ordem de um elemento (cont.)

algumas propriedades

Proposição. Sejam G um grupo e $a, b \in G$. Então, a e $b^{-1}ab$ têm a mesma ordem.

Demonstração. Suponhamos que $o(a) = n_0$ é finita. Sabemos que $(b^{-1}ab)^{n_0} = b^{-1}a^{n_0}b$ (ver exercício 9b da folha 2). Logo, como $a^{n_0} = 1_G$, obtemos

$$(b^{-1}ab)^{n_0} = b^{-1}1_G b = b^{-1}b = 1_G.$$

Suponhamos agora que k é um inteiro positivo tal que $(b^{-1}ab)^k = 1_G$. Então,

$$\begin{aligned}(b^{-1}ab)^k = 1_G \quad &\Leftrightarrow b^{-1}a^k b = 1_G \\ &\Leftrightarrow b(b^{-1}a^k b)b^{-1} = b1_G b^{-1} \\ &\Leftrightarrow (bb^{-1})a^k(bb^{-1}) = 1_G \\ &\Leftrightarrow a^k = 1_G.\end{aligned}$$

Como a ordem de a é n_0, segue-se que $k \geq n_0$. Assim, n_0 é, de facto, o menor inteiro positivo n tal que $(b^{-1}ab)^n = 1_G$, ou seja, $o(b^{-1}ab) = n_0$.
Mostramos de seguida que, se a tiver ordem infinita, então, $b^{-1}ab$ também tem ordem infinita, usando a regra do contrarrecíproco. Suponhamos que $o(b^{-1}ab) = k$ é finita. Então, pelo que acabámos de provar, $o\left(b(b^{-1}ab)b^{-1}\right) = k$ e, portanto, $o(a) = k$ é finita. $\square$

Observação. Se G é abeliano, o resultado anterior não tem qualquer interesse porque se reduz a $o(a) = o(a)$.

Proposição. Seja G um grupo e $a \in G$ um elemento de ordem finita n. Então, para qualquer $p \in \mathbb{N}$, $o(a^p) = \frac{n}{d}$, onde $d = \mathrm{m.d.c.}(n, p)$.

Demonstração. Sejam $p \in \mathbb{N}$ e $d = \mathrm{m.d.c.}(n, p)$. Então $\frac{n}{d}, \frac{p}{d} \in \mathbb{N}$ e $d = xn + yp$, para certos $x, y \in \mathbb{N}$. Temos

$$(a^p)^{\frac{n}{d}} = (a^n)^{\frac{p}{d}} = 1_G^{\frac{p}{d}} = 1_G.$$

Se $k \in \mathbb{N}$ é tal que $(a^p)^k = 1_G$, então, como $o(a) = n$, temos que $n \mid pk$ (ponto 2 da Proposição do slide 35), i.e., $pk = nq$ para certo $q \in \mathbb{N}$.

$$\begin{aligned} d = xn + yp \quad & \Rightarrow dk = xnk + ypk = xnk + ynq = n(xk + yq) \\ & \Rightarrow k = \tfrac{n}{d}(xk + yq), \end{aligned}$$

pelo que $\frac{n}{d} \mid k$. Portanto, $o(a^p) = \frac{n}{d}$. □

Exemplo 22. Considere-se o grupo $(\mathbb{Z}_{31}^*, \otimes)$. Facilmente se verifica que, neste grupo, $o\left([2]_{31}\right) = 5$. Então,

$$o\left([8]_{31}\right) = o\left([2]_{31}^3\right) = \frac{5}{\mathrm{m.d.c.}(5, 3)} = 5.$$

Lema. Sejam G um grupo e $a, b \in G$. Então, para qualquer inteiro positivo k,

$$(ab)^k = 1_G \Leftrightarrow (ba)^k = 1_G.$$

Demonstração. Sejam a, b elementos arbitrários de um grupo G e k um inteiro positivo. Temos:

$$\begin{aligned}
(ab)^k = 1_G \quad & \Leftrightarrow (ab)^{k+1} = ab \\
& \Leftrightarrow a(ba)^k b = ab \\
& \Leftrightarrow a^{-1}\left[a(ba)^k b\right] b^{-1} = a^{-1}(ab)b^{-1} \\
& \Leftrightarrow (a^{-1}a)(ba)^k(bb^{-1}) = (a^{-1}a)(bb^{-1}) \\
& \Leftrightarrow (ba)^k = 1_G. \qquad \square
\end{aligned}$$

Corolário. Sejam G um grupo e $a, b \in G$. Se ab tem ordem finita então $o(ba) = o(ab)$.

Proposição. Sejam G um grupo e $a \in G$. Então, $o(a^{-1}) = o(a)$.

Demonstração. O resultado é imediato tendo em conta que, para todo $k \in \mathbb{Z}$,

$$a^k = 1_G \Leftrightarrow (a^{-1})^k = 1_G. \qquad \square$$

Proposição. Se a e b são elementos de ordem finita de um grupo abeliano G, então $o(ab) \mid o(a)\, o(b)$.

Demonstração. Se G é abeliano, sabemos que, para todo $n \in \mathbb{Z}$, $(ab)^n = a^n b^n$ (exercício 9 da folha 2). Assim, temos que

$$(ab)^{o(a)\,o(b)} = a^{o(a)\,o(b)} b^{o(a)\,o(b)} = (a^{o(a)})^{o(b)} (b^{o(b)})^{o(a)} = (1_G)^{o(b)} (1_G)^{o(a)} = 1_G 1_G = 1_G.$$

Pelo ponto 2 da proposição do slide 35 estamos em condições de concluir que $o(ab) \mid o(a)\, o(b)$. $\square$

Observação. Que relação terá de existir entre as ordens finitas de a e b para que a ordem de ab seja não só um divisor mas sim igual ao produto daquelas ordens?

Exemplo 23. No grupo aditivo $(\mathbb{Z}_6)$, temos que $o\left([2]_6\right) = 3$, $o\left([3]_6\right) = 2$ e $o\left([4]_6\right) = 3$.

Temos que

$$o\left([2]_6 \oplus [4]_6\right) = o\left([0]_6\right) = 1 \text{ e } o\left([2]_6\right) o\left([4]_6\right) = 3 \times 3 = 9.$$

Temos também que

$$o\left([2]_6 \oplus [3]_6\right) = o\left([5]_6\right) = 6 \text{ e } o\left([2]_6\right) o\left([3]_6\right) = 3 \times 2 = 6.$$