o teorema de Lagrange

produto de subconjuntos de um grupo

Definição. Sejam G um grupo e $X, Y \subseteq G$. Chama-se *produto de X por Y*, e representa-se por XY, ao conjunto

$$XY = \begin{cases} \{xy \in G : x \in X \text{ e } y \in Y\} & \text{se } X \neq \emptyset \text{ e } Y \neq \emptyset; \\ \emptyset & \text{se } X = \emptyset \text{ ou } Y = \emptyset. \end{cases}$$

Se $X \neq \emptyset$, chama-se *inverso de X*, e representa-se por X^{-1}, ao conjunto $X^{-1} = \{x^{-1} : x \in X\}$.

Proposição. Sejam G um grupo e $\mathcal{P}(G) = \{X \mid X \subseteq G\}$. Então, $\mathcal{P}(G)$ é um semigrupo com identidade $\{1_G\}$, quando algebrizado com o produto de subconjuntos de G. □

Observação. Na prática, a proposição anterior assegura que dados um grupo G e $A, B, C \subseteq G$, podemos falar no subconjunto ABC de G, uma vez que $ABC = A(BC) = (AB)C$. É também importante referir que, de um modo geral, no semigrupo $\mathcal{P}(G)$, o elemento A^{-1} não é elemento oposto de A , como mostra o seguinte exemplo.

Exemplo. Seja $G = \{e, a, b, c\}$ o grupo de *4-Klein*, i.e., o grupo cuja operação é dada pela tabela

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

.

Se $A = \{a, b\}$, então, $A^{-1} = \{a^{-1}, b^{-1}\} = \{a, b\}$, pelo que

$$A^{-1}A = \{aa, ab, ba, bb\} = \{e, c\} \neq \{e\}.$$

Logo, no semigrupo $\mathcal{P}(G)$, o elemento A^{-1} não é o oposto do elemento A.

Notação. Dados $a \in G$ e $Y \subseteq G$, escreve-se aY para representar $\{a\}\, Y$ e Ya para representar $Y\, \{a\}$. Assim,

$$aY = \{ay \in G \mid y \in Y\}, \qquad Ya = \{ya \in G \mid y \in Y\}.$$

relações de congruência num grupo

Recordar. Dado um conjunto X, chamamos *relação binária* em X a qualquer subconjunto R de $X \times X$. Para $x, y \in X$, dizemos que x *está* R *relacionado com* y se $(x, y) \in R$ e podemos escrever $x\,R\,y$ em vez de $(x, y) \in R$.

Uma relação binária R num dado conjunto X diz-se uma *relação de equivalência* se R é:

- *Reflexiva* $(\forall x \in X,\ x\,R\,x)$;
- *Simétrica* $(\forall x, y \in X,\ x\,R\,y \Rightarrow y\,R\,x)$;
- *Transitiva* $(\forall x, y, z \in X,\ (x\,R\,y \wedge y\,R\,z \Rightarrow x\,R\,z)$.

Se num conjunto X estiver definida uma operação binária (como é o caso dos grupos), uma relação de equivalência ρ em X diz-se:

- *uma relação de congruência à esquerda* se: $\forall x, y, z \in X,\ x\,\rho\,y \Rightarrow zx\,\rho\,zy$;
- *uma relação de congruência à direita* se: $\forall x, y, z \in X,\ x\,\rho\,y \Rightarrow xz\,\rho\,yz$;
- *uma relação de congruência* se: $\forall x, y, z \in X,\ x\,\rho\,y \Rightarrow (zx\,\rho\,zy \wedge xz\,\rho\,yz)$.

Proposição. Sejam G um grupo e $H < G$. A relação $\equiv^e \pmod{H}$, definida em G por

$$\forall x, y \in G, \qquad x \equiv^e y \pmod{H} \iff x^{-1}y \in H$$

é uma relação de congruência à esquerda. □

Demonstração. Primeiro, verifiquemos que $\equiv^e \pmod{H}$ é uma relação de equivalência. De facto:

(i) Para todo $x \in G$, $x^{-1}x = 1_G \in H$, pelo que a relação é reflexiva.

(ii) Sejam $x, y \in G$ tais que $x \equiv^e y \pmod{H}$. Então,

$$x \equiv^e y \pmod{H} \Leftrightarrow x^{-1}y \in H \Rightarrow y^{-1}x = \left(x^{-1}y\right)^{-1} \in H \Leftrightarrow y \equiv^e x \pmod{H}.$$

Logo, a relação é simétrica.

