→ Lista 12:

Ex 2: Dem:

(a) Considere $f = a_2X^2 + a_1X + a_0$, $a_2 \neq 0$

Veja que para a_2 temos uma possibilidade ($a_2 = 1$) e, para a_1 e a_0 tem k possibilidades para cada um. Assim, pelo Princ. fundamental da Contagem, existem $1 \cdot k \cdot k = k^2$ polinômios de grau 2 em $\mathbb{K}[X]$.

∎

(b): Agora, queremos saber quantos pol. irredutíveis de grau 2 em $\mathbb{K}[x]$.

Inicialmente, consideremos os polinômios mônicos. Veja que um polinômio f é redutível ou irredutível em $\mathbb{K}$. Do item (a) já sabemos que o número de polinômios mônicos de grau 2 é k^2. Vamos encontrar a quantidade de pol. mônicos redutíveis de

de grau 2. Observe que se f for redutível então

$$f = (x-a)(x-b), \quad a, b \in \mathbb{K}.$$

Para a temos k possibilidades, assim como para b. Mas, como $(x-a)(x-b) = (x-b)(x-a)$, existem $\frac{k^2}{2}$ pol. mônicos redutíveis de grau 2. Logo, existem $k^2 - \frac{k^2}{2} = \frac{k^2}{2}$ polinômios mônicos irredutíveis de grau 2.

Por fim, para encontrar o nº de polinómios irredutíveis de grau 2 em $\mathbb{K}[x]$ basta multiplicar $\frac{k^2}{2}$ por $(k-1)$, pois para cada polinómio mónico irred. de grau 2, seu associado também será irredutível. ∎

$$\underbrace{f\ (\text{mónico})}_{\text{irred}} \to \underbrace{\alpha f}_{\text{irred}},\ \alpha \in \mathbb{K}\setminus\{0\}.$$

obs: f e g são assoc. $\Leftrightarrow f = \alpha g$, $\alpha \in \mathbb{K}$

Monitoria: Lista 12

Ex 4:

item ii) As condições (1) e (2) são "tranquilas".

Vamos provar (3). Temos que

$$\langle f_1, \dots, f_n \rangle = \{\alpha_1 f_1 + \dots + \alpha_n f_n : \alpha_i \in A\}$$

Tome $f = \beta_1 f_1 + \dots + \beta_n f_n$ e $g \in A$. Então

$$fg = (\beta_1 f_1 + \dots + \beta_n f_n) \cdot g = (\beta_1 g) f_1 + \dots + (\beta_n g) f_n$$

Como $\beta_i g \in A$, $\forall i$ segue que $fg \in \langle f_1, \dots, f_n \rangle$. ∎

(iii) Dem: Queremos provar que se $\mathbb{K}$ é um corpo então todo ideal de $\mathbb{K}[x]$ é principal, isto é, queremos ver que se I é um ideal de $\mathbb{K}[x]$ então $I = \langle f \rangle = f \cdot \mathbb{K}[x]$, para algum $f \in \mathbb{K}[x]$.

Se $I = \{0\}$, não há o que fazer, pois $I = \langle 0 \rangle$.

Se $I \neq \{0\}$, então existe pelo menos um

um $\tilde{f} \in I$, $\tilde{f} \neq 0$ com o menor grau (pode-
mos tomar esse polinômio pelo PBO (explicar))

Seja $g \in I$, pelo algoritmo da divisão

$$g = f \cdot q + r, \quad 0 \leq gr(r) < gr(f) \text{ ou}$$

$r = 0$ (*)

Usando que I é um ideal, como $\tilde{f} \in I$
e $q \in \mathbb{K}[x]$, $\tilde{f} \cdot q \in I$. Assim, $g - \tilde{f} \cdot q = r \in$
I. No entanto, $gr(f) < gr(r)$, daí, por (*)
$r = 0$ e $g = \tilde{f} \cdot q \Rightarrow I = \langle \tilde{f} \rangle$. ∎

(iv) Dem:

($\Rightarrow$) Consideremos que A é um corpo. Se $I \subseteq A$ é um ideal de A e $I \neq \{0\}$, temos que existe $a \in I$ tal que $a \neq 0$.

