Estruturas Algébricas II

Kalasas Vasconcelos de Araujo

São Cristóvão/SE
2009

Estruturas Algébricas II

Elaboração de Conteúdo
Kalasas Vasconcelos de Araujo

Capa
Hermeson Alves de Menezes

Ficha catalográfica produzida pela Biblioteca Central
Universidade Federal de Sergipe

A663e Araujo, Kalasas Vasconcelos de.
Estruturas Algébricas II / Kalasas Vasconcelos de Araujo.
-- São Cristóvão: Universidade Federal de Sergipe, CESAD, 2009.

1. Matemática. 2. Álgebra. I. Título.

CDU 512

UNIVERSIDADE FEDERAL DE SERGIPE
Cidade Universitária Prof. "José Aloísio de Campos"
Av. Marechal Rondon, s/n - Jardim Rosa Elze
CEP 49100-000 - São Cristóvão - SE
Fone(79) 2105 - 6600 - Fax(79) 2105- 6474

Sumário

AULA

Polinômios 1

META:

Apresentar polinômios em uma indeterminada sobre um anel.

OBJETIVOS:

Ao fim da aula os alunos deverão ser capazes de:

Definir polinômios em uma indeterminada sobre um anel.

Compatibilizar a estrutura do anel A com a de $A[x]$.

Efetuar as operações de soma e produto de polinômios.

Reconhecer o grau de um polinômio.

Reconhecer coeficientes, termos, termo líder, coeficiente líder, monômio líder e o termo constante de um polinômio.

PRÉ-REQUISITOS

Definição de anel, domínio de integridade e corpo.

1.1 Introdução

Prezado aluno, bem vindo ao curso estruturas algébricas II. Esta é nossa primeira aula e começarei fazendo-lhe a seguinte pergunta: você sabe a diferença entre as seguintes expressões?

a) $f(X) = X^2 + X + 1$, $X \in \mathbb{R}$.

b) $X \in \mathbb{R}$ tal que $X^2 + X + 1 = 0$.

c) $X^2 + X + 1$.

Até o momento, você deveria saber tratarem-se, respectivamente, de uma função polinomial, uma equação polinomial e um polinômio.

Para diferenciarmos um objeto de um outro se faz necessário sabermos a definição precisa de cada um deles. Neste caso, o que é uma função? O que é uma equação algébrica? O que é um polinômio?

À luz da teoria dos conjuntos, a diferença entre função e equação torna-se evidente. Os nomes variável e incógnita servem justamente para diferenciarmos o papel de x quando o mesmo representa o elemento genérico do domínio de uma função ou uma solução genérica de uma equação. Já o x figurando-se em um polinômio passa a ser chamado de *indeterminada*.

Nesta aula, definiremos polinômios via um certo tipo de sequências. Esta definição evita o uso de indeterminada e ressalta a importância da estrutura do anel dos coeficientes na estrutura de anel dos polinômios.

1.2 Polinômios

A definição de polinômio que trazes consigo certamente é como uma expressão formal do tipo

$$a_n x^n + \cdots + a_1 x^1 + a_0$$

em que $a_0, a_1, \ldots, a_n$ são números reais e $i \in \mathbb{Z}$ é um inteiro positivo para todo i, $0 \leq i \leq n$.

Mas, você sabe o que é uma *expressão formal*? Qual o significado do termo ax^n? Isto é um produto ou meramente uma aglutinação de letras? Os coeficientes a_i's devem necessariamente ser reais ou complexos? O que mudaria no conjunto dos polinômios se considerássemos seus coeficientes em $\mathbb{Q}$, em $\mathbb{Z}$ ou até mesmo em $\mathbb{Z}_n$? Até que ponto a estrutura algébrica dos coeficientes interfere na estrutura algébrica do conjunto de polinômios? E o x, o que realmente ele representa?

A definição a seguir tanto evita qualquer tipo de obstrução psicológica quanto resolve a crise existencial dos polinômios e do x enquanto indeterminada.

