DMat-FCTUC **1ª Frequência de Corpos e Equações Algébricas**

Duração: 1h30m 25/03/2019

Soluções

1. (a) Uma vez que os irredutíveis em $\mathbb{R}[x]$ são os polinómios de grau 1 e os de grau 2 com discriminante $\Delta = b^2 - 4ac < 0$, então $6x + 6$ e $x^2 + 4$ são irredutíveis enquanto $x^3 + 1$ é redutível.

   (b) Os dois primeiros são irredutíveis (pelo critério de Eisenstein, $p = 3$ e $p = 2$, respectivamente), enquanto $x^3 + 1 = (x + 1)(x^2 - x + 1)$ é redutível.

   (c) São ambos redutíveis: $2x^2 + 2 = 2(x^2 + 1)$ (e 2 não é uma unidade de $\mathbb{Z}[x]$) enquanto $x^2 - 1 = (x - 1)(x + 1)$.

2. (a) Se $1 + i$ é raiz de $p(x)$, então o seu conjugado $1 - i$ também o é, logo $p(x)$ é divisível por $(x - (1 + i))(x - (1 - i)) = x^2 - 2x + 2$. Efectuando a divisão de $p(x)$ por $x^2 - 2x + 2$ obtemos $p(x) = (x^2 - 2x + 2)(x^3 - 4x^2 + 5x - 2)$. O primeiro factor já é irredutível em $\mathbb{Q}[x]$ uma vez que é de grau 2 e, como vimos, não tem raízes racionais. E o segundo? As possíveis raízes racionais são ± 1 e ± 2. Verificando, concluímos que 1 e 2 são de facto raízes, 1 é mesmo raiz dupla: $x^3 - 4x^2 + 5x - 2 = (x - 1)^2(x - 2)$. Portanto, a factorização única de $p(x)$ em irredutíveis será

   $$(x^2 - 2x + 2)(x - 1)^2(x - 2).$$

   Alternativa: As possíveis raízes racionais de $p(x)$ são ± 1, ± 2 e ± 4. Como 1 e 2 são de facto raízes, $p(x) = q(x)(x - 1)(x - 2)$. Dividindo, obtemos $q(x) = x^3 - 3x^2 + 4x - 2$. Mas $q(x)$ ainda é redutível pois 1 também é raiz de $q(x)$. Temos

   $$p(x) = q(x)(x - 1)(x - 2) = (x^2 - 2x + 2)(x - 1)^2(x - 2).$$

   Como $x^2 - 2x + 2$ é irredutível pois as suas duas raízes são imaginárias ($1 + i$ e $1 - i$), está terminada a factorização.

   (b) Da alínea anterior segue imediatamente que a lista (12 ao todo)

   $$\begin{array}{l} 1 \\ x - 1,\ x - 2,\ x^2 - 2x + 2 \\ (x - 1)^2,\ (x - 1)(x - 2),\ (x - 1)(x^2 - 2x + 2),\ (x - 2)(x^2 - 2x + 2) \\ (x - 1)^2(x - 2),\ (x - 1)^2(x^2 - 2x + 2),\ (x - 1)(x - 2)(x^2 - 2x + 2) \\ p(x) \end{array}$$

   representa todos os divisores de $p(x)$ (isto é, todos os outros divisores são associados de um destes).

3. (a) Como

$$\begin{aligned} A/I &= \{p(x) + I \mid p(x) \in \mathbb{Z}_2[x]\} \\ &= \{r(x) + I \mid r(x) \in \mathbb{Z}_2[x], \mathrm{gr}(r(x)) \leq 2\} \\ &= \{ax^2 + bx + c + I \mid a, b, c \in \mathbb{Z}_2\} \qquad (*) \end{aligned}$$

(onde em $(*)$ já não temos classes repetidas), A/I tem 8 elementos:

$$0,\ 1,\ x,\ x+1,\ x^2+x+1,\ x^2+1,\ x^2,\ x^2+1.$$

(b) A/I é um corpo sse I é um ideal maximal. Por um teorema estudado nas aulas sabemos que um ideal principal $I = \langle m(x) \rangle$ de $\mathbb{Z}_2[x]$ é maximal se e só se $m(x)$ é irredutível em $\mathbb{Z}_2[x]$. No caso presente, $m(x) = x^3 + xp1$ é claramente irredutível (pois é de grau 3 e não tem raízes em $\mathbb{Z}_2$) pelo que a resposta é afirmativa: I é maximal. Logo A/I é um corpo.

