36. Seja G um grupo. Para cada $a \in G$, considere a aplicação $\theta_a : G \to G$ definida por $\theta_a(x) = axa^{-1}$. Mostre que:

(a) Para cada $a \in G$ a aplicação θ_a é um automorfismo de G. Para cada $a \in G$, o automorfismo θ_a designa-se por *automorfismo interno de* G;

(b) Para cada $\alpha \in \mathrm{Aut}\,(G)$ e cada $a \in G$, $\alpha\theta_a\alpha^{-1} = \theta_{\alpha(a)}$;

(c) $\{\theta_a : a \in G\}$ é um subgrupo normal do grupo $\mathrm{Aut}\,(G)$. Este subgrupo representa-se por Inn(G);

(d) A correspondência ϕ definida por $a \mapsto \theta_a$, com $a \in G$, é um morfismo de G em $\mathrm{Aut}\,(G)$;

(e) $\mathrm{Nuc}\ \phi = Z(G)$.

Resolução

(a) *Consideremos um elemento qualquer $a \in G$ e θ_a a aplicação definida conforme o enunciado. Observemos primeiro que θ_a é um morfismo. De facto, para quaisquer $x, y \in G$, temos*

$$\theta_a(xy) = a(xy)a^{-1} = (ax)(a^{-1}a)(ya^{-1}) = (axa^{-1})(aya^{-1}) = \theta_a(x)\theta_a(y).$$

Vejamos de seguida que θ_a é sobrejetiva. Seja y um elemento qualquer de G. Procuramos $x \in G$ tal que $\theta_a(x) = y$, i.e., tal que $axa^{-1} = y$. Por G ser grupo, sabemos que esta equação tem, exatamente, uma solução. Calculemo-la:

$$\begin{aligned} axa^{-1} = y \quad &\Leftrightarrow a^{-1}(axa^{-1})a = a^{-1}ya \\ &\Leftrightarrow (a^{-1}a)x(a^{-1})a = a^{-1}ya \\ &\Leftrightarrow 1_G x 1_G = a^{-1}ya \\ &\Leftrightarrow x = a^{-1}ya. \end{aligned}$$

Assim, o elemento $x \in G$ tal que $\theta_a(x) = y$ é $x = a^{-1}ya$. Finalmente, mostremos que θ_a é injetiva. Sejam $x, y \in G$ tais que $\theta_a(x) = \theta_a(y)$. Então $axa^{-1} = aya^{-1}$ e

$$\begin{aligned} axa^{-1} = aya^{-1} \quad &\Leftrightarrow a^{-1}(axa^{-1})a = a^{-1}(aya^{-1})a \\ &\Leftrightarrow (a^{-1}a)x(a^{-1}a) = (a^{-1}a)y(a^{-1}a) \\ &\Leftrightarrow 1_G x 1_G = 1_G y 1_G \Leftrightarrow x = y. \end{aligned}$$

Portanto, θ_a é um automorfismo.

(b) *Sejam $\alpha \in \mathrm{Aut}\,(G)$ e $a \in G$. Claramente $\theta_{\alpha(a)}$ e $\alpha\theta_a\alpha^{-1}$ são morfismos de G em G. Para qualquer $b \in G$, temos*

$$\begin{aligned} (\alpha\theta_a\alpha^{-1})(b) \quad &= \alpha[\theta_a[\alpha^{-1}(b)]] = \alpha[a\,\alpha^{-1}(b)a^{-1}] \\ &= \alpha(a)\,\alpha(\alpha^{-1}(b))\,\alpha(a^{-1}) \\ &= \alpha(a)b(\alpha(a))^{-1} = \theta_{\alpha(a)}(b). \end{aligned}$$

Assim, $\alpha\theta_a\alpha^{-1} = \theta_{\alpha(a)}$.

