MAT 0120 Lista 12 - Solução:

Exercício 1:

Demonstração:

Inicialmente, consideremos que f é redutível, assim, $f = g \cdot h$, onde $0 < gr(g), gr(h) < gr(f)$ (vimos algo parecido no ex 22(a)). Assim, como f tem grau 2 ou 3, então ou g ou h tem grau 1. Consideremos que $gr(g) = 1$, daí, $g = ax + b$, $a, b \in \mathbb{K}$. Logo $\frac{b}{a} \in \mathbb{K}$ é raiz de g, e, portanto de f.

Reciprocamente, se f tem uma raiz, digamos $\alpha \in \mathbb{K}$ então $g = (x - \alpha)$ divide f. De fato,

$$f = g \cdot q + r, \quad 0 \leq gr(r) < g(g) = 1 \quad (*)$$

Veja que de (*), podemos concluir que $gr(r) = 0$. Logo r é um polinômio constante. Como $r(\alpha) = 0$ então $r = 0$. Assim $f = g \cdot q$, onde g e q são próprios logo f é redutível.

■

Exercício 2: Seja $\mathbb{K}$ um corpo finito com κ elementos

(a) Demonstração:

Considere $f = a_2 x^2 + a_1 x + a_0$. Note que $gr(f) = 2$ se, e somente se, $a_2 \neq 0$. Portanto, para a_2 temos 1 possibilidade, e, para a_1 e a_0 temos κ possibilidades. Pelo Princípio fundamental da contagem, o número de polinômios de grau 2 em $\mathbb{K}[x]$ é

$$1 \cdot \kappa \cdot \kappa = \kappa^2$$

(b) Demonstração:

Agora, queremos saber quantos polinômios irredutíveis de grau 2 em $\mathbb{K}[x]$ existem.

Inicialmente consideremos os polinômios mônicos. Veja que um polinômio f é redutível ou irredutível. Do item (a) já sabemos que o número de polinômios mônicos de grau 2 é κ^2. Vamos encontrar a quantidade de pol. mônicos redutíveis de grau 2. Veja 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 veja que $(x-a)(x-b) = (x-b)(x-a)$. Portanto, existem $\frac{k^2}{2}$ polinômios mônicos irredutíveis 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 número de polinômios irredutíveis de grau 2 em $\mathbb{K}[x]$ basta multiplicar $\frac{k^2}{2}$ por $(k-1)$, donde temos $\frac{k^2(k-1)}{2}$, isso se deve ao fato de que temos $k-1$ possibilidade do polinômios associados.

Exercício 3:

Demonstração:

Lembrando que, na lista 11, vimos que o mdc deve satisfazer as condições (i) e (iii) do ex. 14. Assim se d é o polinômio descrito no enunciado, suponhamos que exista $\tilde{d} \in \mathbb{K}[x]$ tal que $\tilde{d}$ satisfaça (i), com $gr(g) < gr(\tilde{g})$. Daí, como $\tilde{d} \mid f$ e $\tilde{d} \mid g$, usando (i), com relação à d, $\tilde{d} \mid d \Rightarrow d = \tilde{d} \cdot q \Rightarrow gr(d) = gr(\tilde{d}) + gr(q)$,

contradição. Portanto d é polinômio mônico de maior grau que divide f e g ∎

Exercício 4:

(i) Demonstração:

Basta provar que ⟨f⟩ satisfaz (1), (2) e (3). De fato, como $0 \in A$, $0 \cdot f = 0 \in \langle f \rangle$.

Sejam $g, h \in I$, então $g = a_1 f$ e $h = a_2 f$,

$g + h = (a_1 + a_2) \cdot f$, com $a_1 + a_2 \in A$, pois $a_1, a_2 \in A$.

Por fim, se $g \in I$ e $h \in A$ então $g = a \cdot f$ e

$g \cdot h = a \cdot f \cdot h = (a \cdot h) \cdot f$, onde $a \cdot h \in A$.

