Universidade Federal do Paraná
Centro Politécnico
ET-DMAT
Prof. Maria Eugênia Martin

MATE7003 - Álgebra Linear Avançada

Lista 4: Polinômios

Exercício 1. Seja A um anel, mostre que para todo $a, b \in A$ vale:

a. $0 \cdot a = a \cdot 0 = 0$

b. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

c. $(-a) \cdot (-b) = a \cdot b$

Se A tem identidade 1_A então:

d. $(-1_A) \cdot a = -a$

e. $(-1_A) \cdot (-1_A) = 1_A$

Exercício 2. Seja A um anel comutativo. Mostre que de fato o conjunto $(a) = \{x \cdot a \mid x \in A\}$ é um ideal de A para todo $a \in A$.

Exercício 3. Mostre que $(\mathbb{K}[x], +, \cdot)$ é um anel comutativo com identidade.

Exercício 4. Sejam $p, q \in \mathbb{K}[x]$ não nulos, mostre que:

a. Se $p \neq -q$ então $\deg(p+q) \leq \max\{\deg(p), \deg(q)\}$

b. $\deg(p \cdot q) = \deg(p) + \deg(q)$

Exercício 5. Seja $S \subseteq \mathbb{K}[x]$ um subconjunto não vazio, mostre que o conjunto

$$M(S) = \left\{ \sum_{p \in F} a_p \cdot p \in \mathbb{K}[x] \mid F \subseteq S \text{ é finito } a_p \in \mathbb{K}[x] \text{ para todo } p \in F \right\}$$

é um ideal de $\mathbb{K}[x]$ que contém S.

Exercício 6. Sejam $p_1, \ldots, p_n \in \mathbb{K}[x]$ polinômios coprimos dois a dois (i.e., $\mathrm{mdc}(p_i, p_j) = 1$ para todo $i \neq j$) tais que $p_i \mid q$ para todo i, onde $q \in \mathbb{K}[x]$. Mostre que $p_1 \cdot \ldots \cdot p_n \mid q$.

Exercício 7. Mostre que se $p \in \mathbb{K}[x]$ é irredutível e $p \nmid q$ então p e q são coprimos.

Exercício 8. Mostre que $p \in \mathbb{K}[x]$ é um polinômio primo se e somente se é irredutível.

Exercício 9. Mostre que os polinômios $x - \alpha$ e $x - \beta \in \mathbb{K}[x]$ são coprimos se e somente se $\alpha \neq \beta$.

Exercício 10. Sejam $p, q \in \mathbb{K}[x]$ polinômios não nulos e sejam $a_1, a_2, \ldots, a_m$ elementos distintos de $\mathbb{K}$. Se $p(a_i) = q(a_i)$ para cada $i = 1, 2, ..., m$ e m é maior do que os graus de p e de q, então $p = q$.

Exercício 11. Seja $p \in \mathbb{K}[x]$ um polinômio não constante. Mostre que

a. Se $\deg(p) = 1$ então p é irredutível.

b. Se $\deg(p) = 2$ ou 3 então p é irredutível se e somente se não tem raízes em $\mathbb{K}$.

c. É verdade que se $\deg(p) > 3$ então p é irredutível se e somente se não tem raízes em $\mathbb{K}$?

Exercício 12. Seja $T : \mathbb{K}^n \to \mathbb{K}^n$ um operador linear. Mostre que:

a. O conjunto de todos os polinômios p tais que $p(T) = 0$ formam um ideal não nulo $F(T)$ de $\mathbb{K}[x]$.

b. Seja m_T o gerador mônico de $F(T)$, mostre que se $p \in \mathbb{K}[x]$ é tal que $p(T) = 0$ então $m_T | p$.

