Oitava Lista

MAT0222 – Álgebra Linear II

Prof. Daniel Victor Tausk
01/06/2014

Exercício 1. Seja K um corpo e sejam $p_1(X), \dots, p_n(X) \in K[X]$ polinômios. Um polinômio mônico $m(X) \in K[X]$ é dito um *mínimo múltiplo comum* (*mmc*) para os polinômios $p_1(X)$, ..., $p_n(X)$, se valem as seguintes condições:

(i) $m(X)$ é um múltiplo comum de $p_1(X)$, ..., $p_n(X)$, isto é, vale que:
$$p_i(X)|m(X),$$
para $i = 1, \dots, n$;

(ii) dado $\widetilde{m}(X) \in K[X]$, se $\widetilde{m}(X)$ é um múltiplo comum dos polinômios $p_1(X)$, ..., $p_n(X)$, então $m(X)|\widetilde{m}(X)$.

Mostre que, se $p_1(X), \dots, p_n(X) \in K[X]$ são todos não nulos, então existe um único $m(X) \in K[X]$ que é mínimo múltiplo comum dos polinômios $p_1(X)$, ..., $p_n(X)$. (Sugestão: considere o ideal $\bigcap_{i=1}^n \langle p_i(X) \rangle$ de $K[X]$.)

Definição 1. Seja K um corpo e seja $p(X) = a_0 + a_1 X + \dots + a_n X^n \in K[X]$ um polinômio, onde $a_0, a_1, \dots, a_n \in K$. Definimos:

- a *avaliação* de $p(X)$ num elemento $u \in K$, fazendo:
$$p(u) = a_0 + a_1 u + \dots + a_n u^n \in K;$$
- a *avaliação* de $p(X)$ numa matriz $A \in M_n(K)$, fazendo:
$$p(A) = a_0 I + a_1 A + \dots + a_n A^n \in M_n(K),$$
onde $I \in M_n(K)$ denota a matriz identidade;
- a *avalição* de $p(X)$ num operador linear $T : V \to V$, fazendo:
$$p(T) = a_0 I + a_1 T + \dots + a_n T^n \in \mathrm{L}(V, V),$$
onde V é um espaço vetorial sobre K e $I : V \to V$ denota o operador identidade.

Exercício 2. Seja K um corpo e sejam $p(X), q(X) \in K[X]$ polinômios. Mostre que:

(a) $(p+q)(u) = p(u) + q(u)$ e $(pq)(u) = p(u)q(u)$, para todo $u \in K$;

(b) $(p+q)(A) = p(A) + q(A)$ e $(pq)(A) = p(A)q(A)$, para toda matriz $A \in M_n(K)$;

(c) $(p+q)(T) = p(T) + q(T)$ e $(pq)(T) = p(T)q(T)$, para todo operador linear $T : V \to V$, onde V é um espaço vetorial sobre K.

Exercício 3. Sejam K um corpo e V um espaço vetorial sobre K de dimensão finita. Seja $\mathcal{B}$ uma base de V. Mostre que se $T : V \to V$ é um operador linear e $p(X) \in K[X]$ é um polinômio, então:

$$[p(T)]_{\mathcal{B}} = p\big([T]_{\mathcal{B}}\big).$$

Exercício 4. Sejam K um corpo e V um espaço vetorial sobre K. Mostre que se W é um subespaço T-invariante de V e se $p(X) \in K[X]$ é um polinômio, então W também é $p(T)$-invariante; além do mais, avaliando p no operador $T|_W : W \to W$, obtemos o operador $p(T)|_W : W \to W$.

Exercício 5. Sejam K um corpo e V um espaço vetorial sobre K. Mostre que se $T : V \to V$ e $S : V \to V$ são operadores lineares que comutam (isto é, $T \circ S = S \circ T$), então $p(T)$ e $q(S)$ também comutam, para quaisquer polinômios $p(X), q(X) \in K[X]$. Mostre também que se $A, B \in M_n(K)$ são matrizes que comutam, então $p(A)$ e $q(B)$ comutam, para quaisquer polinômios $p(X), q(X) \in K[X]$.