(c) *Seja $A = \{\theta_a : a \in G\}$. Pela alínea (a), A está contido no grupo $\mathrm{Aut}\,(G)$. Além disso, $\theta_{1_G} \in A$ e, portanto, $A \neq \emptyset$. Sejam θ_a, θ_b elementos arbitrários de A. Vejamos que $\theta_a\theta_b$ é ainda um elemento de A. Como $a, b \in G$ e G é grupo, $ab \in G$ e, portanto, o candidato natural de A a ser a aplicação $\theta_a\theta_b$ é θ_{ab}. Verifiquemos que, de facto, $\theta_a\theta_b = \theta_{ab}$. Ambas as aplicações têm o mesmo domínio e o mesmo conjunto de chegada, pelo que resta ver que cada elemento de G tem a mesma imagem por ambas as aplicações. Seja $x \in G$. Temos:*

$$\begin{aligned} (\theta_a\theta_b)(x) = \theta_a(\theta_b(x)) = \theta_a\left(bxb^{-1}\right) = a\left(bxb^{-1}\right)a^{-1} \\ = (ab)x(b^{-1}a^{-1}) = (ab)x(ab)^{-1} = \theta_{ab}(x). \end{aligned}$$

Portanto, $\theta_a\theta_b = \theta_{ab} \in A$. Seja $\theta_a \in A$. Começamos por observar que, como $a \in G$ e G é grupo, $a^{-1} \in G$, pelo que $\theta_{a^{-1}} \in A$. Mostremos que $(\theta_a)^{-1} = \theta_{a^{-1}}$. Dado $x \in G$, tem-se

$$\begin{aligned} (\theta_a\theta_{a^{-1}})(x) \quad &= \theta_a(\theta_{a^{-1}}(x)) = \theta_a(a^{-1}xa) \\ &= a(a^{-1}xa)a^{-1} \\ &= (aa^{-1})x(aa^{-1}) \\ &= x \end{aligned}$$

e, analogamente, $(\theta_a\theta_{a^{-1}})(x) = x$. *Portanto,* $\theta_a\theta_{a^{-1}} = \theta_{a^{-1}}\theta_a = \mathrm{id}_G$, *pelo que* $\theta_{a^{-1}} = (\theta_a)^{-1}$. *Por uma das caracterizações de subgrupo, concluimos que* $A < \mathrm{Aut}(G)$.

Finalmente, seja $\alpha \in \mathrm{Aut}(G)$. *Por (b),* $\alpha\theta_a\alpha^{-1} = \theta_{\alpha(a)}$ *e, portanto,* $\alpha A \alpha^{-1} \subseteq A$. *Logo,* $A \triangleleft \mathrm{Aut}(G)$.

(d) *Por* (a), *para cada* $a \in G$, $\theta_a \in \mathrm{Aut}(G)$. *Além disso, é claro que, dados* $a, b \in G$,

$$a = b \Rightarrow \theta_a = \theta_b,$$

uma vez que, para qualquer $x \in G$, *se tem*

$$\theta_a(x) = axa^{-1} = bxb^{-1} = \theta_b(x).$$

Assim, ϕ *é uma aplicação de* G *em* $\mathrm{Aut}(G)$. *Mostremos, de seguida, que* ϕ *respeita as operações dos grupos* G *e* $\mathrm{Aut}(G)$. *Sejam* g_1, g_2 *elementos quaisquer de* G. *Temos, por* (c), *que*

$$\phi(g_1g_2) = \theta_{g_1g_2} = \theta_{g_1}\theta_{g_2} = \phi(g_1)\phi(g_2).$$

Portanto, ϕ *é um morfismo.*

(e) *Por definição de núcleo de um morfismo, sabemos que*

$$\mathrm{Nuc}\ \phi = \{g \in G : \phi(g) = \mathrm{id}_G\}.$$

Assim,

$$\begin{aligned}\mathrm{Nuc}\ \phi &= \left\{g \in G : \theta_g = 1_{\mathrm{Aut}(G)}\right\}\\ &= \{g \in G : \theta_g(x) = \mathrm{id}_G(x),\ \textit{para todo } x \in G\}\\ &= \left\{g \in G : gxg^{-1} = x,\ \textit{para todo } x \in G\right\}\\ &= \{g \in G : gx = xg,\ \textit{para todo } x \in G\}\\ &= Z(G).\end{aligned}$$

resolução de exercícios

exercício 41. Seja G um grupo não abeliano de ordem 8.

(a) Mostre que G tem um subgrupo H tal que $|H| = 4$.

(b) Prove que $H \lhd G$.

