o teorema de Lagrange

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. $\square$

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

$$\begin{array}{c|cccc} \cdot & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array}.$$

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,

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

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

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

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

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

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

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

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

$$\begin{array}{c|cccc} \cdot & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array}.$$

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 24.

$$\begin{array}{c|cccccc}
\circ & \rho_1 & \rho_2 & \rho_3 & \theta_1 & \theta_2 & \theta_3 \\
\hline
\rho_1 & \rho_1 & \rho_2 & \rho_3 & \theta_1 & \theta_2 & \theta_3 \\
\rho_2 & \rho_2 & \rho_3 & \rho_1 & \theta_3 & \theta_1 & \theta_2 \\
\rho_3 & \rho_3 & \rho_1 & \rho_2 & \theta_2 & \theta_3 & \theta_1 \\
\theta_1 & \theta_1 & \theta_2 & \theta_3 & \rho_1 & \rho_2 & \rho_3 \\
\theta_2 & \theta_2 & \theta_3 & \theta_1 & \rho_3 & \rho_1 & \rho_2 \\
\theta_3 & \theta_3 & \theta_1 & \theta_2 & \rho_2 & \rho_3 & \rho_1
\end{array}.$$

Considere-se o grupo diedral do triângulo, D_3.

Então, considerando o subgrupo $H = \{\rho_1, \theta_1\}$, as classes laterais esquerdas são

$$\rho_1 H = H = \theta_1 H, \quad \theta_2 H = \{\theta_2, \rho_3\} = \rho_3 H \quad \text{e} \quad \theta_3 H = \{\theta_3, \rho_2\} = \rho_2 H$$

e as classes laterais direitas são

$$H\rho_1 = H = H\theta_1, \quad H\theta_2 = \{\theta_2, \rho_2\} = H\rho_2 \quad \text{e} \quad H\theta_3 = \{\theta_3, \rho_3\} = H\rho_3.$$

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

Proposição. Sejam G um grupo finito e $H < G$. Se $a_1 H, a_2 H, \ldots, a_r H$ 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. $\square$

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

$$G/_{\equiv^d (\mathrm{mod}\, H)} = \left\{Ha_1^{-1}, Ha_2^{-1}, \ldots, Ha_r^{-1}\right\}.$$

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. $\square$

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 $a \in G$. $\square$

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 $o(a) = p$. □