Exercício 13. Seja $\mathbb{Q}$ o corpo dos racionais. Determine qual dos seguintes subconjuntos de $\mathbb{Q}[x]$ são ideais. Quando o conjunto for um ideal, ache seu gerador mônico.

a. O conjunto dos polinômios de grau impar.

b. O conjunto dos polinômios de grau maior igual que 5.

c. O conjunto dos polinômios tal que $p(0) = 0$.

d. O conjunto dos polinômios tal que $p(2) = p(4) = 0$.

e. A imagem do operador linear T definido por:

$$T\left(\sum_{i=0}^{n} c_i x^i\right) = \sum_{i=0}^{n} \frac{c_i}{i+1} x^{i+1}$$

Exercício 14. Ache o máximo divisor comum dos seguintes polinômios:

a. $2x^5 - x^3 - 3x^2 - 6x + 4$ e $x^4 + x^3 - x^2 - 2x - 2$

b. $3x^4 + 8x^2 - 3$ e $x^3 + 2x^2 + 3x + 6$

c. $x^4 - 2x^3 - 2x^2 - 2x - 3$ e $x^3 + 6x^2 + 7x + 1$

Exercício 15. O Teorema Fundamental da Álgebra diz que todo polinômio não constante $p \in \mathbb{C}[x]$ tem uma raiz em $\mathbb{C}$.

a. Use isso para mostrar que todo polinômio $p \in \mathbb{C}[x]$ se escreve como produto de fatores lineares.

b. Se p é um polinômio com coeficientes reais e α é uma raiz complexa de p, então o complexo conjugado $\overline{\alpha}$ é também uma raiz de p.

c. Seja α um número complexo com parte imaginária não nula. Mostre que $(x - \alpha)(x - \overline{\alpha})$ é um polinômio com coeficientes reais. Mostre que é irredutível sobre $\mathbb{R}$.

d. Mostre que todo polinômio com coeficientes reais se fatora em $\mathbb{R}[x]$ como produto de polinômio irredutíveis de graus 1 e 2.

e. Mostre que todo polinômio p de coeficientes reais que tem grau ímpar tem pelo menos uma raiz real.

Exercício 16. Mostre que se $p(x) = x^n - q \in \mathbb{Q}[x]$ e q é primo então $p(x)$ é irredutível sobre $\mathbb{Q}$. Isto mostra que existem polinômios irredutíveis de qualquer grau positivo em $\mathbb{Q}[x]$.

Exercício 17. [Fórmula de Taylor] A **derivada** do polinômio $p = a_0 + a_1 x + \cdots + a_n x^n$ é o polinômio $p' = a_1 + 2a_2 x \cdots + n a_n x^{n-1}$. Definimos o operador linear $D : \mathbb{K}[x] \to \mathbb{K}[x]$ tal que $D(p) = p'$ e assim temos que as derivadas formais de ordem superior de p são $p'' = D^2(p)$, $p''' = D^3(p)$, etc. Seja $\mathbb{K}$ um corpo de característica 0, $a$um elemento de $\mathbb{K}$ e n um inteiro positivo. Se $p \in \mathbb{K}[x]$ com $\deg(p) \leq n$, mostre que

$$p = \sum_{k=0}^{n} \frac{D^k(p)}{k!}(a)(x-a)^k.$$

Dica: use o Teorema do Binômio, $(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^k$.

Exercício 18. Seja c uma raiz do polinômio p, a multiplicidade de c como raiz de p é o maior inteiro positivo r tal que $(x-c)^r$ divide p. Seja $\mathbb{K}$ um corpo de característica 0 e $p \in \mathbb{K}[x]$ com $\deg(p) \leq n$. Mostre que o escalar c é uma raiz de p de multiplicidade r se, e somente se, $D^k(p)(c) = 0$ para todo $0 \leq k \leq r-1$ e $D^r(p)(c) \neq 0$.

Exercício 19. Assumindo o teorema fundamental da álgebra prove que se p e q são polinômios sobre os complexos, então $\text{mdc}(p,q) = 1$ se e somente se p e q não possuem raízes em comum.

Exercício 20. Seja p um polinômio mônico sobre os complexos. Prove que um polinômio tem todas as raízes distintas se e somente se p e p' (derivada) são coprimos.

Exercício 21.

a. Mostre que para qualquer $n \geq 2$, existe um polinômio $p \in \mathbb{K}_{n-1}[x]$ tal que x^n divide $1 + x - p^2$.

b. Deduza que para qualquer matriz nilpotente $N \in M_n(\mathbb{K})$, $I + N$ admite uma raiz quadrada, i.e.: existe $A \in M_n(\mathbb{K})$ tal que $I + N = A^2$.

c. Dê um exemplo para $n = 3$.

