Resolução da terceira prova de álgebra 1 (2018-2).

1. **Exercício 1 [2 pontos].**

   Faça a divisão com resto entre X^3+X^2+1 e $X+2$ em $\mathbb{Q}[X]$.

$$\begin{array}{c|c}
X^3+X^2+1 & X+2 \\
X^3+2X^2 & X^2-X+2 \\
\hline
-X^2+1 & \\
-X^2-2X & \\
\hline
2X+1 & \\
2X+4 & \\
\hline
-3 &
\end{array}$$

2. **Exercício 2 [1 ponto].**

   Faça a divisão com resto entre X^3+1 e $2X+1$ em $\mathbb{Z}/5\mathbb{Z}[X]$.

$$\begin{array}{c|c}
X^3+1 & 2X+1 \\
X^3+3X^2 & 3X^2+X+2 \\
\hline
2X^2+1 & \\
2X^2+X & \\
\hline
4X+1 & \\
4X+2 & \\
\hline
4 &
\end{array}$$

3. **Exercício 3 [1 ponto].**

   Escreva a lista dos polinômios de grau 3 em $\mathbb{Z}/2\mathbb{Z}[X]$.

   Eles têm a forma aX^3+bX^2+cX+d com $a,b,c,d \in \mathbb{Z}/2\mathbb{Z}$ e $a \neq 0$, logo temos uma escolha para a e duas escolhas para b,c,d, em total $1\cdot 2\cdot 2\cdot 2 = 8$ polinômios. Eles são:

   - X^3
   - X^3+1
   - X^3+X
   - X^3+X^2
   - X^3+X+1
   - X^3+X^2+1
   - X^3+X^2+X
   - X^3+X^2+X+1

4. **Exercício 4 [1 ponto].**

   Resolva a equação $x^2 \equiv 2x \mod 8$.

   A equação pode ser escrita $x^2-2x \equiv 0 \mod 8$. Para resolvê-la é só substituir todas as classes módulo 8 na expressão $f(x)=x^2-2x$ para ver quais verificam a equação. Temos $f(0)=0$, $f(1)=7$, $f(2)=0$, $f(3)=3$, $f(4)=0$, $f(5)=7$, $f(6)=0$, $f(7)=3$. Logo as soluções são 0, 2, 4, 6.

5. **Exercício 5 [5 pontos]**. Considere o conjunto $A = \mathbb{Z}$ dos números inteiros com as operações

$$\textit{Soma} \qquad a \oplus b := a + b - 3,$$

$$\textit{Produto} \qquad a \star b := 3a + 3b - ab - 6.$$

(a) Mostre que $a \star (b \oplus c) = (a \star b) \oplus (a \star c)$ para todo $a, b, c \in A$ (ou seja a propriedade distributiva).

Temos

$$\begin{aligned} a \star (b \oplus c) &= a \star (b + c - 3) \\ &= 3a + 3(b + c - 3) - a(b + c - 3) - 6 \\ &= (3a + 3b - ab - 6) + (3a + 3c - ac - 6) - 3 \\ &= (a \star b) \oplus (a \star c). \end{aligned}$$

(b) Mostre que $\oplus$ e $\star$ são associativas.

Temos que

$$\begin{aligned} a \oplus (b \oplus c) &= a + (b + c - 3) - 3 \\ &= a + b - 3 + c - 3 = (a \oplus b) \oplus c, \end{aligned}$$

$$\begin{aligned} a \star (b \star c) &= a \star (3b + 3c - bc - 6) \\ &= 3a + 3(3b + 3c - bc - 6) - a(3b + 3c - bc - 6) - 6 \\ &= 3(3a + 3b - ab - 6) + 3c - (3a + 3b - ab - 6)c - 6 \\ &= (a \star b) \star c. \end{aligned}$$

(c) Encontre $d, e \in A$ tais que $a \oplus d = a$, $a \star e = a$ para todo $a \in A$ (ou seja os elementos neutros de $\oplus$ e $\star$).

A condição $a \oplus d = a$ significa $a + d - 3 = a$ ou seja $d = 3$, segue que 3 é o elemento neutro de $\oplus$ (de fato $a \oplus 3 = a + 3 - 3 = a$ para todo $a \in A$). A condição $a \star e = a$ para todo $a \in A$ significa $3a + 3e - ae - 6 = a$ para todo $a \in A$, em particular vale para $a = 0$ logo $e = 2$ é o elemento neutro de $\star$ (de fato $a \star 2 = 3a + 6 - 2a - 6 = a$ para todo $a \in A$).

(d) A é um corpo?

Não, por exemplo 1 é diferente de 3 (o elemento neutro da soma) mas 1 não tem inverso multiplicativo porque $1 \star b = 2$ significa $3 + 3b - b - 6 = 2$ ou seja $2b = 5$ contradição (b é inteiro).

Atenção: alguém argumentou que A não é corpo mostrando que 3 não possui inverso multiplicativo. Mas 3 é o elemento neutro da soma (ou seja é o "zero" de A). Para mostrar que A não é corpo precisa encontrar $a \neq 3$ que não possua inverso multiplicativo.

(e) $I = \{2x - 3 \ : \ x \in A\}$ é um ideal de A?

Sendo $2x - 3 = x \star 1$, temos $I = \{x \star 1 \ : \ x \in A\}$ logo I é o ideal principal gerado por 1, ou seja $I = (1)$.

Podia-se também verificar todos os axiomas de ideal. Escolhendo $x = 2$ obtemos que $3 \in I$ (o elemento neutro da soma). O inverso aditivo de $a \in A$ é $6 - a$, de fato $a \oplus (6-a) = a + (6-a) - 3 = 3$ logo o inverso aditivo de $2x - 3$ é $6 - (2x - 3) = 2(6 - x) - 3 \in I$. Se $2x - 3, 2y - 3 \in I$ então $(2x-3) \oplus (2y-3) = 2x - 3 + 2y - 3 - 3 = 2(x + y - 3) - 3 \in I$. Se $2x - 3 \in I$ e $a \in A$ então $a \star (2x - 3) = 3a + 3(2x-3) - a(2x-3) - 6 = 2(3a + 3x - ax - 6) - 3 \in I$.

Para quem sabe o que significa, o anel A do exercício 5 é isomorfo ao anel $\mathbb{Z}$ (com as operações usuais), um isomorfismo é $f : \mathbb{Z} \to A$, $f(x) = 3 - x$.