(iii) Sejam $x, y, z \in G$ tais que $x \equiv^e y \pmod{H}$ e $y \equiv^e z \pmod{H}$. Então,

$$\begin{aligned} x \equiv^e y \pmod{H} \text{ e } y \equiv^e z \pmod{H} &\iff x^{-1}y \in H \text{ e } y^{-1}z \in H \\ &\Rightarrow x^{-1}z = x^{-1}yy^{-1}z \in H \\ &\iff x \equiv^e z \pmod{H}, \end{aligned}$$

pelo que a relação é transitiva.

Verifiquemos agora que a relação é compatível com a multiplicação à esquerda:

Sejam $x, y \in G$ tal que $x \equiv^e y \pmod{H}$ e $a \in G$. Queremos provar que $ax \equiv^e ay \pmod{H}$. De facto,

$$\begin{aligned} x \equiv^e y \pmod{H} &\iff x^{-1}y \in H \\ &\iff x^{-1}ey \in H \\ &\iff x^{-1}a^{-1}ay \in H \\ &\iff (ax)^{-1}ay \in H \\ &\iff ax \equiv^e ay \pmod{H}. \end{aligned}$$

Concluímos então que $\equiv^e \pmod{H}$ é uma relação de congruência à esquerda. □

Analogamente, provamos que

Proposição. Sejam G um grupo e $H < G$. A relação $\equiv^d \pmod{H}$, definida em G por

$$\forall x, y \in G, \qquad x \equiv^d y \pmod{H} \iff xy^{-1} \in H$$

é uma relação de congruência à direita. □

Definição. Sejam G um grupo e $H < G$. À relação $\equiv^e \pmod{H}$ chama-se *congruência esquerda módulo H* e à relação $\equiv^d \pmod{H}$ chama-se *congruência direita módulo H*.

Cada uma destas relações de equivalência define em G uma partição (que pode não ser necessariamente a mesma). Representando por $[a]_e$ a classe de equivalência do elemento $a \in G$ quando consideramos a congruência esquerda módulo H, temos que

$$\begin{aligned} x \in [a]_e \quad &\Leftrightarrow \quad x \equiv^e a \,(\mathrm{mod}\, H) \Leftrightarrow x^{-1}a \in H \Leftrightarrow \exists h \in H : x^{-1}a = h \\ &\Leftrightarrow \quad \exists h \in H : x^{-1} = ha^{-1} \Leftrightarrow \exists h \in H : x = ah^{-1} \Leftrightarrow x \in aH, \end{aligned}$$

pelo que

$$[a]_e = aH, \quad \forall a \in G.$$

De modo análogo, representando por $[a]_d$ a classe de equivalência do elemento $a \in G$ quando consideramos a congruência direita módulo H, temos que

$$[a]_d = Ha, \quad \forall a \in G.$$

Definição. Sejam G um grupo e $H < G$. Para cada $a \in G$, o subconjunto aH designa-se por *classe lateral esquerda de a módulo H* e o subconjunto Ha designa-se por *classe lateral direita de a módulo H.*

Exemplo 22. Seja $G = \{e, a, b, c\}$ o grupo de *4-Klein,* i.e., o grupo cuja operação é dada pela tabela

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

.

Considerando o subgrupo $H = \{e, a\}$, as classes laterais esquerdas são

$$eH = H = aH \quad \text{e} \quad bH = \{b, c\} = cH$$

e as classes laterais direitas são iguais já que o grupo é comutativo.

Exemplo 23. Seja $G = \{e, p, q, a, b, c\}$ o grupo cuja operação é dada pela tabela

$\cdot$	e	p	q	a	b	c
e	e	p	q	a	b	c
p	p	q	e	c	a	b
q	q	e	p	b	c	a
a	a	b	c	e	p	q
b	b	c	a	q	e	p
c	c	a	b	p	q	e

.

Então, considerando o subgrupo $H = \{e, a\}$, as classes laterais esquerdas são

$$eH = H = aH, \quad bH = \{b, q\} = qH \quad \text{e} \quad cH = \{c, p\} = pH$$

e as classes laterais direitas são

$$He = H = Ha, \quad Hb = \{b, p\} = Hp \quad \text{e} \quad Hc = \{c, q\} = Hq.$$

Proposição. Sejam G um grupo e $H < G$. Se H é finito então cada classe módulo H tem a mesma cardinalidade que H.