Exercício 6. Seja $p(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{C}[X]$ um polinômio com coeficientes complexos, onde $a_0, a_1, \ldots, a_n \in \mathbb{C}$. O *complexo conjugado de* $p(X)$ é o polinômio $\bar{p}(X) \in \mathbb{C}[X]$ definido por:

$$\bar{p}(X) = \overline{a_0} + \overline{a_1}\, X + \cdots + \overline{a_n}\, X^n \in \mathbb{C}[X].$$

Mostre que:

(a) dados $p(X) \in \mathbb{C}[X]$ e $z \in \mathbb{C}$, então $\overline{p(z)} = \bar{p}(\bar{z})$;

(b) dados $p(X), q(X) \in \mathbb{C}[X]$, então:

$$\overline{p+q}(X) = \bar{p}(X) + \bar{q}(X), \quad \overline{pq}(X) = \bar{p}(X)\bar{q}(X);$$

(c) dados $p(X) \in \mathbb{C}[X]$ e uma matriz $A \in M_n(\mathbb{C})$, então $\overline{p(A)} = \bar{p}(\bar{A})$.

Exercício 7 (fórmula de interpolação de Lagrange)**.** Sejam K um corpo e sejam dados $u_1, \ldots, u_n, v_1, \ldots, v_n \in K$, com $u_1, \ldots, u_n$ distintos. Considere o polinômio:

$$p(X) = \sum_{i=1}^{n} v_i \, \frac{(X - u_1) \cdots \widehat{(X - u_i)} \cdots (X - u_n)}{(u_i - u_1) \cdots \widehat{(u_i - u_i)} \cdots (u_i - u_n)} \in K[X],$$

onde o chapéu indica que o fator está omitido do produtório. Mostre que $p(X)$ é o único polinômio de grau menor do que n tal que $p(u_i) = v_i$, para todo $i = 1, \ldots, n$.

Exercício 8. Seja V um espaço vetorial de dimensão finita sobre $K = \mathbb{R}$ ou $K = \mathbb{C}$ munido de um produto interno e seja $T : V \to V$ um operador linear. O objetivo deste exercício é mostrar o seguinte resultado: se T é normal, então existe um polinômio $p(X) \in K[X]$ tal que $p(T) = T^\dagger$. (A recíproca é obviamente verdadeira, isto é, se $T^\dagger = p(T)$ para algum $p(X) \in K[X]$, então T é normal.)

(a) Mostre o resultado supondo que $K = \mathbb{C}$. (Sugestão: pela fórmula de interpolação de Lagrange, existe $p(X) \in \mathbb{C}[X]$ tal que $p(\lambda) = \bar{\lambda}$, para todo autovalor $\lambda \in \mathbb{C}$ de T. Use o Teorema Espectral.)

(b) Seja $A \in M_n(\mathbb{C})$ uma matriz complexa e suponha que A seja normal, isto é, A comuta com a sua matriz adjunta $A^\dagger = \overline{A^{\mathrm{t}}}$. Mostre que existe $p(X) \in \mathbb{C}[X]$ tal que $p(A) = A^\dagger$. (Sugestão: considere o espaço vetorial $\mathbb{C}^n$ munido de seu produto interno canônico e aplique o resultado do item (a) ao operador $T : \mathbb{C}^n \to \mathbb{C}^n$ que é representado por A na base canônica.)

(c) Mostre o resultado supondo que $K = \mathbb{R}$. (Sugestão: seja $A \in M_n(\mathbb{R})$ a matriz que representa T numa base ortonormal de V. Pelo resultado do item (b), existe $q(X) \in \mathbb{C}[X]$ tal que $q(A) = A^\dagger = A^{\mathrm{t}}$. Tome $p(X) = \frac{1}{2}\big(q(X) + \bar{q}(X)\big) \in \mathbb{R}[X]$. Use o resultado do item (c) do Exercício 6.)

Exercício 9. Seja V um espaço vetorial de dimensão finita sobre $K = \mathbb{R}$ ou $K = \mathbb{C}$ munido de um produto interno e seja $T : V \to V$ um operador normal.

(a) Mostre que todo subespaço de V invariante por T é também invariante por $T^\dagger$. (Sugestão: use os resultados dos Exercícios 4 e 8.)