(c) Determinemos o inverso de $x^2 + x$ em A/I. Bastará determinar $ax^2 + bx + c \in \mathbb{Z}_2[x]/I$ tal que $(x^2+x)(ax^2+bx+c) = 1$. Para isso teremos que determinar $a, b, c \in \mathbb{Z}_2$ tais que

$$ax^4 + (a+b)x^3 + (b+c)x^2 + cx - 1 = 0.$$

Como, em A/I, $x^3+x+1 = 0$, então $x^3 = -x-1 = x+1$. Substituindo acima, obtemos

$$(a+b+c)x^2 + (b+c)x + (a+b-1) = 0,$$

ou seja, $a+b+c = 0$, $b+c = 0$ e $a+b = 1$ (porque já vimos que as classes de polinómios de grau ≤ 2 são todas diferentes). Daqui sai imediatamente $a = 0, b = c = 1$. Portanto,

$$(x^2+x)^{-1} = x+1.$$

<u>Alternativa</u>: Uma vez que $x^3 + x = 1$ em A/I, então

$$\frac{1}{x^2+x} = \frac{x^3+x}{x^2+x}.$$

Fazendo a divisão obtemos $x^3 + x = (x^2+x)(x+1)$. Portanto,

$$\frac{1}{x^2+x} = x+1.$$

4. (a) <u>Dos Apontamentos das aulas</u>:

Seja I um ideal de $C[x]$. Se $I = \{0\}$, então $I = \langle 0 \rangle$ é um ideal principal. Podemos pois admitir que $I \neq \{0\}$. Nesse caso, seja $m(x) \neq 0$ um polinómio em I de grau o mais pequeno possível. Provemos que $I = \langle m(x) \rangle$:

Como $m(x) \in I$, é óbvio que $\langle m(x) \rangle \subseteq I$. Por outro lado, se $p(x) \in I$, usando o algoritmo de divisão temos $p(x) = q(x)m(x) + r(x)$, onde $gr(r(x)) < gr(m(x))$. Dado que I é um ideal, podemos concluir que $r(x) = p(x) - q(x)m(x) \in I$. Mas então $r(x)$ só pode ser igual a 0 pois, com excepção do polinómio nulo, não pode haver nenhum polinómio em I de grau inferior a $gr(m(x))$. Assim, $p(x)$ é um múltiplo de $m(x)$ pelo que pertence ao ideal $\langle m(x) \rangle$.

(b) Por um teorema estudado nas aulas, $\langle a(x), b(x)\rangle = \langle \text{mdc}(a(x), b(x))\rangle$. Calculemos então $m(x) = \text{mdc}(x^2 - 2x + 1, x^3 - 6x^2 + 11x - 6)$:

Como

$$x^3 - 6x^2 + 11x - 6 = (x^2 - 2x + 1)(x - 4) + (2x - 2)$$

e

$$x^2 - 2x + 1 = (2x - 2)(\frac{x}{2} - \frac{1}{2}).$$

então, pelo Algoritmo de Euclides, $\text{mdc}(a(x), b(x))$ é o polinómio mónico associado de $2x - 2 = 2(x - 1)$, isto é, $x - 1$. Portanto, $m(x) = x - 1$.

Alternativa: Basta calcular as factorizações em irredutíveis dos dois polinómios:

$$x^3 - 6x^2 + 11x - 6 = (x - 1)(x - 2)(x - 3) \text{ e } x^2 - 2x + 1 = (x - 1)^2$$

donde $\text{mdc}(x^2 - 2x + 1, x^3 - 6x^2 + 11x - 6) = (x - 1)$.