Demonstração. Sejam G um grupo e $a \in G$. As aplicações

$$\begin{array}{rccc} \lambda_a : G & \longrightarrow & G \\ x & \longmapsto & ax \end{array} \quad \text{e} \quad \begin{array}{rccc} \rho_a : G & \longrightarrow & G \\ x & \longmapsto & xa \end{array}$$

são bijecções em G. Logo, $\lambda_a|_H$ e $\rho_a|_H$ são bijecções de H em $\lambda_a(H) = aH$ e de H em $\rho_a(H) = Ha$, respetivamente. Assim, se H for finito,

$$\sharp(aH) = \sharp H = \sharp(Ha).$$

□

Proposição. Sejam G um grupo finito e $H < G$. Se $a_1H, a_2H, \ldots, a_rH$ são exatamente as classes laterais esquerdas de H em G (com $r \geq 1$ e $a_1, a_2, \ldots, a_r \in G$), então, $Ha_1^{-1}, Ha_2^{-1}, \ldots, Ha_r^{-1}$ são exatamente as classes laterais direitas de H em G.

Demonstração. Cada elemento de G pertence exatamente a uma e uma só classe lateral esquerda $a_1H, a_2H, \ldots, a_rH$. Sejam $x \in G$ e $1 \leq i \leq r$. Então,

$$\begin{aligned} x \in Ha_i^{-1} &\Leftrightarrow x\left(a_i^{-1}\right)^{-1} \in H \Leftrightarrow xa_i \in H \Leftrightarrow \left(x^{-1}\right)^{-1} a_i \in H \\ &\Leftrightarrow x^{-1} \in a_iH. \end{aligned}$$

Como a condição $x^{-1} \in a_iH$ é verdadeira para exatamente um valor de i, então também a expressão $x \in Ha_i^{-1}$ é verdadeira para exatamente um valor de i. □

Observação. No seguimento desta proposição, escrevemos

$$G/_{\equiv^e (\mathrm{mod}\, H)} = \{a_1 H, a_2 H, \ldots, a_r H\}$$

se e só se

$$G/_{\equiv^d (\mathrm{mod}\, H)} = \left\{ H a_1^{-1}, H a_2^{-1}, \ldots, H a_r^{-1} \right\}.$$

Definição. Sejam G um grupo finito e $H < G$. Chama-se:

1. *ordem do grupo* G, e representa-se por $|G|$, ao número de elementos de G;
2. *índice de* H, e representa-se por $[G : H]$, ao número de classes laterais esquerdas (ou direitas) de H em G.

Teorema. (*Teorema de Lagrange*) Sejam G um grupo finito e $H < G$. Então,

$$|G| = [G : H] \cdot |H| .$$

Demonstração. Imediata, tendo em conta que, se se considerar a partição em G definida pela congruência esquerda módulo H, temos $[G : H]$ classes, cada uma das quais com $|H|$ elementos. □

Corolário. Num grupo finito G, a ordem de cada elemento divide a ordem do grupo.

Demonstração. Imediata, tendo em conta que $o(a) = |\langle a \rangle|$, para todo $a \in G$. □

Corolário. Sejam G um grupo finito e p um primo tal que $|G| = p$. Então, existe $b \in G$ tal que $G = \langle b \rangle$.

Demonstração. Como p é primo, $p \neq 1$, pelo que $G \neq \{1_G\}$. Seja $x \in G$ tal que $x \neq 1_G$. Então,

$$\begin{aligned} o(x) \mid p \quad &\Rightarrow o(x) = p \\ &\Rightarrow |\langle x \rangle| = p \\ &\Leftrightarrow G = \langle x \rangle . \end{aligned}$$

□

O recíproco do teorema de Lagrange nem sempre é verdadeiro: o facto de a ordem de um grupo admitir um determinado fator, não implica que exista necessariamente um subgrupo desse grupo cuja ordem é esse fator.

No entanto, se esse fator é um número primo, temos:

Teorema. (*Teorema de Cauchy*) Sejam G um grupo de ordem $n \in \mathbb{N}$ e p um primo divisor de n. Então, existe um elemento $a \in G$ tal que $o(a) = p$. □

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 24. Seja $G = \{e, p, q, a, b, c\}$ o grupo cuja operação é dada pela tabela

$\cdot$	e	p	q	a	b	c
e	e	p	q	a	b	c
p	p	q	e	c	a	b
q	q	e	p	b	c	a
a	a	b	c	e	p	q
b	b	c	a	q	e	p
c	c	a	b	p	q	e

.