(b) Mostre que se um operador linear $S : V \to V$ comuta com T, então ele também comuta com $T^\dagger$. (Sugestão: use os resultados dos Exercícios 5 e 8.)

Observação. O Exercício 3 da Sétima Lista mostra que o resultado do Exercício 8 e o resultado do item (a) do Exercício 9 não valem em geral se V tem dimensão infinita.

Os exercícios a seguir dão a fundamentação completa da teoria geral de anéis de polinômios com coeficientes em anéis. Podem ser um pouco abstratos para quem está tendo um primeiro contato com o assunto.

Exercício* 10. Seja R um anel e considere o conjunto $R[X]$ das seqüências quase nulas $(a_n)_{n\geq 0}$ de elementos de R, munido das operações:

$$(a_n)_{n\geq 0} + (b_n)_{n\geq 0} = (a_n + b_n)_{n\geq 0}, \quad (a_n)_{n\geq 0} \cdot (b_n)_{n\geq 0} = (c_n)_{n\geq 0},$$

onde:

$$c_n = \sum_{i=0}^{n} a_i b_{n-i}, \quad n \geq 0.$$

Mostre que:

(a) $R[X]$ é um anel;

(b) a aplicação $\iota : R \to R[X]$ definida por:

$$\iota(r) = (r, 0, 0, 0, \ldots) \in R[X],$$

é injetora e é um *homomorfismo de anéis*, isto é:

$$\iota(r_1 + r_2) = \iota(r_1) + \iota(r_2), \quad \iota(r_1 r_2) = \iota(r_1)\iota(r_2),$$

para todos $r_1, r_2 \in R$;

(c) se R tem unidade $1 \in R$, então $R[X]$ tem unidade e essa unidade é $\iota(1)$;

(d) se R é comutativo, então $R[X]$ é comutativo.

O anel $R[X]$ é chamado o *anel de polinômios* com coeficientes em R. Dado $p = (a_n)_{n\geq 0} \in R[X]$ não nulo, então o *grau* de p, denotado $\mathrm{gr}(p)$, é o maior índice $n \geq 0$ tal que $a_n \neq 0$; se $p = 0$, convencionamos que o grau de p é $-\infty$. Se p é não nulo, então o *coeficiente dominante* de p é a_n, onde $n = \mathrm{gr}(p)$.

(e) Suponha que o produto de elementos não nulos de R seja sempre não nulo[1]. Mostre que, nesse caso, o produto de elementos não nulos de $R[X]$ é não nulo. Mais especificamente, mostre que vale a igualdade:

$$\mathrm{gr}(pq) = \mathrm{gr}(p) + \mathrm{gr}(q),$$

para todos $p, q \in R[X]$ e que se p e q são não nulos, então o coeficiente dominante de pq é o produto do coeficiente dominante de p pelo coeficiente dominante de q.

Suponha agora que R tenha unidade e defina:

$$X = (0, 1, 0, 0, \ldots).$$

(f) Dados $a_0, a_1, \ldots, a_n \in R$, mostre que:

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n = (a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots),$$

onde identificamos cada elemento $r \in R$ com o elemento $\iota(r)$ de $R[X]$.

[1] Um anel comutativo com unidade em que vale essa propriedade é chamado um *domínio de integridade*. Todo corpo é um domínio de integridade.

Exercício* 11. Sejam R e S anéis e $\phi : R \to S$ um homomorfismo de anéis. Dado $p = (a_n)_{n\geq 0} \in R[X]$, defina p^ϕ fazendo:

$$p^\phi = \big(\phi(a_n)\big)_{n\geq 0} \in S[X].$$

Mostre que a aplicação:

$$R[X] \ni p \longmapsto p^\phi \in S[X]$$

é um homomorfismo de anéis, isto é, valem as igualdades:

$$(p+q)^\phi = p^\phi + q^\phi, \quad (pq)^\phi = p^\phi q^\phi,$$

para todos $p, q \in R[X]$. Note que o resultado do item (b) do Exercício 6 é um caso particular do resultado deste exercício, fazendo $R = S = \mathbb{C}$ e $\phi(z) = \bar{z}$.

