Resolução da segunda prova de Álgebra 1 do dia 23/05/2017.

1. **Exercício 1 [4 pontos]**

   Seja $G = C_{20} = \langle x \rangle$ o grupo multiplicativo cíclico de ordem 20, onde $o(x) = 20$.

   (a) (1 ponto) Calcule a ordem de x^2.
   Como $o(x) = 20$ temos $o(x^2) = 20/(20, 2) = 20/2 = 10$.

   (b) (1 ponto) Calcule a ordem de x^{18}.
   Como $o(x) = 20$ temos $o(x^{18}) = 20/(20, 18) = 20/2 = 10$.

   (c) (1 ponto) Conte os elementos de ordem 5 em G.
   Sabemos pela teoria que se d divide n o grupo C_n contem $\varphi(d)$ elementos de ordem d. Logo C_{20} contem $\varphi(5) = 4$ elementos de ordem 5. Uma outra maneira de responder era encontrar os elementos x^k tais que $o(x^k) = 5$ ou seja $20/(20, k) = 5$ ou seja $(20, k) = 4$ encontrando as soluções $k = 4$, $k = 8$, $k = 12$ e $k = 16$.

   (d) (1 ponto) Conte os subgrupos de G.
   Os subgrupos de G têm a forma $\langle x^d \rangle$ onde d divide 20, o número de subgrupos é igual ao número de divisores de 20. Como $20 = 2^2 \cdot 5$, o número de divisores de 20 é $3 \cdot 2 = 6$ (eles têm a forma $2^a 5^b$ onde $a \in \{0, 1, 2\}$ e $b \in \{0, 1\}$).

2. **Exercício 2 [2 pontos]**

   Seja $G = U(\mathbb{Z}/18\mathbb{Z})$ o grupo multiplicativo das classes módulo 18 que admitem inverso modular.

   (a) (1 ponto) Calcule a ordem do elemento $5 \in G$.
   Temos $5^2 = 25 = 7 \neq 1$, $5^3 = 5^2 \cdot 5 = 7 \cdot 5 = 35 = -1 \neq 1$, $5^4 = 5^3 \cdot 5 = -5 \neq 1$, $5^5 = 5^3 \cdot 5^2 = -25 \neq 1$ e $5^6 = (5^3)^2 = (-1)^2 = 1$. Logo $o(5) = 6$.

   (b) (1 ponto) Mostre que G é cíclico.
   Temos $G = \{1, 5, 7, 11, 13, 17\}$, logo $|G| = 6$. O elemento $5 \in G$ tem ordem 6, como visto no item acima. G é um grupo de ordem 6 que contem um elemento de ordem 6, logo G é cíclico.

3. **Exercício 3 [3 pontos]**

   Seja G um grupo multiplicativo comutativo, ou seja $xy = yx$ para todo $x, y \in G$.

(a) (1 ponto) Mostre que se A e B são subgrupos de G então

$$AB = \{ab \ : \ a \in A, \ b \in B\}$$

é um subgrupo de G.

- Elemento neutro: temos que $1 \in A$ e $1 \in B$ (sendo A e B subgrupos) logo $1 = 1 \cdot 1 \in AB$.
- Inverso: se $x \in AB$ podemos escrever $x = ab$ com $a \in A$, $b \in B$ logo $x^{-1} = (ab)^{-1} = b^{-1}a^{-1}$ e sendo G comutativo temos $b^{-1}a^{-1} = a^{-1}b^{-1} \in AB$ sendo $a^{-1} \in A$ e $b^{-1} \in B$ (pois A e B são subgrupos).
- Produto: se $x, y \in AB$ podemos escrever $x = a_1b_1$, $y = a_2b_2$ com $a_1, a_2 \in A$ e $b_1, b_2 \in B$. Precisamos mostrar que $xy \in AB$. Temos $b_1a_2 = a_2b_1$ sendo G comutativo, logo $xy = a_1b_1a_2b_2 = a_1a_2b_1b_2 \in AB$ sendo $a_1a_2 \in A$ e $b_1b_2 \in B$ (pois A e B são subgrupos).

(b) (1 ponto) Mostre que $\{x \in G \ : \ x^3 = 1\}$ é um subgrupo de G.

Seja $H := \{x \in G \ : \ x^3 = 1\}$.

- Elemento neutro: temos que $1^3 = 1$ logo $1 \in H$.
- Inverso: se $x \in H$ então $x^3 = 1$ logo $(x^{-1})^3 = x^{-3} = (x^3)^{-1} = 1^{-1} = 1$ logo $x^{-1} \in H$.
- Produto: se $x, y \in H$ então $x^3 = 1$, $y^3 = 1$. Precisamos mostrar que $xy \in H$, ou seja que $(xy)^3 = 1$. Temos $(xy)^3 = xyxyxy = xxxyyy = x^3y^3$ sendo G comutativo, daí $(xy)^3 = x^3y^3 = 1 \cdot 1 = 1$ logo $xy \in H$.

(c) (1 ponto) Calcule $|\{x \in G \ : \ x^3 = 1\}|$ quando $G = C_n$ é um grupo cíclico de ordem n.

Seja $H = \{x \in C_n \ : \ x^3 = 1\}$. Queremos calcular $|H|$. A igualdade $x^3 = 1$ significa que a ordem de x é 1 ou 3. Se 3 não divide n então nenhum elemento de C_n tem ordem 3 (pois a ordem de um elemento divide a ordem do grupo) logo $x \in H$ se e somente se $o(x) = 1$ ou seja $x = 1$, logo $H = \{1\}$ neste caso, e $|H| = 1$. Se 3 divide n então C_n contem $\varphi(3) = 2$ elementos de ordem 3, e um único elemento de ordem 1 (a identidade) logo $|H| = \varphi(1) + \varphi(3) = 1 + 2 = 3$. H é o único subgrupo de C_n de ordem 3 neste caso.

4. **Exercício 4 [1 ponto]**

Seja G um grupo finito e seja $g \in G$. Seja $H = G - \{g\}$ o conjunto dos elementos de G diferentes de g.

Mostre que se H é um subgrupo de G então $|G| = 2$.

Suponha por hipótese H subgrupo de G. Temos $|H| = |G - \{g\}| = |G| - 1$. Pelo teorema de Lagrange $|H|$ divide $|G|$, ou seja $|G| - 1$ divide $|G|$. A única possibilidade para que isso aconteça é que $|G| - 1 = 1$ logo $|G| = 2$.

Mais detalhadamente, escrevendo $n = |G|$ obtemos que $|H| = n - 1$ divide $|G| = n$, ou seja existe um inteiro positivo d tal que (*) $d(n-1) = n$ daí $d \leq n$ (pois d divide n) e a igualdade (*) pode ser escrita $n(d-1) = d$ assim n divide d, logo $n \leq d$ também e obtemos $n = d$. Substituindo em (*) obtemos $n(n-1) = n$ daí $n^2 = 2n$ e dividindo por n obtemos $n = 2$.