Definição 1.1. Seja A um anel. Um polinômio com coeficientes no anel A é uma sequência infinita de elementos em A escrita na forma

$$(a_0, a_1, a_2, \ldots)$$

na qual todos os a_i's são nulos exceto para uma quantidade finita de índices. Os elementos $a_0, a_1, a_2, \ldots$ são chamados coeficientes do polinômio.

Usaremos o símbolo $\mathcal{P}_A$ para denotar o conjunto de todos os polinômios definidos sobre um anel A. Dois polinômios $P = (a_0, a_1, a_2, \ldots)$ e $Q = (b_0, b_1, b_2, \ldots)$ em $\mathcal{P}_A$ são iguais se são iguais como sequências, isto é, $a_i = b_i$ para cada índice i.

A sequência nula $(0, 0, 0, \ldots)$ é um polinômio chamado *polinômio nulo* e denotado por 0. Se $P = (a_0, a_1, a_2, \ldots) \in \mathcal{P}_A$ é não nulo então existe $n \geq 0$ tal que $a_n \neq 0$ e $a_i = 0$ para todo $i > n$. Tal inteiro n é chamado *grau* de P e denotado por $deg\ P$. Em símbolos,

$$deg\ P := max\{i\ :\ a_i \neq 0\}, \qquad (P \neq 0).$$

OBS 1.1. O grau do polinômio nulo não está definido. No entanto, a convenção $deg\ (0, 0, 0, \ldots) = -\infty$ não põe abaixo nenhuma das propriedades requeridas para o grau de polinômios. Definiremos $\deg 0 = \infty$ para estendermos a noção de grau à todos polinômios. O uso deste símbolo requer certa maturidade matemática mas, para nossos propósitos, basta termos em mente que $-\infty + k = -\infty$ qualquer que seja $k \in \mathbb{Z}$.

1.3 A estrutura algébrica dos polinômios e o significado da expressão $a_n x^n + \ldots a_1 x + a_0$

Seja A um anel. Por definição de anel, estão definidas em A duas operações: a adição $(a, b) \mapsto a + b$ e a multiplicação $(a, b) \mapsto a.b$ em que $(a, b) \in A \times A$. Usaremos tais operações em A para induzir uma adição e uma multiplicação no conjunto dos polinômios $\mathcal{P}_A$.

Teorema 1.1. *As operações*
Adição:

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots)$$

onde $c_k = a_k + b_k$ para todo índice k.
Multiplicação:

$$(a_0, a_1, a_2, \ldots).(b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots)$$

onde $c_k = a_0 b_k + a_1 b_{k-1} + \cdots a_{k-1} b_1 + a_k b_0$ para todo índice k.

estão bem definidas em $\mathcal{P}_A$.

Prova: Devemos mostrar que $\mathcal{P}_A$ é fechado com respeito a tais operações. Sejam P e Q dois polinômios em $\mathcal{P}_A$. Se P ou Q é o polinômio nulo então $P+Q$ é P ou Q e $PQ=0$. Suponhamos então P e Q ambos não nulos de graus n e m, respectivamente. Se $k > max\{n,m\}$ então $a_k + b_k = 0$, por definição de grau. Com relação ao produto, se $k > n+m$ então $c_k = \sum_{i=0}^{i=k} a_i b_{k-i}$ é nulo. De fato, se $i > n$ então $a_i = 0$ donde $a_i b_{k-i} = 0$. Se $i \leq n$ então $-i \geq -n$. Deste modo, $k > n+m$ implica $k - i > n + m - i \geq n + m - n = m$ donde $a_i b_{k-i} = 0$ pois $b_{k-i} = 0$. Assim, $c_k = 0$ para todo $k > n+m$. $\square$

O propósito de definir tais operações em $\mathcal{P}_A$ é determinar uma estrutura de anel compatível com a estrutura do anel A de modo que A possa ser visto como subanel de $\mathcal{P}_A$.

