Primeira prova de Álgebra 2 – Semestre 2021-1 – 02/09/2021.

Aqui a, b, c são inteiros não negativos e $p \geq 11$ é um número primo que dependem do número de matrícula do/a aluno/a.

1. (1.5 ponto) Sejam $r := a + b + c + 12$, $s := r + 10$. Encontre $x, y \in \mathbb{Z}$ tais que
$$rx + sy = \mathrm{MDC}(r, s).$$

   Seguem exemplos com $r = 33$, $s = 43$, $\mathrm{MDC}(r, s) = 1$ e com $r = 34$, $s = 44$, $\mathrm{MDC}(r, s) = 2$. Aplicando o algoritmo de Euclides temos

43	33	
1	0	43
0	1	33
1	-1	10
-3	4	3
10	-13	1

44	34	
1	0	44
0	1	34
1	-1	10
-3	4	4
7	-9	2

   Segue que $10 \cdot 43 + (-13) \cdot 33 = 1$ e $7 \cdot 44 + (-9) \cdot 34 = 2$.

2. (1 ponto) Conte os ideais do anel $\mathbb{Z}/m\mathbb{Z}$ onde $m = 4p$.

   Os ideais de $A = \mathbb{Z}/m\mathbb{Z}$ são do tipo $(d)/I$ onde $I = m\mathbb{Z}$ e d é um divisor positivo de m. Como p é primo, os divisores positivos de $m = 4p$ são 1, 2, 4, p, $2p$ e $4p$, logo A admite exatamente 6 ideais.

3. (1 ponto) Seja $I = (X^3 - p) \trianglelefteq \mathbb{Q}[X]$ o ideal principal de $\mathbb{Q}[X]$ gerado por $X^3 - p$. Encontre o inverso de $\overline{X} = X + I$ no anel $\mathbb{Q}[X]/I$.

   A divisão com resto entre $X^3 - p$ e X é $X^3 - p = X \cdot X^2 - p$, que implica que $(X/p + I)(X^2 + I) = X^3/p = (X^3 - p)/p + 1 + I = 1 + I$, ou seja o inverso de $X + I$ é $X^2/p + I$.

4. (2.5 pontos) Sejam $L := S_3$, $N := A_3 \trianglelefteq L$. Seja $\mathrm{sgn} : S_3 \to \{1, -1\}$ o homomorfismo "sinal", cujo núcleo é N. Considere
$$G := \{(x, y) \in L \times L \ : \ \mathrm{sgn}(x) = \mathrm{sgn}(y)\}.$$

   É um subgrupo do produto direto $L \times L$ (não precisa mostrar isso).

   (a) (1 ponto) Mostre que $T = N \times \{1\}$ é um subgrupo normal de G.

   (b) (1.5 ponto) Mostre que $G/T \cong S_3$ e deduza o valor de $|G|$.

   Item 1. Primeiramente observe que T está contido em G sendo $\mathrm{sgn}(x) = \mathrm{sgn}(1) = 1$ para todo $(x, 1) \in T$. Obviamente $(1, 1) \in T$ sendo $1 \in N$. Se $(x, 1), (y, 1) \in T$ então $(x, 1)(y, 1) = (xy, 1) \in T$ pois $N \leq L$, e o inverso de $(x, 1) \in T$ é $(x^{-1}, 1)$, que pertence a T pois $N \leq L$. Se $(a, b) \in G$ e $(x, 1) \in T$ então $(a, b)(x, 1)(a, b)^{-1} = (axa^{-1}, b1b^{-1}) = (axa^{-1}, 1) \in T$ pois N é normal em G. Isso mostra que $T \trianglelefteq G$.

Item 2. Considere $f : G \to L$, $f(x,y) := y$. Se trata de um homomorfismo de grupos pois $f((x_1,y_1)(x_2,y_2)) = f(x_1x_2, y_1y_2) = y_1y_2 = f(x_1,y_1)f(x_2,y_2)$. É sobrejetivo pois $f(x,x) = x$ para todo $x \in L$ (**observe que** $(x,x) \in G$). O núcleo de f é dado pelos elementos $(x,y) \in G$ tais que $y = 1$, e como $\mathrm{sgn}(x) = \mathrm{sgn}(y)$ obtemos $\ker(f) = N \times \{1\} = T$. Pelo teorema de isomorfismo $G/T \cong L$. Segue que $|G/T| = |L|$, ou seja $|G|/|T| = |L|$. Sendo $|T| = |N| = 3$ e $|L| = 6$, obtemos que $|G| = 3 \cdot 6 = 18$.

