

ÁLGEBRA A.

RESOLUÇÃO DE EXERCÍCIOS DAS LISTAS

Lista 01:

12. Sejam $(G_1, \perp)$ e $(G_2, \square)$ dois grupos. No conjunto $G_1 \times G_2$ defina a operação

$$(g_1, g_2) \cdot (g'_1, g'_2) = (g_1 \perp g'_1, g_2 \square g'_2).$$

Mostre que $G_1 \times G_2$ com a operação acima é um grupo.

Sol.:

(a) Sejam $(x, y), (a, b), (p, q) \in G_1 \times G_2$. (fica subentendido que $x, a, p \in G_1$ e $y, b, q \in G_2$). Mostremos a associatividade para $\cdot$ em $G_1 \times G_2$.

$$\begin{aligned}(x, y) \cdot ((a, b) \cdot (p, q)) &= (x, y) \cdot (a \perp p, b \square q) = (x \perp (a \perp p), y \square (b \square q)) = \\ &= ((x \perp a) \perp p, (y \square b) \square q) = (x \perp a, y \square b) \cdot (p, q) = ((x, y) \cdot (a, b)) \cdot (p, q).\end{aligned}$$

(b) Sejam e_1 e e_2 os neutros, respectivamente, dos grupos G_1 e G_2 (claro que em cada um destes grupos o neutro é único!). Assim, é natural que (e_1, e_2) seja o neutro de $G_1 \times G_2$.

De fato, basta notar que para qualquer $(x, y) \in G_1 \times G_2$, segue que

$$(x, y) \cdot (e_1, e_2) = (x \perp e_1, y \square e_2) = (x, y).$$

(c) Dado $(x, y) \in G_1 \times G_2$. Então, $x \in G_1$ e $y \in G_2$. Como, G_1 e G_2 são grupos, segue que $\exists x^{-1} \in G_1$ e $\exists y^{-1} \in G_2$ tais que

$$x \perp x^{-1} = e_1 \quad \text{e} \quad y \square y^{-1} = e_2.$$

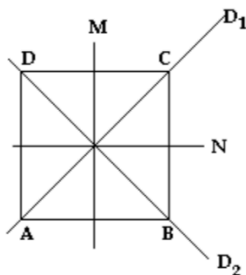
Assim, é natural que (x^{-1}, y^{-1}) seja o inverso de (x, y) em $G_1 \times G_2$. Verifique.

13. Construa o conjunto das simetrias espaciais $D_{\square}$ de um quadrado com a multiplicação sendo a composição, e verifique que é um grupo. Construa a tábua da multiplicação. Quais elementos geram o grupo?

SOL.



Considerando o esquema a seguir,



temos que o conjunto $D_{\square}$ será $D_{\square} = \{id, R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3\pi}{2}}, R_1, R_2, R_M, R_N\}$.

Pela tábua a seguir, usando a composição entre os elementos temos que, o conjunto acima é um grupo.

$\circ$	id	$R_{\frac{\pi}{2}}$	R_{π}	$R_{\frac{3\pi}{2}}$	R_1	R_2	R_M	R_N
id	id	$R_{\frac{\pi}{2}}$	R_{π}	$R_{\frac{3\pi}{2}}$	R_1	R_2	R_M	R_N
$R_{\frac{\pi}{2}}$	$R_{\frac{\pi}{2}}$	R_{π}	$R_{\frac{3\pi}{2}}$	id	R_M	R_N	R_2	R_1
R_{π}	R_{π}	$R_{\frac{3\pi}{2}}$	id	$R_{\frac{\pi}{2}}$	R_2	R_1	R_N	R_M
$R_{\frac{3\pi}{2}}$	$R_{\frac{3\pi}{2}}$	id	$R_{\frac{\pi}{2}}$	R_{π}	R_N	R_M	R_1	R_2
R_1	R_1	R_M	R_2	R_N	id	R_{π}	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$
R_2	R_2	R_N	R_1	R_M	R_{π}	id	$R_{\frac{3\pi}{2}}$	$R_{\frac{\pi}{2}}$
R_M	R_M	R_2	R_N	R_1	$R_{\frac{3\pi}{2}}$	$R_{\frac{\pi}{2}}$	id	R_{π}
R_N	R_N	R_1	R_M	R_2	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$	R_{π}	id

18. Sejam a, b, c elementos de um grupo multiplicativo G . Prove que $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$.
Obtenha $x \in G$ tal que $abxc = c$.

sol.:

~~✎~~ Basta usar a propriedade associativa, visto que G é um grupo. Assim:

$$(abc)^{-1} = ((ab)c)^{-1} = c^{-1}(ab)^{-1} = c^{-1}(b^{-1}a^{-1}) = c^{-1}b^{-1}a^{-1}.$$

vejamos agora a segunda parte do exercício. Multiplicando $abxc = c$ à esquerda por $(abc)^{-1}$, que obtivemos acima, temos

$$\begin{aligned}(abc)^{-1}(abxc) &= (abc)^{-1}c \Rightarrow (abc)^{-1}(abc)(xb) = c^{-1}b^{-1}a^{-1}c \\ &\Rightarrow xb = c^{-1}b^{-1}a^{-1}c.\end{aligned}$$

Agora, multiplicando à direita por b^{-1} , temos

$$xb b^{-1} = c^{-1}b^{-1}a^{-1}c b^{-1} \Rightarrow x = c^{-1}b^{-1}a^{-1}c b^{-1}$$

LISTA 03:

8. Seja G um grupo e $a \in G$ tal que $O(a) = m$. Mostre que se $a^t = e$, então $m|t$.

Sol.:

Seja $O(a) = m$, segue que $a^m = e$. Suponha que $a^t = e$. Queremos mostrar que $m|t$.

