Resolução da terceira prova - Álgebra 1 turma B - 2017-2

1. (2 pontos) Mostre por indução que
$$\sum_{i=1}^{n} i \cdot 2^i = (n-1) \cdot 2^{n+1} + 2$$
para todo $n \geq 1$.

   A base da indução é $n = 1$ e vale porque $\sum_{i=1}^{1} i \cdot 2^i = 2$ e $(1-1) \cdot 2^{1+1} + 2 = 2$ são iguais. Agora suponha por hipótese $\sum_{i=1}^{n} i \cdot 2^i = (n-1) \cdot 2^{n+1} + 2$. Mostraremos que $\sum_{i=1}^{n+1} i \cdot 2^i = (n+1-1) \cdot 2^{n+1+1} + 2$. Temos
$$\begin{aligned}\sum_{i=1}^{n+1} i \cdot 2^i &= \sum_{i=1}^{n} i \cdot 2^i + (n+1)2^{n+1} = (n-1)2^{n+1} + 2 + (n+1)2^{n+1} \\ &= 2n \cdot 2^{n+1} + 2 = n \cdot 2^{n+2} + 2.\end{aligned}$$

2. (2 pontos) Conte os ideais de $\mathbb{Z}/5\mathbb{Z}[X]$ contendo $(X^3 - 2)$.

   A fatoração de $X^3 - 2$ em $\mathbb{Z}/5\mathbb{Z}[X]$ é $(X-3)(X^2+3X+4)$ (é obtida observando que 3 é raiz de $X^3 - 2$ e fazendo a divisão com resto entre $X^3 - 2$ e $X - 3$). O segundo fator $X^2 + 3X + 4$ é irredutível (tem grau 2 e não tem raizes em $\mathbb{Z}/5\mathbb{Z}$). Os ideais contendo $(X^3 - 2)$ correspondem aos divisores de $X^3 - 2$, logo são $(X^3 - 2)$, $(1) = \mathbb{Z}/5\mathbb{Z}[X]$, $(X - 3)$ e $(X^2 + 3X + 4)$ (esses últimos dois são ideais maximais).

3. (1 ponto) Faça a divisão com resto entre $X^3 - 2X^2 + X - 2$ e $X^2 - 4$ em $\mathbb{Q}[X]$.
$$\begin{array}{c|c} X^3 - 2X^2 + X - 2 & X^2 - 4 \\ X^3 - 4X & X - 2 \\ \hline -2X^2 + 5X - 2 & \\ -2X^2 + 8 & \\ \hline 5X - 10 & \end{array}$$
   O quociente é $X - 2$, o resto é $5X - 10$.

4. (1 ponto) Calcule a fatoração de $X^3 - X - 6$ em $\mathbb{Q}[X]$.

   Seja $P(X) = X^3 - X - 6$. As raizes inteiras dividem 6, logo as candidatas raizes inteiras são $1, -1, 2, -2, 3, -3, 6, -6$. Temos $P(2) = 0$ logo $X - 2$ divide $P(X)$, uma divisão com resto dá $P(X) = (X-2)(X^2+2X+3)$. O segundo fator é irredutível porque tem grau 2 e não tem raizes racionais (isso segue da formula de Bhaskara).

5. (4 pontos) Seja $\mathbb{Q}$ o corpo dos números racionais.

Considere $A = \mathbb{Q} \times \mathbb{Q}$ com as operações

$$(x, y) + (z, w) = (x + z, y + w), \qquad (x, y) \cdot (z, w) = (xz, xw + yz).$$

Temos que A é um anel comutativo unitário com tais operações (não precisa mostrar isso). Os elementos neutros da soma e do produto são $(0, 0)$ e $(1, 0)$. Sejam

$$I_1 = \{(x, y) \in A \ : \ x = 0\}, \qquad I_2 = \{(x, y) \in A \ : \ y = 0\}.$$

(a) Mostre que $(x, y) \in A$ admite inverso multiplicativo se e somente se $x \neq 0$ e calcule o inverso de (x, y) neste caso.

Se $(x, y)(z, w) = (1, 0)$ então temos $(xz, xw + yz) = (1, 0)$ ou seja $xz = 1$ e $xw + yz = 0$, a relação $xz = 1$ implica $x \neq 0$ e $z = 1/x$ e substituindo na segunda $w = -yz/x = -y/x^2$. Logo o inverso de (x, y) é $(1/x, -y/x^2)$.

(b) Mostre que I_1 é ideal de A.

Temos $(0, 0) \in I_1$ (basta escolher $y = 0$), se $(0, y)$ e $(0, w)$ pertencem a I_1 então $(0, y) + (0, w) = (0, y + w) \in I_1$ e se $(0, y) \in I_1$ então $-(0, y) = (0, -y) \in I_1$. Isso mostra que I_1 é um subgrupo aditivo de A. Para mostrar que é ideal basta mostrar o segundo axioma da definição de ideal, ou seja que se $(0, y) \in I_1$ e $(z, w) \in A$ então $(0, y)(z, w) \in I_1$. Mas $(0, y)(z, w) = (0, yz) \in I_1$.

(c) Mostre que I_2 não é ideal de A.

Por exemplo $(1, 0) \in I_2$ mas $(1, 0)(0, 1) = (0, 1) \notin I_2$. Logo o segundo axioma da definição de ideal não vale para I_2.

(d) Mostre que os únicos ideais de A são $\{(0, 0)\}$, I_1 e A. [Dica: o que acontece se um ideal I de A contem um elemento inversível?]

Seja I um ideal de A. Se I contem um elemento $u \in A$ que é inversível em A então por definição de ideal I contem $u \cdot u^{-1} = 1$ logo $I = A$ (se $a \in A$ então $a = 1 \cdot a \in I$). Agora suponha que I não contem elementos inversíveis (equivalentemente $I \neq A$). Pelo item (a) temos que se $(x, y) \in I$ então $x = 0$, em outras palavras $I \subseteq I_1$. Se todos os elementos de I são nulos então $I = \{(0, 0)\}$, agora suponha que exista um elemento $(0, y) \in I$ com $y \neq 0$. Temos então $(0, 1) = (0, y)(0, 1/y) \in I$, logo se z é um elemento qualquer de $\mathbb{Q}$ então $(0, z) = (0, 1)(0, z) \in I$. Isso implica que $I_1 \subseteq I$ logo $I = I_1$.