Exercício* 12. Sejam R' um anel e $R \subset R'$ um subanel[2] de R'. Seja $u \in R'$ um elemento que comuta com R, isto é, $ur = ru$, para todo $r \in R$. Para $p = (a_n)_{n\geq 0} \in R[X]$, defina a *avalição de p em u*, fazendo:

$$p(u) = a_0 + a_1 u + \cdots + a_n u^n,$$

onde $n \geq 0$ é tal que $a_k = 0$ para todo $k > n$.

(a) Mostre que a *aplicação de avaliação em u*:

$$R[X] \ni p \longmapsto p(u) \in R' \tag{1}$$

é um homomorfismo de anéis, isto é, valem as igualdades:

$$(p+q)(u) = p(u) + q(u), \quad (pq)(u) = p(u)q(u),$$

para todos $p, q \in R[X]$. Esse resultado generaliza o resultado do item (a) do Exercício 2.

(b) Se S é um anel e $\phi : R' \to S$ é um homomorfismo de anéis, mostre que:

$$\phi\big(p(u)\big) = p^\phi\big(\phi(u)\big),$$

para todo $p \in R[X]$, onde p^ϕ é definido como no Exercício 11. Note que p^ϕ pertence ao anel de polinômios com coeficientes em $\phi[R]$, o qual é um subanel de S. Como $u \in R'$ comuta com R, temos que $\phi(u) \in S$ comuta com $\phi[R]$. Assim, estamos no contexto em que se define a avaliação $p^\phi\big(\phi(u)\big)$.

[2]Isso significa que: (a) se $r_1, r_2 \in R$, então $r_1 + r_2 \in R$ e $r_1 r_2 \in R$; (b) se $r \in R$, então $-r \in R$; (c) $0 \in R$; (d) as operações de R são as restrições das operações de R'. Nesse caso, R é também um anel.

Observação. Usando a terminologia dos Exercícios 11 e 12, aquilo que na Definição 1 foi denotado por $p(A)$, com $p \in K[X]$, $A \in M_n(K)$ e K um corpo, seria denotado por $p^\delta(A)$, onde $\delta : K \to M_n(K)$ é o homomorfismo de anéis definido por:

$$\delta(a) = aI, \quad a \in K,$$

e $I \in M_n(K)$ é a matriz identidade. Observe que p^δ pertence ao anel de polinômios com coeficientes em $\delta[K]$, que $\delta[K]$ é um subanel de $M_n(K)$ e que qualquer $A \in M_n(K)$ comuta com $\delta[K]$. O resultado do item (b) do Exercício 2 pode então ser obtido como corolário do resultado do Exercício 11 e do resultado do item (a) do Exercício 12; de fato, temos:

$$(p+q)^\delta(A) = (p^\delta + q^\delta)(A) = p^\delta(A) + q^\delta(A),$$
$$(pq)^\delta(A) = (p^\delta q^\delta)(A) = p^\delta(A)q^\delta(A),$$

para todos $p, q \in K[X]$. Considerações análogas podem ser feitas para o caso de avaliações da forma $p(T)$, onde $T : V \to V$ é um operador linear num espaço vetorial V sobre K. Nesse caso, o anel de matrizes $M_n(K)$ é substituído pelo anel $\mathrm{L}(V, V)$ de operadores lineares em V e a matriz identidade é substituída pelo operador identidade de V.

Observação. O resultado do Exercício 3 pode ser visto como caso particular do resultado do item (b) do Exercício 12, tendo em mente que a aplicação:

$$\phi : \mathrm{L}(V, V) \ni T \longmapsto [T]_{\mathcal{B}} \in M_n(K)$$

é um homomorfismo de anéis. O resultado dos itens (a) e (c) do Exercício 6 também podem ser vistos como caso particular do resultado do item (b) do Exercício 12, considerando-se os homomorfismos de anéis:

$$\mathbb{C} \ni z \longmapsto \bar{z} \in \mathbb{C}, \quad M_n(\mathbb{C}) \ni A \longmapsto \bar{A} \in M_n(\mathbb{C}).$$