Exercício 22. [Resultado do tipo Bezout em $M_n(\mathbb{Z})$)] Sejam $A, B \in M_n(\mathbb{Z})$ matrizes invertíveis. Assuma que seus determinantes são inteiros coprimos (i.e., $\text{mdc}(\det A, \det B) = 1$). Mostrar que existem matrizes $U, V \in M_n(\mathbb{Z})$ tais que $AU + BV = I_n$.

Exercício 1)

a) $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$
$\Rightarrow 0 \cdot a = 0$
Análogo p/ $a \cdot 0$.

b) $a \cdot (-b) + (a \cdot b) = a \cdot (b + (-b))$
$= a \cdot 0 = 0 \Rightarrow$
$\Rightarrow a \cdot (-b) = -(a \cdot b)$
$(-a) \cdot b + (a \cdot b) = ((-a) + a) \cdot b = 0 \cdot b = 0$
$\Rightarrow (-a) \cdot b = -(a \cdot b)$

c) $(-a)(-b) + (-(a \cdot b)) = (-a)(-b) + (-a)(b)$
$= (-a)(-b+b)$
$= (-a) \cdot 0 = 0$
Logo $(-a)(-b) = (a \cdot b)$

d) $(-1) \cdot a + a = (-1+1) a = 0 \cdot a = 0$
$\Rightarrow (-1) \cdot a = -a$

e) $(-1) \cdot (-1) + (-1) = (-1)(-1) + (-1) \cdot 1$
$= (-1) \cdot (1 + (-1))$
$= (-1) \cdot 0 = 0$
$\Rightarrow (-1)(-1) = 1$

Exercício 2)

De fato, dados $x \in A$ e $y \in (a)$, temos que $\exists z \in A$, $y = z \cdot a$.
Assim $x \cdot y = x \cdot (z \cdot a) = (x \cdot z) \cdot a \in (a)$, pois $x \cdot z \in I$.

Exercício 3)

De fato, $\mathbb{K}[x]$ é comutativo pois $\mathbb{K}$ o é.
Além disso se $1 = 1_{\mathbb{K}} \in \mathbb{K}[x]$ e $p = \sum a_i x^i$, então

$$1 \cdot p = 1 \cdot \sum a_i x^i = \sum a_i x^i$$

Logo $1_{\mathbb{K}} = 1_{\mathbb{K}[x]}$.

Exercício 4)

Sejam $p, q \in \mathbb{K}[x]$ não nulos.

a) Se $p \neq q$, então $p + q \neq 0$, logo $\exists \deg(p+q)$.
Sejam $p = a_0 + a_1 x + \dots + a_n x^n$, $a_n \neq 0$ e
$q = b_0 + b_1 x + \dots + b_m x^m$, $b_m \neq 0$.
Assim se $n > m$

$$p + q = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_m + b_m)x^m + a_{m+1}x^{m+1} + \dots + a_n x^n$$

$a_n \neq 0 \Rightarrow \deg(p+q) = n = \deg(p) = \max\{\deg(p), \deg(q)\}$

Se $m < n$, vale análogo.

Agora, se $n = m$, então
$$(p+q) = (a_0 + b_0) + \dots + (a_n + b_n) x^n \neq 0$$
Se $a_n + b_n = 0 \Rightarrow \deg(p+q) < n = \max\{\deg(p), \deg(q)\}$. Se $a_n + b_n \neq 0 \Rightarrow \deg(p+q) = n = \max$. $\square$

b) Sejam p e q como em a. Então
$$p \cdot q = \sum_{j=0}^{n+m} \Big(\underbrace{\sum_{k=0}^{j} a_k b_{j-k}}_{c_j} \Big) x^j$$

Assim
$$c_{n+m} = \sum_{k=0}^{n+m} a_k b_{n+m-k}$$

Mas $\quad b_{n+m-k} = 0, \quad \forall k < n$

e $\quad a_k = 0, \quad \forall k > n$

Logo
$$c_{n+m} = a_n b_m \neq 0$$
Pois $\mathbb{K}$ é corpo, e $\deg(p \cdot q) = n + m = \deg(p) + \deg(q)$.

Exercício 5)

Seja $S \subseteq \mathbb{K}[x]$ não vazio. Mostre que
$$M(S) = \left\{ \sum_{p \in F} a_p \cdot p \in \mathbb{K}[x] : F \subseteq S \text{ é finito e } a_p \in \mathbb{K}[x], \forall p \in F \right\}$$

é um ideal de $\mathbb{K}[x]$ que contém S.