Teorema 1.2. *A estrutua de anel em A induz uma estrutura de anel em $(\mathcal{P}_A, +, \bullet)$. Além disso, se A é comutativo e/ou com identidade então assim é $\mathcal{P}_A$.*

Prova: Com relação à adição devemos mostrar que $\mathcal{P}_A$ é um grupo abeliano. Mais precisamente,

G1 **Elemento neutro**: O polinômio nulo $\mathbf{0} = (0,0,0,\ldots)$ é tal que $\mathbf{O} + P = P + = P$ qualquer que seja $P \in \mathcal{P}_A$. Logo, $\mathbf{0}$ é o elemento neutro.

G2 **Inverso aditivo**: Se $P = (a_0, a_1, a_2, \ldots) \in \mathcal{P}_A$ então $-P = (-a_0, -a_1, -a_2, \ldots) \in \mathcal{P}_A$ é tal que $P + (-P) = \mathbf{0}$. Logo, todo polinômio admite inverso aditivo.

G3 **Associatividade**: Sejam $P_1 = (a_0, a_1, a_2, \ldots)$, $P_2 = (b_0, b_1, b_2, \ldots)$ e $P_3 = (c_0, c_1, c_2, \ldots)$ polinômios em $\mathcal{P}_A$.

Desde que

$$(a_i + b_i) + c_i = a_i + (b_i + c_i)$$

em A segue que $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$.

G4 **Comutatividade**: Analogamente, a comutatividade em $\mathcal{P}_A$ decorre diretamente da comutatividade em A.

Com relação à multiplicação:

M1 **Associatividade**: Sejam $A = (a_0, a_1, a_2, \ldots)$, $B = (b_0, b_1, b_2, \ldots)$ e $C = (c_0, c_1, c_2, \ldots)$ polinômios em $\mathcal{P}_A$. Por definição, a n-ésima coordenada do produto $(A.B).C$ é

$$\begin{aligned}
\sum_{i=0}^{n}(A.B)_i.c_{n-i} &= \sum_{i=0}^{n}\left[\sum_{j=0}^{i} a_j b_{i-j}\right] c_{n-i} \\
&= \sum_{i=0}^{n}\sum_{j=0}^{i} a_j b_{i-j} c_{n-i} \\
&= \sum_{u+v+w=n} a_u b_v c_w \quad (u, v, w \geq 0) \quad (*)
\end{aligned}$$

Por outro lado, a n-ésima coordenada do produto $A.(B.C)$ é

$$\begin{aligned}
\sum_{r=0}^{n} a_r (B.C) &= \sum_{r=0}^{n}\left[\sum_{s=0}^{n-r} c_s b_{n-r-s}\right] \\
&= \sum_{r=0}^{n}\sum_{s=0}^{n-r-s} a_r b_s c_{n-r-s} \\
&= \sum_{u+v+w=n} a_u b_v c_w \quad (u, v, w \geq 0) \quad (**)
\end{aligned}$$

Deste modo, $[(A.B).C]_n = [A.(B.C)]_n$ para todo índice n. Isto mostra a associatividade.

- **Distributividade** : Sejam $A, B, C \in \mathcal{P}_A$ como anteriormente. Então,

$$\begin{aligned}
[A.(B+C)]_n &= \sum_{i=0}^{n} a_i.(B+C)_{n-i} \\
&= \sum_{i=0}^{n} a_i.(b_{n-i}+c_{n-i}) \\
&= \sum_{i=0}^{n} a_i.b_{n-i} + a_i c_{n-i} \\
&= \sum_{i=0}^{n} a_i.b_{n-i} + \sum_{i=0}^{n} a_i.c_{n-i} \\
&= A.B + A.C
\end{aligned}$$

  Logo, $A.(B+C) = A.B + A.C$. Do mesmo modo, $(A+B).C = A.C + B.C$.