(a) Se $|G| = 8$, sabemos que $o(x) \mid 8$, para todo $x \in G$. Assim,

$$\forall x \in G \backslash \{1_G\},\ o(x) = 2 \text{ ou } o(x) = 4 \text{ ou } o(x) = 8.$$

Suponhamos que, para todo $x \in G \backslash \{1_G\}$, $o(x) = 2$. Então, G é abeliano (recordar ex. 20), o que é uma contradição.

Logo, temos que existe $x_0 \in G \backslash \{1_G\}$ tal que $o(x_0) = 4$ ou $o(x_0) = 8$.

Se $o(x_0) = 8$, como $|G| = 8$, temos que G é cíclico e, por isso, abeliano, o que também é uma contradição.

Estamos então em condições de concluir que $o(x_0) = 4$ e, por isso, $< x_0 >$ é um subgrupo de G com ordem 4.

(b) Se $|H| = 4$ e $|G| = 8$, pelo Teorema de Lagrange, concluímos que $[G : H] = 2$. Assim, estamos em condições de concluir que $H \lhd G$ (recordar exemplo 26 das teóricas - slide 56).

exercício 42. Determine os subgrupos cíclicos de um grupo cíclico de ordem 10.

Seja $G =< a >= \{1_G, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9\}$. Podemos responder a este exercício determinando o subgrupo gerado por cada um dos elementos de G. Como sabemos que $o(a) = 10$ e $o(a^k) = \frac{10}{\text{m.d.c.}(k,10)}$, concluímos que:

- $< 1_G >= \{1_G\}$
- $< a >= G$
- $o(a^2) = 5$ e, por isso, $< a^2 >= \{1_G, a^2, (a^2)^2, (a^2)^3, (a^2)^4\} = \{1_G, a^2, a^4, a^6, a^8\}$
- $o(a^3) = 10$ e, por isso, $< a^3 >= G$
- $o(a^4) = 5$ e, por isso, $< a^4 >= \{1_G, a^4, (a^4)^2, (a^4)^3, (a^4)^4\} = \{1_G, a^4, a^8, a^2, a^6\}$
- $o(a^5) = 2$ e, por isso, $< a^5 >= \{1_G, a^5\}$
- $o(a^6) = 5$ e, por isso, $< a^6 >= \{1_G, a^6, (a^6)^2, (a^6)^3, (a^6)^4\} = \{1_G, a^6, a^2, a^8, a^4\}$
- $o(a^7) = 10$ e, por isso, $< a^7 >= G$
- $o(a^8) = 5$ e, por isso, $< a^8 >= \{1_G, a^8, (a^8)^2, (a^8)^3, (a^8)^4\} = \{1_G, a^8, a^6, a^4, a^2\}$
- $o(a^9) = 10$ e, por isso, $< a^9 >= G$

Assim, os subgrupos cíclicos de G (de facto, são todos os subgrupos de G) são:

- $\{1_G\}$
- $\{1_G, a^5\}$
- $\{1_G, a^2, a^4, a^6, a^8\}$
- G

Alternativa: Sabemos que para cada divisor k de 10, $< a^{\frac{n}{k}} >$ é um subgrupo de G com ordem igual a k. Como os divisores de 10 são 1, 2, 5 e 10, temos que $< a >= G$, $< a^5 >= \{1_G, a^5\}$,
$< a^2 >= \{1_G, a^2, a^4, a^6, a^8\}$ e $< a >= G$ são subgrupos de G.

Como $o(a^4) = \frac{10}{\mathrm{m.d.c.}(4,10)} = 5$ e $a^4 \in < a^2 >$, podemos concluir que $< a^4 >=< a^2 >$. De igual modo, concluímos que $< a^6 >=< a^8 >=< a^2 >$.

Finalmente, se $\mathrm{m.d.c.}(r, 10) = 1$ (ou seja, se $r \in \{3, 7, 9\}$, temos que $o(r) = 10$ e, por isso, $< a^r >= G$.

exercício 43. Seja $G = \langle a \rangle$ um grupo cíclico de ordem ímpar tal que $a^{47} = a^{17}$, $a^{10} \neq 1_G$ e $a^6 \neq 1_G$. Determine, justificando:

(a) a ordem de G;

(b) o número de subgrupos de G;

(c) todos os geradores distintos de G;

(d) o número de automorfismos de G.