Logo, $g \cdot h \in I$. ∎

(ii) Demonstração:

Basta verificar (1), (2) e (3). ∎

(iii) Demonstração:

Queremos que todo ideal de $\mathbb{K}[x]$ seja principal, isto é, se I é um ideal que $\mathbb{K}[x]$, então, $I = \langle f \rangle$, $f \in \mathbb{K}[x]$

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

Consideremos que $I \neq \{0\}$, então existe pelo menos um $f \in I$, $f \neq 0$, com o menor grau (podemos tomar esse polinômio pelo PBO). Seja $g \in I$, pelo algoritmo da Divisão,

$$(1) \quad g = f \cdot q + r,$$

onde $0 \leq gr(r) < gr(f)$ ou $r = 0$

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

(iv) Demonstração:

Vamos considerar que A é um anel comutativo com unidade. Suponha que os únicos ideais são $\{0\}$ e A. Devemos provar que todo elemento de A possui inverso multiplicativo. Seja $a \in A$, $a \neq 0$, então $\langle a \rangle$ é um ideal de A. Como $\langle a \rangle \neq 0$, segue que $A = \langle a \rangle$. Logo, existe $b \in A$ tal que $a \cdot b = 1$. Assim,

como "a" é genérico, segue que A é um corpo. então

Por outro lado, considere que A é um corpo, se I é um ideal e $I \neq \{0\}$, temos que para $a \in I$, tomando $a^{-1} \in A$,

$$a \cdot a^{-1} = 1 \in I.$$

Logo, $A \subseteq I$ e, portanto $I = A$.

Exercício 6:

(a) Demonstração:

obs: Ideais maximais: Seja A um anel comutativo, um ideal $M \neq A$ diz-se maximal se não existe outro ideal N de A tal que $M \subsetneq N \subsetneq A$.
(Essa definição será usada numa prova alternativa do item a)

—•—

Veja que $\langle p(x) \rangle$ é um ideal como vimos em 4(i).
Agora, pelo ex 5, sabemos que $K[x]/\langle p \rangle$ é um anel (comutativo com unidade, isto é herdado de $K[x]$)

precisamos mostrar que todo elemento não nulo do anel quociente possui inverso. Seja $f + \langle p \rangle \neq \bar{0}$, então, devemos ter que $p \nmid f$, desse modo $mdc(p, f) = 1$. Assim, pelo teorema de Bezout, existem $r, s \in \mathbb{K}[\bar{x}]$

$$fr + ps = 1$$

Tomando as classes, temos que

$$\overline{fr + ps} = \bar{1} \Rightarrow \bar{f}\bar{r} + \bar{p}\bar{s} = \bar{1} \Rightarrow$$

$$\bar{f}\bar{r} = \bar{1}.$$

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

obs/ Como eu disse, uma alternativa é mostrar que $\langle p \rangle$ é um ideal maximal e provar que o quociente de um anel por um ideal maximal é um corpo.

(b) Demonstração:

Queremos mostrar que $\frac{\mathbb{K}[\bar{x}]}{\langle p \rangle}$ é um espaço vetorial

Temos que $\mathbb{K}[\bar{x}]$ é um espaço vetorial sobre $\mathbb{K}$. (Verifiquem as propriedades) e $\langle p \rangle$ é um subespaço (Verifique) Logo $\frac{\mathbb{K}[\bar{x}]}{\langle p \rangle}$ é um espaço vetorial. ☐

- Outra possibilidade é verificar os axiomas esp. vet usando $+ \cdot \bar{a} + \bar{b} = \overline{a+b}$ e $\alpha \cdot \bar{f} = \overline{\alpha \cdot f}$, $\forall \alpha \in \mathbb{K}$

(c) Demonstração:

Considere $\mathbb{K}$ um corpo com $\mathbb{K}$ elementos Pelo exercício 2b, tomemos um polinômio

$p(x) = x^2 + bx + c$ mônico e irredutível. Veja que $\frac{\mathbb{K}[\bar{x}]}{\langle p \rangle}$ é um corpo (ex 6.a) Precisamos apenas saber quantos elementos existem nesse corpo Tome $\bar{f} \in \frac{\mathbb{K}[\bar{x}]}{\langle p \rangle}$. Caso $gr(f) > 2$, podemos usar o a/g. da Divisão e

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

Se $r = 0$, temos que $\bar{f} = \overline{p \cdot q} = \bar{p} \cdot \bar{q} = \bar{0}$ Se

$0 \leq gr(r) < 2$, $\bar{f} = \bar{r}$.