Isto mostra que $(\mathcal{P}_A, +, \bullet)$ é um anel. Se A tem identidade 1_A, então $(1_A, 0, 0, 0, \ldots) \in \mathcal{P}_A$ é a identidade de $\mathcal{P}_A$ (verifique!) e se A é comutativo então

$$[A.B]_n = \sum_{i=0}^{n} a_i.b_{n-i} = \sum_{i=0}^{n} b_{n-i}a_i = \sum_{i=0}^{n} b_j a_{n-j}.$$

Donde $A.B = B.A$. Isto conclui a demonstração. $\square$

O próximo passo é tornarmos A um subanel de $\mathcal{P}_A$. Lembramos que um subanel de um anel B é um subconjunto $A \subset B$ tal que A é um anel com as operações definidas em B. Se, além disso, B é anel com identidade então é exigido, adicionalmente, que $1_A \in B$. Um anel B é dito uma extensão de um anel A se A é subanel de B. Costuma-se denotar isto simplesmente por $A \subset B$.
Queremos tornar $\mathcal{P}_A$ uma extensão de A de modo que se $a, b \in A$ e P_a, P_b são os polinômios associados aos elementos a e b, respectivamente, então $P_{a+b} = P_a + P_b$ e $P_{ab} = P_a.P_b$. Lembra-se de

homomorfismos de anéis? Desejamos definir um homomorfismo de A em $\mathcal{P}_A$. Uma função $\phi : A \to \mathcal{P}_a$ tal que $\phi(a+b) = \phi(a) + \phi(b)$ e $\phi(a.b) = \phi(a).\phi(b)$. Além disso, se A é um anel comutativo com identidade devemos ter satisfeita a condição $\phi(1_A) = 1_{\mathcal{P}_A}$. Queremos também que Im $\phi \subset \mathcal{P}_A$ seja uma cópia de A. Isto se realiza exigindo-se que o homomorfismo ϕ seja injetivo. Deste modo, A será isomorfo ao anel Im $\phi \subset \mathcal{P}_A$ e então poderemos fazer a identificação $a = \phi(a) = P_a$. Em álgebra, tal procedimento é canônico quando se quer tornar um anel A subanel de outro anel B e não se tem $A \subset B$. Tudo isto resume-se por meio de um teorema.

Teorema 1.3. *Seja $\mathcal{P}_A$ o anel dos polinômios sobre um anel A. Se $A^* \subset \mathcal{P}_A$ é o conjunto de todos os polinômios da forma $(a, 0, 0, 0 \ldots)$, $a \in A$, então A^* é um subanel de $\mathcal{P}_A$ isomorfo à A.*

Prova: Defina a aplicação $\phi : A \to A^*$, $a \mapsto \phi(a) = P_a = (a, 0, 0, 0, \ldots)$. Você mesmo, prezado aluno, pode verificar que ϕ é bijetiva (Faça isto!). Além disso,

$$\phi(a+b) = (a+b, 0, 0, 0, \ldots) = (a, 0, 0, 0, \ldots)+(b, 0, 0, 0, \ldots) = \phi(a)+\phi(b)$$

e

$$\phi(a.b) = (a.b, 0, 0, 0, \ldots) = (a, 0, 0, 0, \ldots).(b, 0, 0, 0, \ldots) = \phi(a).\phi(b).$$

Finalmente, $\phi(1_A) = (1_A, 0, 0, 0, \ldots) = 1_{\mathcal{P}_A}$. Assim, ϕ é um isomorfismo de anéis e caso A tenha identidade, ϕ é um isomorfismo de anéis com identidade. $\square$

Até o momento, estabelecemos os fatos básicos sobre polinômios. Agora, precisamos achar um jeito de exibir um polinômio em sua forma usual. Denotaremos por x ao polinômio $(0, 1, 0, 0, 0, \ldots)$. De acordo com o teorema acima, podemos fazer a identificação