(ver Exemplo 23) e $H = \{e, a\}$. Então, como $bH = \{b, q\} \neq \{b, p\} = Hb$, concluímos que H não é subgrupo normal de G. No entanto, se considerarmos o subgrupo $K = \{e, p, q\}$, temos que $K \lhd G$, uma vez que

$$eK = Ke = pK = Kp = qK = Kq = K = \{e, p, q\}$$

e

$$aK = Ka = bK = Kb = cK = Kc = \{a, b, c\}.$$

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

Demonstração. Sejam G um grupo e $a \in G$. Então, como as equações $ax = b$ e $ya = b$ têm soluções únicas, para qualquer $b \in G$, temos que

$$aG = \{ag : g \in G\} = G = \{ga : g \in G\} = Ga,$$

o que permite concluir que $G \lhd G$.Além disso,

$$a\{1_G\} = \{a1_G\} = a = \{1_G a\} = \{1_G\}a,$$

ou seja, $\{1_G\} \lhd G$. □

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

Demonstração. Basta ter em conta que, se G é abeliano e $a \in G$, então, $aH = \{ah \in G : h \in H\} = \{ha \in G : h \in H\} = Ha$. □

Exemplo 25. Seja G um grupo. Então, $Z(G) \lhd G$. De facto, seja $g \in G$. Então,

$$\begin{aligned} x \in gZ(G) &\Leftrightarrow (\exists a \in Z(G)) \quad x = ga \\ &\Leftrightarrow (\exists a \in Z(G)) \quad x = ag \Leftrightarrow x \in Z(G)g. \end{aligned}$$

Exemplo 26. Sejam G um grupo e $H < G$ tal que $[G : H] = 2$. Então, $H \lhd G$. De facto, de $[G : H] = 2$, temos que existe $x \in G \backslash H$ tal que $Hx = xH$. Assim, para todo $y \in G$, como

$$yH = \begin{cases} H & \text{se } y \in H \\ xH & \text{se } y \notin H \end{cases}$$

e

$$Hy = \begin{cases} H & \text{se } y \in H \\ Hx & \text{se } y \notin H, \end{cases}$$

temos que $yH = Hy$, qualquer que seja $y \in G$. □

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,

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

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

Exemplo 27. O Teorema anterior pode ser usado para provar facilmente que a interseção de dois subgrupos normais de um mesmo grupo é ainda um subgrupo normal desse grupo.

Sejam G um grupo e H_1 e H_2 dois subgrupos normais de G. Sabemos já que $H_1 \cap H_2 < G$. Para provar que este subrupo é normal em G, basta considerar $x \in G$ e $h \in H_1 \cap H_2$ e provar que $xhx^{-1} \in H_1 \cap H_2$. De facto, se $h \in H_1 \cap H_2$, então $h \in H_1$ e $h \in H_2$.

Como $H_1 \lhd G$, $x \in G$ e $h \in H_1$, temos, pelo teorema anterior, que $xhx^{-1} \in H_1$. Analogamente, como $H_2 \lhd G$, temos que $xhx^{-1} \in H_2$. Logo $xhx^{-1} \in H_1 \cap H_2$ e, novamente pelo teorema anterior, $H_1 \cap H_2 \lhd G$.

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 28. 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 $x, y \in \mathbb{Z}$,

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

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 $x, y \in G$,

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

Demonstração. Seja G um grupo e θ uma relação de congruência em G.

Pretendemos provar, primeiro, que

$$[1_G]_\theta = \{x \in G \mid x\theta 1_G\} \lhd G.$$

De facto,

(i) $[1_G]_\theta \neq \emptyset$, pois é uma classe de congruência;
(ii) Sejam $x, y \in [1_G]_\theta$. Então,

$$x\,\theta\,1_G \Rightarrow xy\,\theta\,1_G y = y\,\theta\,1_G \Rightarrow xy\,\theta\,1_G,$$

pelo que $xy \in [1_G]_\theta$;
(iii) Seja $x \in [1_G]_\theta$. Então,

$$x\,\theta\,1_G \Rightarrow xx^{-1}\,\theta\,1_G x^{-1} \Leftrightarrow 1_G\,\theta\,x^{-1} \Rightarrow x^{-1}\,\theta\,1_G,$$

pelo que $x^{-1} \in [1_G]_\theta$.

Logo, $[1_G]_\theta$ é um subgrupo de G.

Mais ainda, sejam $x \in G$ e $a \in [1_G]_\theta$. Então,

$$a\,\theta\,1_G \Rightarrow xax^{-1}\,\theta\,x1_Gx^{-1} = xx^{-1} = 1_G,$$

pelo que $xax^{-1} \in [1_G]_\theta$ e, portanto, $[1_G]_\theta$ é invariante.

Finalmente, sejam $x, y \in G$. Então,

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

e

$$x^{-1}y \in [1_G]_\theta \Leftrightarrow x^{-1}y\,\theta\,1_G \Rightarrow xx^{-1}y\,\theta\,x1_G \Leftrightarrow y\,\theta\,x.$$

Logo,

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

□

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).