Assim, como A é corpo temos $a^{-1} \in A$, daí,

$$a \cdot a^{-1} = 1 \in I \quad (*)$$

Agora, vamos provar que $A \subseteq I$. Seja $b \in A$, como $1 \in I$, então $1.b = b \in I$. Logo $A \subseteq I$.

A outra inclusão segue por def. de ideal.

Portanto, $A = \underline{I}$.

($\Leftarrow$) Se A e $\{0\}$ são os únicos ideais $\Rightarrow$ A é corpo

Dica:

1) A ideia é provar que todo elemento não nulo em A possui inverso multiplicativo.

(2) Tome $a \in A$, $a \neq 0$ e considere o ideal $\langle a \rangle$.

3) $1 \in A$.

Ex 6:

1a) Dem:

Vamos provar que $\underbrace{\mathbb{K}[x]/_{\langle p \rangle}}_{\text{anel}}$ é um corpo

Pelo ex 5, sabemos que $\mathbb{K}[x]/_{\langle p \rangle}$ é um anel (comutativo com unidade, isto é herdado do anel $\mathbb{K}[x]$). Precisamos provar que todo elemento não nulo do anel quociente possui inverso. Se $\bar{f} = f + \langle p \rangle \neq \bar{0}$, então temos que

p ∤ f (expliquem!). Daí, mdc(p, f) = 1.

Logo, pelo teorema de Bezout, existem $r, s \in \mathbb{K}[x]$ tal que

$$f \cdot r + p \cdot s = 1$$

Tomando as classes de equivalência:

$$\overline{f \cdot r + p \cdot s} = \overline{1} \Rightarrow \overline{f} \cdot \overline{r} + \overline{p} \cdot \overline{s} = \overline{1} \Rightarrow$$

$$\overline{f} \cdot \overline{r} + \overline{p}\,\overline{s} = 1 \Rightarrow \overline{f}\,\overline{r} = 1.$$

Logo $\mathbb{K}[x]/\langle p \rangle$ é um corpo. $\square$

(b) Dem: Queremos provar $\mathbb{K}[\bar{x})/_{\langle p \rangle}$ é um esp. vetorial sobre $\mathbb{K}$.

Temos que $\mathbb{K}[\bar{x}]$ é um esp. vetorial sobre $\mathbb{K}$ (verifiquem as prop.) e $\langle p \rangle$ é subespaço (verifique). Logo $\mathbb{K}[\bar{x}]/_{\langle p \rangle}$ é um espaço vetorial.

2ª opção: Verifiquem "na raça" que $\mathbb{K}[\bar{x}]/_{\langle p \rangle}$ satisfaz as cond. de esp. vetorial.

(c) Dem:

Considere $\mathbb{K}$ um corpo com k elementos. Pelo ex 2.b, sabemos que existe um polinômio $p(x) = x^2 + bx + c$ mônico e irredutível.

Veja que $\mathbb{K}[\bar{X}]/\langle p \rangle$ é um corpo (ex 6.a)

Precisamos apenas saber quantos elementos existem nesse corpo. Tome $\bar{f} \in \mathbb{K}[x]/\langle p \rangle$.

Caso $gr(f) > 2$, podemos usar o alg. da

Divisão e

$$f = p \cdot q + r, \quad 0 \leq gr(r) \leq 2 \text{ ou } r = 0$$

Se $r = 0$, temos que $\overline{f} = \overline{p} \cdot \overline{q} = \overline{0}$. Se $0 \leq gr(r) < 2$, $\overline{f} = \overline{r}$.

De todo modo, todo elemento de $\mathbb{K}[x]/\langle p \rangle$ é da forma $\overline{ax+b}$. Como temos k possibilidades tanto para a quanto para b, segue

que o nº de elementos em $K[x]/(p)$ é K^2.

Vejo que se $a_1x + b_1 \neq a_2x + b_2$ temos que $\overline{a_1x + b_1} \neq \overline{a_2x + b_2}$ (verifiquem).

∎