$a := (a, 0, 0, 0, \ldots)$ para cada $a \in A$ e obtermos a inclusão de anéis $A \subset \mathcal{P}_A$. Deste modo, ao escrevermos a estaremos pensando no polinômio $(a, 0, 0, 0, \ldots)$. Com isto em mente vamos analisar as potências x^n de x e os produtos ax^n.
Por definição de potência:

$$\begin{aligned} x^0 = 1_{\mathcal{P}_A} &= (1_A, 0, 0, 0, \ldots) \\ x^1 = x &= (0, 1, 0, 0, 0, \ldots) \\ x^2 = x \cdot x &= (0, 0, 1, 0, 0, 0, \ldots) \end{aligned}$$

e $x^n = x^{n-1} \cdot x$. Supondo $x^{n-1} = (0, \ldots, 0, 1, 0, \ldots)$ com 1 na entrada de índice $n-1$ (hipótese indutiva!) obtemos

$$x^n = x^{n-1} \cdot x = (0, \ldots, 0, 1, 0, \ldots)$$

com 1 na posição de índice n. Logo, por indução segue que

$$X^n = (a_0, a_1, a_2, \ldots, a_n, \ldots)$$

em que $a_n = 1$ e $a_i = 0$ para todo $i \neq n$. Temos ainda

$$\begin{aligned} ax^n &= (a, 0, 0, 0, \ldots) \cdot (a_0, a_1, a_2, \ldots) \\ &= (aa_0, aa_1, aa_2, \ldots, aa_n \ldots) \\ &= (0, 0, 0 \ldots, 0, a, 0, \ldots) \end{aligned}$$

pois $a_n = 1$ e $a_i = 0$ para todo $i \neq n$. Assim, dado um polinômio $(a_0, a_1, a_2, \ldots)$ de grau n em $\mathcal{P}_A$ podemos escrever

$$\begin{aligned} (a_0, a_1, a_2, \ldots) &= (a_0, 0, 0, \ldots) + (0, a_1, 0, \ldots) + \\ &\quad + \cdots + (0, \ldots, 0, a_n, 0, \ldots) \\ &= a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \end{aligned}$$

Pela definição de igualdade de polinômios temos ainda que se $b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ é uma outra forma de expressar o polinômio $(a_0, a_1, a_2, \ldots)$ então $m = n$ e $a_i = b_i$ para todo índice i. Logo, todo polinômio $(a_0, a_1, a_2, \ldots) \in \mathcal{P}_A$ com grau n se escreve, de maneira única, na forma

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n.$$

OBS 1.2. Nesta forma de expressão para polinômios usamos a notação $A[x]$ em vez de $\mathcal{P}_A$. A notação $A[x]$ é muito mais sugestiva. Por exemplo, se $A = \mathbb{R}$ então podemos ver $A[x]$ como um espaço vetorial sobre $\mathbb{R}$ (você saberia exibir uma base e dizer qual a sua dimensão?). Outra vantagem é que na notação $A[x]$, as operações com polinômios recaem naquelas vistas no ensino médio e fundamental. Nesta notação, costuma-se denotar polinômios pelas letras do alfabeto latino acrescidas de x entre parêntese, isto é, $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = p(x)$, por exemplo.

OBS 1.3. Um elemento ξ é chamado de indeterminada sobre um anel A se as expressões

$$a_0 + a_1\xi + a_2\xi^2 + \cdots + a_n\xi^n$$

estão definidas para todo inteiro não negativo n e a aplicação

$$\varphi : A[x] \to A[\xi]$$

definida por

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mapsto a_0 + a_1\xi + a_2\xi^2 + \cdots + a_n\xi^n$$

define um isomorfismo de anéis.

1.4 Termos e Monômios

Seja A um anel com identidade. Um polinômio da forma ax^n é chamado *termo*. Um termo com coefiente 1 é denominado monômio

ou monomial. Dado um polinômio de grau n

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

define-se:

		Notação
Coeficientes:	$a_0,\ a_1,\ \ldots a_n$	
Termos:	$a_0,\ a_1x,\ \ldots a_nx^n$	
Termo líder:	a_nx^n	LT (f)
Monômio líder:	x^n	LM (f)
Coeficiente líder:	a_n	LC (f)
Termo constante:	a_0	

OBS 1.4. Um polinômio é dito mônico se possui termo líder monomial.