(a) De $a^{47} = a^{17}$ temos que $a^{30} = 1_G$, pelo que $o(a) \mid 30$, ou seja, $o(a) \in \{1, 2, 3, 5, 6, 10, 15, 30\}$.

Como $|G|$ é ímpar e $|G| = o(a)$, temos que $o(a) \in \{1, 3, 5, 15\}$.

- se $o(a) = 1$,$a = 1_G$ e, neste caso, $a^{10} = 1_G$ (contradição)
- se $o(a) = 3$, $a^3 = 1_G$ e, neste caso, $a^6 = 1_G$ (contradição)
- se $o(a) = 5$, $a^5 = 1_G$ e, neste caso, $a^{10} = 1_G$ (contradição)

Logo, $o(a) = 15$ e, portanto, $|G| = 15$.

(b) Um subgrupo cíclico G de ordem finita n tem um e um só subgrupo de ordem k, para cada k divisor de n. Assim, como 15 tem 4 divisores (1,3, 5 e 15), concluímos que G tem 4 subgrupos.

Observação. Não é pedido, mas os 4 subgrupos são $\{1_G\}$, $< a^5 >$, $< a^3 >$ e $< a >$, de ordens 1, 3, 5 e 15, respetivamente.

(c) Sabemos que $G =< a >$ e que $o(a) = 15$. Então, $G =< a^r >$ se e só se $o(a^r) = 15$. Como $o(a^r) = \frac{15}{\mathrm{m.d.c.}(r,15)}$, concluímos que $G =< a^r >$ se e só se $\mathrm{m.d.c.}(r, 15) = 1$. Logo, os geradores de G são: a, a^2, a^4, a^7, a^8, a^{11}, a^{13} e a^{14}.

Observação. O número de geradores distintos de um grupo cíclico de ordem n é igual à imagem de n pela função *phi* de Euler, que nos dá o número de números naturais menores do que n e primos com n (recordar que se $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ é a fatorização em primos de n, então $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$).

Neste caso, como $15 = 3 \times 5$, $\varphi(15) = 15 \times \frac{2}{3} \times \frac{4}{5} = 2 \times 4 = 8$.

(d) Sabemos que, se G e H são grupos cíclicos, para $f : G \to H$ ser um isomorfismo, a imagem de um gerador de G tem de ser um gerador de H.

Assim, para $f : G \to G$ ser um automorfismo (isomorfismo onde domínio e conjunto de chegada são iguais), a imagem de um gerador de G tem de ser um gerador de G. Como temos 8 geradores distintos, vamos ter 8 automorfismos distintos, definidos por:

$$f_1(a) = a, \qquad f_2(a) = a^2, \qquad f_3(a) = a^4, \qquad f_4(a) = a^7$$

$$f_1(a) = a^8, \qquad f_2(a) = a^{11}, \qquad f_3(a) = a^{13}, \qquad f_4(a) = a^{14}$$

Observação. Porque é que é suficiente definir a imagem do gerador? Porque estamos a trabalhar com morfismos e a imagem da potência é a potência da imagem. Por exemplo, de $f_3(a) = a^4$, concluímos que

$$f_3 = \begin{pmatrix} 1_G & a & a^2 & a^3 & a^4 & a^5 & a^6 & a^7 & a^8 & a^9 & a^{10} & a^{11} & a^{12} & a^{13} & a^{14} \\ 1_G & a^4 & (a^4)^2 & (a^4)^3 & (a^4)^4 & (a^4)^5 & (a^4)^6 & (a^4)^7 & (a^4)^8 & (a^4)^9 & (a^4)^{10} & (a^4)^{11} & (a^4)^{12} & (a^4)^{13} & (a^4)^{14} \end{pmatrix}$$

$$= \begin{pmatrix} 1_G & a & a^2 & a^3 & a^4 & a^5 & a^6 & a^7 & a^8 & a^9 & a^{10} & a^{11} & a^{12} & a^{13} & a^{14} \\ 1_G & a^4 & a^8 & a^{12} & a & a^5 & a^9 & a^{13} & a^2 & a^6 & a^{10} & a^{14} & a^3 & a^7 & a^{11} \end{pmatrix}$$