Logo, de um modo geral todo elemento de $\frac{\mathbb{K}[\bar{x}]}{\langle p \rangle}$

é da forma $\overline{ax+b}$. Como temos K possibilidades tanto para a quanto para b, segue que o número de elementos de $K[x]/\langle p \rangle$ é K^2.

Veja que se $a_1x + b_1 \neq a_2x + b_2$ temos que

$\overline{a_1x + b_1} \neq \overline{a_2x + b_2}$ (verifique!)

■

Exercício 7:

Vamos provar que $\phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$ é irredutível sobre $\mathbb{Q}$. Observe que

$$\phi_p(x) = \frac{x^p - 1}{x - 1}$$

Considere o polinômio $g(x) = \phi_p(x+1) = \dfrac{(x+1)^p - 1}{(x+1) - 1} =$

$$\frac{\left(\sum_{i=0}^{p} \binom{p}{i} x^{p-i}\right) - 1}{x} = \frac{\sum_{i=0}^{p-1} \binom{p}{i} x^{p-i} + \binom{p}{p}1 - 1}{x} =$$

$$x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + p$$

Portanto, pelo critério de Eisenstein, g é irredutível em $\mathbb{Q}$.

obs: Vamos provar que se $f \in K[x]$ é redutível sobre K então $h(x) = f(x+1)$ também é redutível sobre K.

De fato se f é redutível em $\mathbb{K}[x]$ então

$$f = g \cdot q, \quad 0 < gr(g), gr(q) < gr(f)$$

Logo, $h(x) = \underbrace{g(x+1)}_{\tilde{g}} \underbrace{q(x+1)}_{\tilde{q}}$ será redutível pois

$$0 < gr(\tilde{g}), gr(\tilde{q}) < gr(h)$$

Usando nossa observação (na verdade, a contrapositiva) segue que $\phi_p(x)$ é irredutível em $\mathbb{Q}$, pois g é irred. em $\mathbb{Q}$. □

Exercício 8:

Demonstração:

Consideremos que $\mathbb{K}$ é algebricamente fechado. Então, temos que todo polinômio de grau 1 é irredutível (pois todos os divisores são impróprios). Seja $f \in \mathbb{K}[x]$ um polinômio de grau $n \geq 2$. Pela definição de corpo algebricamente fechado f possui uma raiz. Seja $\alpha \in \mathbb{K}$ essa raiz, então $(x-\alpha)$ divide f (Prove isso!). Portanto

$$f = (x-\alpha) \cdot q,$$

onde $(x-1)$ e f são divisores próprios de f e, dessa forma, f é redutível.

Por outro lado, se todo polinômio irredutível tem grau 1, consideremos $f \in \mathbb{K}[x]$, já vimos que f pode ser fatorado como produto de irredutíveis,

$$f = p_1 \cdots p_r$$

p_i's $\in \mathbb{K}[x]$ irredutíveis. Com isso, veja que p_1 é da forma $ax + b$. Considere $g = p_2 \cdots p_r$. Temos que $f = p_1 \cdot g$. Não é difícil ver que $\alpha = -\frac{b}{a} \in \mathbb{K}$ é uma raiz de f, pois

$$f(\alpha) = p_1(\alpha)\, g(\alpha) = \left[a\left(-\frac{b}{a}\right) + b\right] \cdot g(\alpha) =$$

$$[-b + b] \cdot g(\alpha) = 0 \cdot g(\alpha) = 0.$$

Portanto, todo polinômio $f \in \mathbb{K}[x]$ tem uma raiz.