OBS 1.5. Em alguns textos, o adjetivo *líder* é trocado por *dominante* e as definições acima ficam: termo dominante, coeficiente dominante e monômio dominante. Neste texto, usaremos líder em conformidade com uma notação mais universal.

1.5 Conclusão

Na aula de hoje, elaboramos uma definição de polinômios que evita qualquer tipo de expressões vagas e torna clara a noção de indeterminada. Vimos duas representações de um polinômio: por meio de sequências e por meio de uma indeterminada x. A segunda é mais apelativa e preferível perante a primeira. Por exemplo, a estrutura de espaço vetorial de $\mathbb{R}[x]$ sobre $\mathbb{R}$ com base infinita $1,\ x,\ x^2, \ldots$, torna-se muito mais evidente usando indeterminada.

RESUMO

Seja A um anel qualquer (não necessariamente comutativo com identidade).

Definições básicas

Polinômio sobre $A :=$ sequência infinita $(a_0, a_1, a_2, \ldots)$ com $a_i \in A$ na qual todos os elementos a_i^s são nulos exceto para um número finito de termos. Os elementos a_i's são chamados coeficientes do polinômio $(a_0, a_1, a_2, \ldots)$.

$\mathcal{P}_A :=$ conjunto dos polinômios com coeficientes em A.

$(0, 0, 0, \ldots) \in \mathcal{P}_A$ é chamado polinômio nulo.

Grau de Polinômios

$$\deg P = \begin{cases} -\infty, \text{ se } P = 0 \\ n = \max\{n \ : \ a_n \neq 0\}, \text{ se} P \neq 0 \end{cases}$$

Operações em $A[x]$:

Adição:

$(\ldots, a_i, \ldots) + (\ldots, b_i, \ldots) = (\ldots, a_i + b_i, \ldots)$

Multiplicação:

$(\ldots, a_i, \ldots) \cdot (\ldots, b_i, \ldots) = (\ldots, c_i, \ldots)$

onde $c_i = \sum_{j+k=i} a_j b_k$.

Estrutura algébrica: $(\mathcal{P}_A, +, \cdot)$ é um anel.

Quadro comparativo entre a estrutura do anel A e a estrutura do anel $A[x]$

A	$A[x]$
Comutativo	Sim
Com identidade	Sim
Domínio	Sim
Corpo	Não

A Aplicação

$$\begin{aligned} \phi : A &\rightarrow A[x] \\ a &\mapsto (a, 0, 0, 0 \ldots) \end{aligned}$$

define um isomorfismo de A no subconjunto

$$A^* = \{(a, 0, 0, 0, \ldots) : a \in A\} \subset \mathcal{P}_A.$$

Os elementos de A^* são chamados *polinômios constantes* ou de grau zero. (O termo *constante* refere-se ao fato da função associada aos polinômios em A^* serem constantes.

O significado da expressão $a_0 + a_1x + \ldots + a_nx^n$:

Fazendo as identificações:

$$a := (a, 0, 0, 0, \ldots)$$

$$x := (0, 1, 0, 0, 0, \ldots)$$

Pode-se mostrar que

$$x^n = (0, 0, \ldots, 0, 1, 0, \ldots)$$

com deg $x^n = n$. E

$$ax^n = (0, 0, \ldots, 0, a, 0, \ldots)$$

também de grau n. Nestas condições, todo polinômio

$$(a_0, a_1, a_2, \ldots) \in \mathcal{P}_A$$

de grau n pode ser escrito de maneira única na forma:

$$a_0 + a_1x + \ldots a_nx^n.$$

Notação: $A[x] := \{p(x) = a_0 + a_1x + \ldots a_nx^n : a_i \in A\}$.

