Resolução da Segunda Prova de Álgebra 1 - 2018-2

1. **Exercício 1 [3 pontos]**.

   Seja $G = \langle x \rangle = C_{25}$ um grupo cíclico de ordem 25.

   (i) Qual é a ordem do elemento x^2?
   $o(x^2) = 25/MDC(25, 2) = 25$.

   (ii) Qual é a ordem do elemento x^5?
   $o(x^5) = 25/MDC(25, 5) = 5$.

   (iii) Conte os subgrupos de G.
   Sendo G um grupo cíclico os subgrupos de G são do tipo $\langle x^d \rangle$ onde d é um divisor de 25, logo G tem três subgrupos, $\langle x^1 \rangle = G$, $\langle x^5 \rangle$ e $\langle x^{25} \rangle = \{1\}$.

2. **Exercício 2 [1 ponto]**.

   Seja $G = U(\mathbb{Z}/11\mathbb{Z})$ o grupo das classes módulo 11 que admitem inverso modular. G é um grupo cíclico?

   $G = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ tem ordem 10. As primeiras potências de 2 são 2, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$. Segue que a ordem de 2 não é 1, não é 2, não é 5. Sendo G um grupo de ordem 10, a ordem de 2 divide 10 logo $o(2) = 10$. Segue que G é um grupo de ordem 10 com um elemento de ordem 10, logo é cíclico.

3. **Exercício 3 [2 pontos]**.

   Considere o conjunto $\mathbb{R}$ dos números reais com a operação

   $$x * y := x + y + 2xy.$$

   (i) Mostre que $*$ é associativa.
   Temos que

   $$(x*y)*z = (x+y+2xy)+z+2(x+y+2xy)z = x+y+2xy+z+2xz+2yz+4xyz,$$

   $$x*(y*z) = x+(y+z+2yz)+2x(y+z+2yz) = x+y+z+2yz+2xy+2xz+4xyz$$

   são iguais.

   (ii) $\mathbb{R}$ com essa operação é um grupo?
   Vamos procurar o elemento neutro e. Temos $x * e = x$ para todo $x \in \mathbb{R}$, ou seja $x + e + 2xe = x$ para todo $x \in \mathbb{R}$, ou seja $(1 + 2x)e = 0$ para todo $x \in \mathbb{R}$. Como $1 + 2x$ não é nulo para todo $x \in \mathbb{R}$ deduzimos $e = 0$, e 0 é o elemento neutro pois $x * 0 = x$ para todo $x \in \mathbb{R}$. Se um elemento x tem inverso igual a y então $x*y = 0$ ou seja $x+y+2xy = 0$ ou seja $y = -x/(1 + 2x)$ se o denominador $1 + 2x$ não é zero, ou seja se $x \neq -1/2$. Observe que esse é o único caso de um elemento que não tem inverso, de fato $-1/2 * y = -1/2 + y + 2(-1/2)y = -1/2$ é diferente de 0 para todo $y \in \mathbb{R}$. Segue que $-1/2$ não admite inverso logo $\mathbb{R}$ com a operação $*$ não é um grupo.

Observação importante:

a operação $*$ definida acima não é DISTRIBUTIVA em relação a $+$, ou seja $a * (b + c)$ em geral não é igual a $a * b + a * c$, por exemplo

$$2 * (1 + 3) = 2 * 4 = 2 + 4 + 16 = 22$$

mas

$$2 * 1 + 2 * 3 = (2 + 1 + 4) + (2 + 3 + 12) = 24$$

(basta esse exemplo para mostrar que $*$ não é distributiva).

4. **Exercício 4 [2 pontos]**.

   Seja G um grupo comutativo e seja $H = \{x^3 \;:\; x \in G\}$.

   (i) Mostre que $H \leq G$.
   $1 \in H$ porque $1 = 1^3$, se $h \in H$ então $h = x^3$ para um $x \in G$ logo $h^{-1} = x^{-3} = (x^{-1})^3 \in H$ e se $h_1 = x^3$, $h_2 = y^3$ pertencem a H então $h_1 h_2 = x^3 y^3 = (xy)^3$ (sendo G comutativo) pertence a H logo $h_1 h_2 \in H$.

   (ii) Calcule a ordem do grupo $\{x^3 \;:\; x \in U(\mathbb{Z}/8\mathbb{Z})\}$.
   Temos $G = U(\mathbb{Z}/8\mathbb{Z}) = \{1, 3, 5, 7\}$. Seja $H = \{x^3 \;:\; x \in G\}$. Precisamos simplesmente fazer os cubos dos elementos de G. Temos $1^3 = 1$, $3^3 = 3$, $5^3 = 5$ e $7^3 = 7$ logo $H = G$ tem ordem 4.

5. **Exercício 5 [1 ponto]**.

   Sejam G um grupo de ordem 10, $x \in G$ um elemento de ordem 2 e $y \in G$ um elemento de ordem 5. Seja H um subgrupo de G tal que $x \in H$ e $y \in H$. Mostre que $H = G$.

   A ordem de um elemento de um grupo divide a ordem do grupo. $x \in H$ logo 2 divide $|H|$, $y \in H$ logo 5 divide $|H|$. Sendo 2 e 5 coprimos, segue que $2 \cdot 5 = 10$ divide $|H|$, em particular $|H| \geq 10$. Mas sendo $|G| = 10$ e $H \subseteq G$ deduzimos que $H = G$.

6. **Exercício 6 [1 ponto]**.

   Seja G um grupo de ordem ímpar e seja $y \in G$. Mostre que existe $x \in G$ tal que $x^2 = y$. [Dica: lembre-se que $y^{|G|} = 1$. Sendo $|G|$ ímpar, tem a forma $2m + 1$ com m inteiro.]

   Precisamos encontrar x tal que $x^2 = y$. Observe que x não é dado, precisamos encontrar o seu valor.

   Sabemos que $y^{2m+1} = 1$ onde $2m + 1 = |G|$, segue que $y^{2m} y = 1$ ou seja $y = y^{-2m} = (y^{-m})^2$ logo basta escolher $x = y^{-m}$.

   Podia-se também observar que $y^{2m+1} = 1$ implica (multiplicando tudo por y) que $y^{2m+2} = y$ ou seja $(y^{m+1})^2 = y$ logo basta escolher $x = y^{m+1}$. As duas resoluções são equivalentes porque sendo $y^{2m+1} = 1$ temos $y^{-m} = y^{m+1}$.