^{-1} \subseteq H$, para todo o $x \in G$, então, tomando $x = a$, tem-se $aH \subseteq Ha$. Por outro lado, tomando $x = a^{-1}$, tem-se $a^{-1}H(a^{-1})^{-1} = a^{-1}Ha \subseteq H$, ou seja, $Ha \subseteq aH$. □

Exemplo

1. Todo o subgrupo de um grupo abeliano é normal.
2. O centro $Z(G)$ de um grupo G é normal.
3. O grupo alterno A_n é um subgrupo normal do grupo simétrico S_n .
4. O subgrupo das rotações de D_4 é um subgrupo normal.

Exercício

Mostre que todo o subgrupo de índice dois de um grupo é um subgrupo normal desse grupo.

Grupos Quociente

Dados um grupo G e $H \trianglelefteq G$, o conjunto $\{aH \mid a \in G\}$ das classes laterais (esquerdas) denota-se por G/H .

Proposição

Sejam G um grupo e $H \trianglelefteq G$. O conjunto G/H é um grupo com a operação $(aH)(bH) = abH$.

Demonstração. Começamos por mostrar que a correspondência definida é de facto uma função (ou seja, que não depende dos representantes escolhidos para as classes).

Suponhamos que $aH = a'H$ e $bH = b'H$. Então $a' = ah_1$ e $b' = bh_2$, para certos $h_1, h_2 \in H$, donde $a'b'H = ah_1bh_2H = ah_1bH = ah_1Hb = aHb = abH$. Agora, observando que $eH = H$ é a identidade, $a^{-1}H$ é o inverso de aH e que é válida a associatividade concluímos que G/H é um grupo. □

O grupo G/H , com a operação dada na proposição anterior diz-se o *grupo quociente* de G por H .

Exemplo

Seja $3\mathbb{Z} = \{0, \pm 3, \pm 6, \dots\}$ o subgrupo de $\mathbb{Z}$ dos múltiplos inteiros de 3. Vamos construir o grupo quociente $\mathbb{Z}/3\mathbb{Z}$. Para o efeito consideramos as classes laterais de $3\mathbb{Z}$ em $\mathbb{Z}$:

$$0 + 3\mathbb{Z} = 3\mathbb{Z} = \{0, \pm 3, \pm 6, \dots\};$$

$$1 + 3\mathbb{Z} = \{1, 4, 7, \dots; -2, -5, -8, \dots\};$$

$$2 + 3\mathbb{Z} = \{2, 5, 8, \dots; -1, -4, -7, \dots\}.$$

(Use o algoritmo de divisão e outros conhecimentos que tem sobre classes laterais para concluir que estas são as únicas.)

A tabela de Cayley de $\mathbb{Z}/3\mathbb{Z}$ (que torna claro que $\mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}_3$) é:

	$0 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$
$0 + 3\mathbb{Z}$	$0 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$
$1 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$	$0 + 3\mathbb{Z}$
$2 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$	$0 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$

Mais geralmente, para $n > 0$, tem-se $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$.

Exercício

Considere o grupo $G = \mathbb{Z}_{12}$ e o subgrupo $H = \langle 3 \rangle$. Construa a tabela de Cayley de G/H .

A proposição seguinte mostra que um grupo quociente pode dar informação acerca do próprio grupo.

Proposição

Seja G um grupo e seja $Z(G)$ o seu centro. Se $G/Z(G)$ for cíclico, então G é abeliano.

Demonstração. Seja $gZ(G)$ um gerador do grupo quociente $G/Z(G)$ e sejam $a, b \in G$. Existem inteiros i e j tais que

$aZ(G) = (gZ(G))^i = g^i Z(G)$ e $bZ(G) = (gZ(G))^j = g^j Z(G)$. Logo $a = g^i x$ e $b = g^j y$, para alguns $x, y \in Z(G)$.

Segue-se que $ab = (g^i x)(g^j y) = g^i (xg^j) y = g^i (g^j x) y = (g^i g^j)(xy) = (g^j g^i)(yx) = (g^j y)(g^i x)$. □

Exercício

Seja H um subgrupo normal de um grupo finito G .

1. Mostre que a ordem de $gH \in G/H$ divide a ordem de g .
2. Conclua que se G/H tem um elemento de ordem n , então G tem um elemento de ordem n .

Proposição (Teorema de Cauchy para grupos abelianos)

Sejam G um grupo abeliano finito e p um divisor da ordem de G . Então G tem um elemento de ordem p .

Demonstração. Vamos usar a segunda forma do princípio de indução matemática sobre a ordem de G .

Claro que o enunciado vale se G tiver ordem 2. Vamos supor que também vale para todos os grupos com menos elementos que G e provar que então também vale para G . Note-se que G tem elementos de ordem prima, pois se $\text{ord}(x) = qn$, então x^n tem ordem q . Seja então x um elemento de G de ordem prima q , digamos. Se $q = p$, não há mais nada a provar, pelo que podemos supor $q \neq p$. Como qualquer subgrupo de um grupo abeliano é normal, podemos considerar o grupo quociente $H = G/\langle x \rangle$. H é abeliano e tem ordem um múltiplo de p . Logo, por indução, H tem um elemento de ordem p , $y\langle x \rangle$, digamos. Agora basta usar o exercício anterior.