
Soluções

1. (a) f não é um homomorfismo pois, por exemplo, $f(1+1) = 2^2 = 4$ enquanto $f(1) + f(1) = 1^2 + 1^2 = 1 + 1 = 2$. Por outro lado, g é um homomorfismo pois, para quaisquer $a, b \in \mathbb{Z}_3$, tem-se
$$g(ab) = (ab)^3 = a^3b^3 = g(a)g(b)$$
(uma vez que $\mathbb{Z}_3$ é comutativo) e
$$g(a+b) = (a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 = a^3 + b^3 = g(a) + g(b)$$
(uma vez que $\mathbb{Z}_3$ tem característica 3).

   (b) (i)
   - $6x + 6$ é de grau 1 logo é irredutível em $\mathbb{R}[x]$ (pois $\mathbb{R}$ é um corpo).
   - $x^2 + 4$ tem grau 2 e não tem raízes reais, logo é irredutível em $\mathbb{R}[x]$.
   - $x^3 + 1$ tem grau 3 logo é redutível em $\mathbb{R}[x]$ (tem-se $x^3 + 1 = (x+1)(x^2 - x + 1)$ em $\mathbb{R}[x]$.

   (ii)
   - $2x^2 + 2 = 2(x^2 + 1)$ em $\mathbb{Z}[x]$ e nem 2 nem $x^2 + 1$ são unidades de $\mathbb{Z}[x]$, pelo que $2x^2 + 2$ é redutível em $\mathbb{Z}[x]$.
   - $x^3 + 3x^2 + 6x + 3$ é irredutível em $\mathbb{Q}[x]$ pelo critério de Eisenstein e como é mónico então é irredutível em $\mathbb{Z}[x]$.
   - $x^2 - 1 = (x-1)(x+1)$ e nem $x - 1$ nem $x + 1$ são unidades de $\mathbb{Z}[x]$, logo $x^2 - 1$ é redutível em $\mathbb{Z}[x]$.

   (c) Seja $p(x) = x^4 - 3x^3 + 2x^2 + 2x - 4$. Se $p(1+i) = 0$ então $p(1-i) = 0$ (pois em geral, se $a + bi$ é raiz de $p(x)$ também $a - bi$ é raiz de $p(x)$). Portanto, $(x - (1+i))(x - (1-i)) = x^2 - 2x + 2$ divide $p(x)$ em $\mathbb{Q}[x]$. De facto,
$$x^4 - 3x^3 + 2x^2 + 2x - 4 = (x^2 - 2x + 2)(x^2 - x - 2).$$
Vejamos agora se $x^2 - x - 2$ tem raízes em $\mathbb{Q}$:
$$x^2 - x - 2 = 0 \Leftrightarrow x = \frac{1 \pm \sqrt{1+8}}{2} = \frac{1 \pm 3}{2} \Leftrightarrow x = 2 \vee x = -1.$$
Em conclusão, $p(x) = (x^2 - 2x + 2)(x - 2)(x + 1)$ é a decomposição de $p(x)$ em factores irredutíveis em $\mathbb{Q}[x]$ ($x^2 - 2x + 2$ é irredutível em $\mathbb{Q}[x]$ porque tem grau 2 e não tem raízes racionais).

2. (a) Como
$$x^5 - 7x^3 + 2x^2 - 14 = (x^3 - x^2 - 7x + 7)(x^2 + x + 1) + 3x^2 - 21$$
e
$$x^3 - x^2 - 7x + 7 = (3x^2 - 21)\Big(\frac{1}{3}x - \frac{1}{3}\Big) + 0$$
então, pelo Algoritmo de Euclides
$$\mathrm{mdc}(x^5 - 7x^3 + 2x^2 - 14, x^3 - x^2 - 7x + 7)$$
é o polinómio mónico associado de $3x^2 - 21$, isto é, $x^2 - 7$.

(b)
$$x^4 - 1 = (x^2)^2 - 1^2 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1)$$
dá-nos a factorização de $x^4 - 1$ em polinómios irredutíveis de $\mathbb{R}[x]$. Portanto, os divisores de $x^4 - 1$ são os polinómios
$$1,\ (x-1),\ (x+1),\ (x^2+1),\ (x-1)(x+1) = x^2 - 1,\ (x-1)(x^2+1) = x^3 - x^2 + x - 1,$$
$$(x+1)(x^2+1) = x^3 + x^2 + x + 1,\ x^4 - 1$$
e os respectivos polinómios associados.

(c) Pelo Teorema do Resto (válido em qualquer anel comutativo com identidade), $x - 1$ divide $x^3 + x^2 + x + 2$ em $\mathbb{Z}_n[x]$ precisamente quando 1 é raiz de $x^3 + x^2 + x + 2$ em $\mathbb{Z}_n[x]$, ou seja, quando
$$1^3 + 1^2 + 1 + 2 = 5 \equiv_n 0,$$
isto é, $n \mid 5$. Portanto, como $n \geq 2$, $x - 1$ divide $x^3 + x^2 + x + 2$ em $\mathbb{Z}_n[x]$ se e só se $n = 5$.

3. (a) Do Exercício 2(a) decorre imediatamente que $I = \langle x^2 - 7 \rangle$.

(b) O ideal $I = \langle x^2 - 7 \rangle$ é maximal se e só se $x^2 - 7$ é irredutível em $\mathbb{Q}[x]$, o que é verdade pelo critério de Eisenstein.

(c) Sim, pois I sendo maximal, então $\mathbb{Q}[x]/I$ é um corpo. Determinemos o inverso de $x + I$ em $\mathbb{Q}[x]/I$. Como
$$\mathbb{Q}[x]/I = \{p(x) + I \mid p(x) \in \mathbb{Q}[x]\} = \{r(x) + I \mid r(x) \in \mathbb{Q}[x], \mathrm{gr}(r(x)) \leq 1\},$$
bastará determinar $a + bx + I \in \mathbb{Q}[x]/I$ tal que $(x + I)(a + bx + I) = 1 + I$. Para isso teremos que determinar $a + bx \in \mathbb{Q}[x]$ tal que $ax + bx^2 - 1 \in I = \langle x^2 - 7 \rangle$.
Basta tomar $a = 0$ e $b = \frac{1}{7}$ pois $\frac{1}{7}x^2 - 1 = \frac{1}{7}(x^2 - 7)$. Portanto,
$$(x + I)^{-1} = \frac{1}{7}x + I.$$