Dem.)

Seja $u = \sum_{i=1}^{n} a_{p_i} \cdot p_i \in M(S)$, i.e: $p_1, \dots, p_n \in S$ e $a_{p_1}, \dots, a_{p_n} \in \mathbb{K}[x]$.

Seja $x \in \mathbb{K}[x]$.

Então

$$x \cdot u = x \cdot \sum_{i=1}^{n} a_{p_i} p_i = \underbrace{\sum_{i=1}^{n} (\overbrace{x \cdot a_{p_i}}^{\in \mathbb{K}[x]}) \cdot \overbrace{p_i}^{\in S}}_{\in M(S)}$$

Logo $M(S)$ é ideal, e claro, $S \subset M(S)$. $\square$

Exercício 6)

De fato, provemos por indução em n. Se $n=1$, OK. Suponha que vale para $i = n$.

Então se $p_1, \dots, p_{n+1}$ são coprimos 2 a 2 e tais que $p_i | q$, $\forall i = 1, \dots, n$

Note que $\exists \alpha, \beta$ tais que $\alpha p_1 + \beta p_2 = 1$ e $\exists q_1, q_2$ $p_1 q_1 = q = p_2 q_2$

Assim

$$p_1 p_2 (\alpha q_2 + \beta q_1) = \alpha p_1 p_2 q_2 + \beta p_2 p_1 q_1$$
$$= \alpha p_1 q + \beta p_2 q$$
$$= (\alpha p_1 + \beta p_2) \cdot q$$
$$= q$$

Logo, $p_1 \cdot p_2 \mid q$

Agora, $p_1 \cdot p_2, p_3, \dots, p_{n+1} \mid q$ e $mdc(p_1 \cdot p_2, p_i) = mdc(p_j, p_i) = 1$, $\forall_{j,} i = 3, 4, \dots, n+1 \Rightarrow$, pela hipótese de indução que $(p_1 \cdot p_2) \cdot p_3 \cdot \ldots \cdot p_{n+1} \mid q$ $\square$

De fato, note que $\exists \alpha, \beta, \gamma, \mu$ /

$$\alpha p_1 + \beta p_3 = 1$$
$$\gamma p_2 + \mu p_3 = 1$$

Assim

$$(\alpha\gamma) p_1 p_2 + (\beta\gamma p_2 + \alpha\mu p_1 + \beta\mu p_3) p_3 = 1$$

$\Rightarrow mdc(p_1 p_2, p_3) = 1$ $\square$

Exercício 7)

De fato, se $m \mid p$ e $m \mid q$, p irredutível $\Rightarrow$ $\Rightarrow m = 1$ ou $m = p$. Como $p \nmid q \Rightarrow m = 1$ e logo $mdc(p, q) = 1$.

Exercício 8)

Suponha p primo e $p \mid ab$. SPG, podemos assumir que $p \mid a$. Então $a = p \cdot v$, para algum v, e logo

$$p = ab = p \cdot v \cdot b$$

Como $K[x]$ é domínio de integridade e

$$p(1 - v \cdot b) = 0$$

Isto implica que $v \cdot b = 1$ e logo b

é unidade.
Agora suponha p irredutível e $p|ab$.
Ainda, suponha que $p \nmid a. \Rightarrow mdc(p,a) = 1$
Pelo Teorema de Gauss $\Rightarrow p|b$ $\square$

Exercício 9)

Se $\alpha = \beta$, $x-\alpha = x-\beta$ e $mdc(x-\alpha, x-\alpha) = x-\alpha \neq 1$. Seja $\alpha \neq \beta$ e suponha que $m \mid x-\alpha$ e $m \mid x-\beta$. Então $\deg(m) \leq \deg(x-\alpha) = 1$. Mas se $x-\alpha = m(x)q(x) \Rightarrow 0 = m(\alpha)q(\alpha) \Rightarrow$ α é raiz de m ou q. Logo, se α é raiz de m, então $m = (x-\alpha) \cdot u$, $u \in K$, pois $\deg(m) \leq 1$. Se α é raiz de q, então $\deg(m) = 0$ e $m = 1$. Mas se $m = (x-\alpha) \cdot u$, temos que $m \mid x-\beta \Rightarrow x-\beta = (x-\alpha) \cdot u \cdot v$, $u, v \in K$, absurdo, pois igualando coeficientes temos

$$\begin{cases} 1 = u \cdot v \\ \beta = \alpha \cdot u \cdot v \end{cases} \Rightarrow \beta = \alpha \rightarrow\leftarrow$$