Por absurdo, se $m \nmid t$, então $\exists p, q \in \mathbb{Z}$, $0 < q < m$, tais que

$$t = mp + q.$$

Portanto,

$$e = a^t = a^{mp+q} = a^{mp} \cdot a^q = (a^m)^p a^q = e^p a^q = a^q,$$

ou seja, $a^q = e$, com $0 < q < m$.

Mas isto é um absurdo pois a ordem de a é m , ou seja, o menor expoente positivo ao qual se deve elevar a para se obter o neutro e é m , e no entanto obtivemos $q < m$. Portanto, $m|t$.

9. Seja $G = \langle a \rangle$ o grupo cíclico gerado por a e suponha que $O(a) = m$. Mostre que a^n gera G se, e somente se, $\text{mdc}(m, n) = 1$.

Sol.:

Suponha que $\text{mdc}(m, n) = 1$. Assim, $\exists \alpha, \beta \in \mathbb{Z}$ tais que $m\alpha + n\beta = 1$. Vamos mostrar que $\langle a^n \rangle \subset G$ e que $G \subset \langle a^n \rangle$.

Af 01. $\langle a^n \rangle \subset G$: é óbvio, por definição.

Af 02. $G \subset \langle a^n \rangle$: Seja $g \in G$. Como $G = \langle a \rangle$, segue que $\exists k \in \mathbb{Z}$ tal que $g = a^k$. Logo,

$$g = g^1 = g^{m\alpha + n\beta} = g^{m\alpha} \cdot g^{n\beta} = (g^m)^\alpha g^{\beta n} = g^{\beta n} = (a^k)^{\beta n} = (a^n)^{\beta k} \in \langle a^n \rangle.$$

Logo, vale a Af 02.

Pelas afirmações 01 e 02 segue que $G = \langle a^n \rangle$.

Reciprocamente, suponhamos que $\langle a^n \rangle = G$. Assim, dado $a \in G$, temos que $a = (a^n)^k = a^{nk}$, para algum $k \in \mathbb{Z}$. Ou seja, $a = a^{nk}$. Multiplicando esta igualdade à direita por a^{-1} , obtemos

$$aa^{-1} = a^{nk}a^{-1} \Rightarrow a^{nk-1} = e \Rightarrow o(a)|(nk-1).$$

Como $o(a) = m$, temos que $m \mid (nk - 1)$, ou seja, $\exists x \in \mathbb{Z}$ tal que $mx = nk - 1$, ou seja,

$$nk - mx = 1,$$

o que equivale dizer que

$$\text{mdc}(m, n) = 1.$$

10. Seja G um grupo multiplicativo tal que $|G| = 100$. Mostre que a equação $x^7 = 1$ tem somente uma solução $x \in G$.

sol.: Se $x^7 = 1$, então $|\langle x \rangle| \mid 7$; e como 7 é um número primo, segue que $|\langle x \rangle| = 1$ ou $|\langle x \rangle| = 7$.

Pelo T. de Lagrange, devemos ter que $|\langle x \rangle| \mid 100$; ou seja,

$$|\langle x \rangle| \mid 100;$$

mas como $\text{mdc}(7, 100) = 1$, a única possibilidade é $|\langle x \rangle| = 1$.

Disto, segue que $x = 1$.

11. Seja G um grupo abeliano e considere o subconjunto $T(G) := \{\alpha \in G : O(\alpha) < \infty\}$.
Mostre que $T(G) < G$.

Obs.: $T(G)$ é chamado de subgrupo *torção* de G .

Sol.:

Primeiramente, observe que sendo e o elemento neutro de G , temos que $O(e) = 1 < \infty$. Portanto, $e \in T(G)$, ou seja, $T(G) \neq \emptyset$. Disso segue que $T(G)$

está bem definido.

Dados $a, b \in T(G)$. Para mostrar que $T(G) < G$ precisamos mostrar que $ab^{-1} \in T(G)$.

Como $a, b \in T(G)$, segue que $\exists m, n > 0$ tais que $O(a) = m < \infty$ e $O(b) = n < \infty$ e disso

$$a^m = e \text{ e } O(b) = n.$$

Daí, observando que G é um grupo abeliano, temos

$$(ab^{-1})^{mn} = a^{mn}(b^{-1})^{mn} = (a^m)^n(b^n)^{-m} = e^n e^{-m} = e,$$

ou seja, $mn | O(ab^{-1})$, o que significa que $O(ab^{-1}) < \infty$, donde segue que $ab^{-1} \in T(G)$.

Isto prova que $T(G) < G$.

14. Determine as classes laterais de $H = \langle \bar{4} \rangle$ em $(\mathbb{Z}_8, +)$ e o conjunto quociente $\mathbb{Z}_8/H$.

Sol.:

em $\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \dots, \bar{7}\}$, temos que

$$H = \langle \bar{4} \rangle = \{\bar{0}, \bar{4}\}. \quad (\text{pois } \bar{4} + \bar{4} = \bar{0})$$

O índice de H em $\mathbb{Z}_8$ é:

$$(\mathbb{Z}_8 : H) = \frac{8}{2} = 4.$$

Disto, segue que não existem 4 classes laterais. A saber:

- $\bar{0} + H = H = \{\bar{0}, \bar{4}\}$;
- $\bar{1} + H = \{\bar{1}, \bar{5}\}$
- $\bar{2} + H = \{\bar{2}, \bar{6}\}$
- $\bar{3} + H = \{\bar{3}, \bar{7}\}$

O grupo quociente $\mathbb{Z}_8/H$ tem, portanto:

$$\mathbb{Z}_8/H = \{\bar{0} + H; \bar{1} + H; \bar{2} + H; \bar{3} + H\}.$$