5. (2 pontos) Seja $\mathscr{T}$ o conjunto dos grupos finitos X tais que $q \leq p$ para todo divisor primo q da ordem de X (onde p é o número primo definido acima). Em outras palavras $X \in \mathscr{T}$ se e somente se nenhum divisor primo de $|X|$ é maior do que p.
   (a) (1 ponto) Diga se o grupo simétrico S_{p+3} pertence a $\mathscr{T}$.
   (b) (1 ponto) Sejam G um grupo finito, $N_1, N_2 \trianglelefteq G$ e seja $N := N_1 \cap N_2$. Mostre que se $G/N_1 \in \mathscr{T}$ e $G/N_2 \in \mathscr{T}$ então $G/N \in \mathscr{T}$. [Dica: considere o homomorfismo de grupos $G \to G/N_1 \times G/N_2$ definido por $g \mapsto (gN_1, gN_2)$.]

   Por exemplo se $p = 23$ então o grupo simétrico $S_{p+3} = S_{26}$ pertence a $\mathscr{T}$ pois os divisores primos de $|S_{26}| = 26!$ são no máximo 23, sendo $26! = 26 \cdot 25 \cdot 24 \cdot 23!$ e $26 = 2 \cdot 13$, $25 = 5^2$ e $24 = 2^3 \cdot 3$.

   Por exemplo se $p = 29$ então $S_{p+3} = S_{32}$ não pertence a $\mathscr{T}$ pois 31 é um primo maior que p e divide $|S_{32}| = 32!$.

   Considere o homomorfismo de grupos $G \to G/N_1 \times G/N_2$ definido por $g \mapsto (gN_1, gN_2)$. O seu núcleo é $N_1 \cap N_2$, logo segue do teorema de isomorfismo que $G/N_1 \cap N_2$ é isomorfo a um **subgrupo** de $G/N_1 \times G/N_2$ (*atenção: esse homomorfismo não é sobrejetivo em geral!*), em particular $|G/N_1 \cap N_2|$ divide $|G/N_1 \times G/N_2| = |G/N_1||G/N_2|$, pelo teorema de Lagrange. Como $G/N_1, G/N_2 \in \mathscr{T}$, segue que $G/N_1 \cap N_2 \in \mathscr{T}$.

6. (1.5 ponto) Seja $A = \mathbb{Q} \times \mathbb{Q}$ com as operações seguintes.

$$(a_1, b_1) + (a_2, b_2) := (a_1 + a_2, b_1 + b_2),$$

$$(a_1, b_1) \cdot (a_2, b_2) := (a_1a_2 + pb_1b_2, a_1b_2 + b_1a_2).$$

   Sabendo que A com essas operações é um anel comutativo unitário, encontre os elementos neutros de A e mostre que A é um corpo.

   Os elementos neutros são $(0,0)$ e $(1,0)$. Considere $(a_1, b_1) \neq (0,0)$. Queremos encontrar $(a_2, b_2) \in A$ tal que $(a_1, b_1) \cdot (a_2, b_2) = (1, 0)$. Isso significa que $a_1a_2 + pb_1b_2 = 1$ e $a_1b_2 + b_1a_2 = 0$. Se $a_1 \neq 0$ então $b_2 = -b_1a_2/a_1$, logo $a_1a_2 - pb_1^2a_2/a_1 = 1$, segue $a_2(a_1 - pb_1^2/a_1) = 1$ e isso determina a_2 se $a_1^2 \neq pb_1^2$. Mas é claro que $a_1^2 \neq pb_1^2$ pois se fosse $a_1^2 = pb_1^2$ então teriamos $p = (a_1/b_1)^2$, contradizendo o fato que $a_1, b_1 \in \mathbb{Q}$, pois p é um número primo, logo não é o quadrado de um número racional. Se $a_1 = 0$ então $b_1 \neq 0$ e $b_1a_2 = 0$, logo $a_2 = 0$ e $pb_1b_2 = 0$, segue que $b_2 = 1/(pb_1)$ e o inverso é determinado.