Exercício 10)

De fato, pelo algoritmo da divisão temos que

$$p(x)-q(x)=(x-a_1)\cdots(x-a_m)S(x)$$

Mas, se $p(x)-q(x)\neq 0$, então

$$\deg(p(x)-q(x))\leq \max\{\deg(p),\deg(q)\}$$

e

$$\deg((x-a_1)\cdots(x-a_m)S(x))=\underbrace{m+\deg(S)}_{\geq m}$$

Logo

$$m\leq \deg(p(x)-q(x))\leq \underbrace{\max\{\deg(p),\deg(q)\}}_{<m}$$

$\Rightarrow m<m$ ⨳. Logo $p(x)-q(x)=0$, i.e: $p=q$

Exercício 11)

a) Suponha $m|p$, $p=m\cdot q$.

Como

$$1=\deg(p)=\deg(m\cdot q)$$
$$=\deg(m)+\deg(q)$$

temos $\deg(m)=1$ e $\deg(q)=0$ ou $\deg(m)=0$ e $\deg(q)=1$, logo p é irredutível.

b) Suponha que p possui raiz $\alpha\in K$

Então pelo algoritmo da divisão

$$p(x) = (x-\alpha)\, q(x) + r$$

com $r=0$ ou $\deg(r) < 1 \Rightarrow \deg(r)=0$.

Mas

$$0 = p(\alpha) = \cancel{(\alpha-\alpha)}^{\,0}\, q(x) + r$$

Logo $r=0$, i.e: $p(x) = (x-\alpha)\, q(x)$

Como $\deg(p) = 2$ ou 3 e $\deg(x-\alpha) = 1$, devemos ter $\deg(q) = 1$ ou 2, i.e: p é redutível. Logo p irredutível $\Rightarrow p$ não possui raízes em $\mathbb{K}$. Agora suponha que $p(x)$ não possui raízes em $\mathbb{K}$, $\deg(p)=2$ ou 3. Suponha

$$p(x) = m(x)\, q(x)$$

Então $3 = \deg(m) + \deg(q)$ Ⓐ

ou $2 = \deg(m) + \deg(q)$ Ⓑ

Logo, em Ⓐ, temos $\deg(m) = 3$ e $\deg(q) = 0$ ou $\deg(m) = 2$ e $\deg(q) = 1$ ou vice-versa. Mas, $\deg(q) = 1 \Rightarrow q(x) = a_1 x + a_0$, $a_1 \neq 0$

Assim $q(-a_0/a_1) = 0$ e portanto

$$p(-a_0/a_1) = 0$$

, contradição com o fato de p não possuir raízes em $\mathbb{K}$. Logo em Ⓐ só ocorre $\deg(m)=3$ e $\deg(q)=0$ ou $\deg(m)=0$ e $\deg(q)=3$,

isto é, p é irredutível.
Em (B) temos $\deg(m) = 2$ e $\deg(q) = 0$ ou $\deg(m) = 1$ e $\deg(q) = 1$ ou $\deg(m) = 0$ e $\deg(q) = 2$.
Mas, se $\deg(q) = 1$, assim como antes podemos escrever $q(x) = a_1 x + a_0$ de modo que $p(-a_0/a_1) = 0$ $\rightarrow\leftarrow$
Logo só ocorre $\deg(m) = 0$, $\deg(q) = 2$ ou $\deg(m) = 2$ e $\deg(q) = 0$, isto é, p é irredutível.

c) Não.
O polinômio

$$p(x) = (x^2+1)(x^2+2) \in \mathbb{R}[x]$$
$$= x^4 + 3x^2 + 2$$

é redutível, mas não possui raízes em $\mathbb{R}$.