A composição de um polinômio

Dado

$$a_0 + a_1x + \ldots a_nx^n \in \mathcal{P}_A$$

defini-se

		Notação
Coeficientes:	a_0, a_1, $\ldots a_n$	
Termos:	a_0, a_1x, $\ldots a_nx^n$	
Termo líder:	a_nx^n	LT (f)
Monômio líder:	x^n	LM (f)
Coeficiente líder:	a_n	LC (f)
Termo constante:	a_0	

PRÓXIMA AULA

Na próxima aula, restringiremos nosso estudo de polinômios para polinômios definidos sobre um corpo. O fato do anel de coeficientes ser um corpo permite definir um algoritmo de divisão no anel de polinômios. Tal algoritmo é o pilar da aritmética dos anéis de polinômios definidos sobre corpos.

ATIVIDADES

ATIV. 1.1. Nos itens abaixo são dados polinômios representados por sequência e pelo uso de indeterminada. Faça a transposição de uma representação para a outra. Em cada caso, determine o grau e o termo líder usando as notações dadas no texto.

a) $(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, \ldots)$.

b) $(0, 2, 0, 4, 0, 6, 0, 8, 0, 0, 0, \ldots)$

c) $9x^8 - 3x^5 + x^3 - x + 4$.

d) $(3x - 7)(x^3 - x + 1)$.

ATIV. 1.2. Efetue a operação indicada e simplifique sua resposta. Em cada caso, determine o grau e o termo líder usando as notações usadas no texto.

a) $(x + 2)^3$ em $\mathbb{Z}_3[x]$.

b) $(x + 1)^5$ em $\mathbb{Z}_5[x]$.

c) $(ax + b)^p$ em $\mathbb{Z}_p[x]$, p primo.

d) $(x^2 - 3x + 2)(2x^3 - 4x + 1)$ em $\mathbb{Z}_7[x]$

Sugestão: Nos itens de (a), (b) e (c) use a expansão do binômio de Newton. Note que $(a+b)^p = a^p + b^p$ em $\mathbb{Z}_p$. No item (d) aplique a propriedade distributiva.

ATIV. 1.3. Quais dos seguintes subconjuntos de $A[x]$ são subanéis de $A[x]$?

a) Polinômios com termo constante nulo.

b) $B = \{a_0 + a_1x + \cdots + a_nx^n \ : \ a_i = 0$, para i ímpar $\}$.

c) $B = \{a_0 + a_1x + \cdots + a_nx^n \ : \ a_i = 0$ sempre que i for par $\}$

ATIV. 1.4. Mostre que se A é um domínio de integridade então $A[x]$ é um dominio de integridade. Se k é um corpo então $k[x]$ também é um corpo?

Sugestão: Para a primeira parte, suponha $A[x]$ não domínio e mostre que A necessariamente não é domínio. Para a segunda, mostre que x não admite inverso multiplicativo em $A[x]$, isto é, a igualdade $g(x).x = 1$ para $g(x) \in A[x]$ conduz à uma contradição.

ATIV. 1.5. Considere a aplicação $\varphi : A \to A[x]$ definida por $\varphi(a) = (0, a, 0, 0, 0 \ldots)$. Tal aplicação é um homomorfismo de anéis?

Sugestão: Repare se a igualdade $\varphi(a.b) = \varphi(a).\varphi(b)$ é ou não satisfeita.

ATIV. 1.6. Mostre que o grau de polinômios satisfaz às seguintes propriedades:

i) $\deg\, p(x) + q(x) \leq \max\, \{\, \deg\, f(x), \deg\, q(x)\}$

ii) $\deg\, p(x)q(x) = \deg\, p(x) + \deg\, q(x)$, se A é domínio.

iii) Dê um exemplo com desigualdade estrita no item (i) e caracterize quando ocorre tal desigualdade.

LEITURA COMPLEMENTAR

GONÇALVES, Adilson, Introdução à álgebra, IMPA, Projeto Euclides, 5.ed., Rio de Janeiro, 2008.

HUNGERFORD, Thomas W., Abstract algebra: an introduction, Saunders College Publishing, 1990.

KAPLANSKY, I., Introdução à teoria de Galois, Notas de Matemática nº 13, IMPA, 1966.