Exercício 12)

a) Seja $p \in F(T)$ e $q \in \mathbb{K}[x]$. Então

$$(p \cdot q)(T) = p(T) \cdot q(T)$$
$$= 0 \cdot q(T)$$
$$= 0$$

Logo $p \cdot q \in F(T)$, i.e.: $F(T)$ é ideal

Além disso, como $\mathcal{L}(\mathbb{K}^n, \mathbb{K}^n)$ tem dimensão n^2, o conjunto

$$\{1, T, T^2, \dots, T^{n^2}\}$$

possui n^2+1 elementos e portanto é L.D. isto significa que $\exists\, a_0, a_1, \dots, a_{n^2} \in \mathbb{K}$ tais que

$$a_0 Id + a_1 T + \dots + a_{n^2} T^{n^2} = 0$$

Assim, pondo

$$p(x) = a_0 + a_1 X + \dots + a_{n^2} X^{n^2} \in \mathbb{K}[X],$$

temos que $p(T) = 0 \therefore p \in F(T)$.

b) De fato, se $p(T) = 0 \Rightarrow p \in F(T)$, logo como m_T é gerador $\exists\, q \in \mathbb{K}[x]$,

$$m_T \cdot q = p$$

$\Rightarrow m_T \mid p$

Exercício 13)

a) Não é ideal: seja I tal conjunto. Temos que $X+1, X-1 \in I$, mas

$$(X+1)\cdot(X-1) = X^2 - 1 \notin I$$

pois $\deg(X^2-1) = 2$.

b) É ideal se permitirmos $0_{\mathbb{Q}[x]} \in I$.

De fato, se $p \in I$ e $q \in \mathbb{Q}[x]$, temos

a) Se $p = 0 \Rightarrow p \cdot q = 0 \in I$

b) Se $p \neq 0 \Rightarrow \deg(p) \geq 5 \Rightarrow \deg(p \cdot q) =$
$= \deg(p) + \deg(q) \geq \deg(p) \geq 5 \Longrightarrow$
$\Rightarrow p \cdot q \in I$

c) É ideal: se $p \in I$ e $q \in \mathbb{Q}[x]$, então
$(p \cdot q)(0) = p(0) \cdot q(0) = 0 \Rightarrow p \cdot q \in I$

d) É ideal, raciocínio análogo ao em c

e) É ideal, pois se $p = \sum_{i=0}^{n} \frac{b_{i+1}}{i+1} x^{i+1} \in I$,
$q(x) = \sum_{j=0}^{m} a_j b_j$
Então

$$(p \cdot q)(x) = \sum_{k=0}^{n+m} c_k x^k$$

onde
$$c_k = \sum_{l=0}^{k} a_l b_{k-l}$$

$c_1 x^1 + c_2 x^2$

Assim $c_0 = a_0 b_0 = 0$
De modo que tomando $c_1 x^0 + c_2 x^1$

$$m(x) = \sum_{k=0}^{n+m-1} c_{k+1}(k+1)\, x^{k}$$

temos $\int (m(x)) = \sum_{k=0}^{n+m-1} \frac{c_{k+1}(k+1)}{(k+1)} x^{k+1}$

$$= \sum_{k=0}^{n+m} c_k x^k = p \cdot q$$

Exercício 14)

?

Exercício 15)

$\longrightarrow$ Provaremos por indução em $\deg(p) = n$.

a) Seja $P(x) \in \mathbb{C}[x]$ não constante.
Pelo T.F.A. $\exists\, \alpha \in \mathbb{C}$ tal que $p(\alpha) = 0$.
Então, pelo algoritmo de divisão,

$$p(x) = (x - \alpha)\, q(x)$$

Mas como $\deg(p) = \deg(q) + 1 \Rightarrow \deg(q) = n - 1 < n$

Logo por hipótese $q(x) = \prod_{k=1}^{n-1} (x - \alpha_k)$, donde

$$P(x) = (X - \alpha) \prod_{k=1}^{n-1} (X - \alpha_k)$$

e P também é produto de fatores lineares.

b) De fato, pois suponha $p(x) = \sum_{j=0}^{n} a_j x^j$
Então

$$p(\bar{\alpha}) = \sum_{j=0}^{n} a_j (\bar{\alpha})^j = \sum_{j=0}^{n} \overline{a_j}\, \overline{(\alpha)^j}$$

$$= \overline{\sum_{j=0}^{n} a_j (\alpha)^j} = \overline{p(\alpha)} = \bar{0} = 0$$

c) Seja $\alpha = a + bi$, $b \neq 0$. Então

$$P(x) = (X - \alpha)(X - \bar{\alpha}) = (X - a - bi)(X - a + bi)$$

$$= (X - a)^2 - (bi)^2$$

$$= X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[x]$$

Além disso, $deg(p)=2$, logo, pelo exercício 11, p é irredutível sobre $\mathbb{R}$.

d) De fato, seja $p(x) \in \mathbb{R}[x]$.
Então vendo $p(x) \in \mathbb{C}[x]$, temos que, por (a), p se fatora em produto de fatores lineares e que, por (b), se α é raiz de p, $\overline{\alpha}$ também o é, logo

$$p(x) = \prod_{k=1}^{n} (x-\alpha_k)(x-\overline{\alpha}_k) \cdot \prod_{j=1}^{m} (x-\beta_j)$$

Onde $\alpha_k \in \mathbb{C}$, $Im(\alpha_k) \neq 0$ e $\beta_j \in \mathbb{R}$
Mas, por (c), para cada $k=1,\dots,n$, $\exists\, p_k \in \mathbb{R}[x]$ tal que

$$p_k(x) = (x-\alpha_k)(x-\overline{\alpha}_k)$$

com $deg(p_k)=2$
Logo

$$p(x) = \prod_{k=1}^{n} p_k(x) \cdot \prod_{j=1}^{m} (x-\beta_j)$$

$\square$

e) Se $p(x) \in \mathbb{R}[x]$ é polinômio de grau ímpar, pelo exercício (c) temos que $m \equiv 1 \mod 2$ e logo $\exists\, \beta \in \mathbb{R}$ tal que $(x-\beta) \mid p(x)$
$\Rightarrow p(\beta) = 0$

Exercício 16)

Seja $n \geq 2$. Então $p(x) \in \mathbb{R}[x]$ e como $p(\sqrt[n]{p}) = 0$, temos

0

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4$$

$\downarrow ''$

$$2a_2 + 3 \cdot 2 \cdot a_3 \cdot x + 4 \cdot 3 \cdot a_4 x^2$$

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

$\hookrightarrow n a_n x^{n-1} + (n-1)$

$\hookrightarrow (n)(n-1)(n-2)$

Exercício 17)

De fato, pondo $q(x) = \sum \frac{D^k(p)}{k!}(a)(x-a)^k$

Basta mostrar que $D^k(p-q)(a) = 0$ $\forall k \in \mathbb{N}$.

De fato, note que, para $k \leq n$, temos

$$D^k(p(a)) = n(n-1)\cdots(n-k+1)a_n x^{n-k} + (n-1)(n-2)\cdots(n-k)a_{n-1}x^{n-1-k} + \cdots + (k)(k-1)\cdots 2\cdot 1\, a_k x^0 \Big|_a$$

$$= \frac{n!}{k!}a_n a^{n-k} + \frac{(n-1)!}{(k-1)!}a_{n-1}a^{n-1-k} + \cdots + k!\,a_k$$

Enquanto que $D^l(q)(a) = D^l(p)(a)$, $l = 1, \dots m$ e $D^l(p)(a) = 0 = D^l(q)(a)$ se $l > m$, logo $p = q$.

Exercício 18)

Suponha que c é raiz de multiplicidade r de p. Então

$$p(x) = (x-c)^r q(x)$$

e $q(c) \neq 0$. Assim, se $0 \leq k \leq r-1$,

$$D^k(p)(c) = \sum_{l=0}^{k} \binom{k}{l} D^l((x-c)^r)\Big|_c D^{k-l}(q(x))\Big|_c$$

$(*)$

Mas para $l = 0, 1, \dots, k$
$$D^l((x-c)^r)|_{x=c} = 0$$
Logo $D^k(p)(c) = 0$ ..
Agora, se $k = r$, temos
$$D^r((x-c)^r)|_{x=c} = r!$$

e logo
$$D^r(p)(c) = D^r((x-c)^r)|_c \cdot D^0(q(x))|_c$$
$$= r!\, q(c) \neq 0.$$

Reciprocamente, suponha que $D^k(p)(c) = 0$, p/ $0 \leq k \leq r-1$ e $D^r(p)(c) \neq 0$.
Então pela fórmula de Taylor em c, temos
$$p(x) = \sum_{k=r}^{n} \frac{D^k(p)(c)}{k!}(x-c)^k$$
$$= (x-c)^r \cdot \sum_{k=0}^{n-r} \frac{D^{k+r}(p)(c)}{(k+r)!}(x-c)^k$$
$\Rightarrow (x-c)^k \mid p$, $k = 0, 1, \dots, r$
Além disso, $D^r(p)(c) \neq 0 \Rightarrow$
$$p(x) = (x-c)^r \cdot q(x)$$
e $q(c) = \frac{D^r(p)(c)}{r!} \neq 0$, logo c não é raiz de q e r é o maior nú_

mero tq $(x-c)^k \mid p$.

Exercício 19)

Suponha que $p(\alpha)=q(\alpha)=0$. Então $(x-\alpha) \mid p$ e $(x-\alpha) \mid q \Rightarrow mdc(p,q) \neq 1$.
Logo $mdc(p,q)=1 \Rightarrow p$ e q não possuem raízes em comum.
Reciprocamente, sejam $\alpha_1, \dots, \alpha_n$ as raízes de p e $\beta_1, \dots, \beta_m$ as raízes de q.
Então

$$p(x)=(x-\alpha_1)\cdot \dots \cdot (x-\alpha_n)$$
$$q(x)=(x-\beta_1)\cdot \dots \cdot (x-\beta_m)$$

Assim, se $m \mid p \Rightarrow \exists I \subset \{1,\dots,n\}, m=\prod_{i\in I}(x-\alpha_i)$
e $m \mid q \Rightarrow \exists J \subset \{1,\dots,m\}, m=\prod_{j\in J}(x-\beta_j)$
Como $\alpha_i \neq \beta_j, \forall i,j \Rightarrow I=J=\phi$, i.e: $m=1$
e $mdc(p,q)=1$. ?

Exercício 20)

Suponha que p tem raiz dupla α.
Então

$$p(x)=(x-\alpha)^2 q(x)$$

Assim

$$p'(x)=(x-\alpha)^2 q'(x)+2(x-\alpha)q(x)$$

$\Rightarrow p'(\alpha)=0 \therefore p$ e p' tem raiz α em

comum.
Suponha agora que p e p' tem raiz α em comum.
Então
$$p(x) = (x-\alpha)q(x) \text{ e } p'(x) = (x-\alpha)r(x)$$
Mas
$$p'(x) = q(x) + (x-\alpha)q'(x) = (x-\alpha)r(x)$$
Assim $0 = p'(\alpha) = q(\alpha)$ e logo $(x-\alpha) | q \Rightarrow$
$\Rightarrow (x-\alpha)^2 | p \Rightarrow \alpha$ é raiz de mult. maior que 1

Ex 22)

$\exists\, r, s \in \mathbb{Z},$

$$r \det A + s \det B = 1$$

$$r\, A\, (\mathrm{cof}(A))^T = r \cdot \det A \cdot Id$$
$$s \cdot B \cdot \mathrm{cof}(B)^T = s \cdot \det B \cdot Id$$

Assim

$$A\, \underbrace{r\,(\mathrm{cof}(A))^T}_{U} + B \cdot \underbrace{s\,(\mathrm{cof}(B))^T}_{V} = Id$$

$\square$

Exercício 21) a)

Para $n=2$ temos $x^2 \mid 1+x-(a_0+a_1x)^2$

$\Rightarrow x^2 \mid 1+x-a_0^2-2a_0a_1x+a_1^2x^2$

$\Rightarrow a_0=1 \Rightarrow a_1=-1/2$

Para $n=3$ temos

$$x^3 \mid 1+x-(a_0+a_1x+a_2x^2)^2$$

$\Rightarrow x^3 \mid 1+x-a_0^2-2a_0a_1x-(a_1^2+2a_0a_2)x^2-$

$- 2a_1 a_2 x^3 - a_2^2 x^4$

$\Rightarrow a_0 = 1 \Rightarrow a_1 = -1/2 \Rightarrow a_2 = -1/8$, etc...

b) De fato,

$$1 + x - p^2 = x^n \cdot q$$

$$\Downarrow$$

Aplicando em N

$$Id + N - (p(N))^2 = \cancel{N^n} \cdot q(N)$$

$$\Rightarrow Id + N = (p(N))^2$$

Logo $p(N)$ é raiz de $Id + N$ ∎