Universidade Estadual de Maringá
Centro de Ciências Exatas
Departamento de Matemática
XXIV Semana da Matemática
05 à 09-08-2013

O "x"da Questão do Polinômios

Autor: Laerte Bemm

Maringá - PR
2013

Sumário

Introdução

Na maior parte dos textos de Álgebra, o conceito de polinômio é definido invariavelmente como uma expressão formal do tipo

$$a_0 + a_1 \cdot x + a_2 \cdot x^2 + \cdots + a_n \cdot x^n \tag{1}$$

onde cada a_i, $i = 1, 2, \cdots n$ é um elemento de algum anel A.

No entanto, com um olhar mais atento e crítico percebemos que uma tal expressão envolve operações entre elementos deste anel e um objeto, a priore, não definido: o símbolo x. Quem é este símbolo não identificado? Qual é a natureza de x? É um elemento do anel de coeficientes A? Vejamos:

Observe que o papel de x em (1) é o mesmo de π na expressão

$$2 - 3 \cdot \pi + 7 \cdot \pi^2 - 5 \cdot \pi^3,$$

onde os coeficientes $2, -3, 7$ e -5 das potências de π estão em $\mathbb{Z}$. Mas tal expressão não tem sentido em $\mathbb{Z}$. Portanto, não é correto dizer que x representa, necessariamente, um elemento do anel de coeficientes.

Seria x um vetor e o termo $a_1 \cdot x$ o produto por escalar de um espaço vetorial? Observe que isto gera um incômodo, uma vez que aparecem as potências de x na expressão (1) e produto de vetores não está definido em espaços vetoriais. Isso descarta a natureza vetorial do objeto x.

O que a expressão (1) sugere é a existência de uma estrutura algébrica "maior"que contém os coeficientes a_i e um objeto especial não pertencente ao anel de coeficientes. Definir polinômio como uma expressão formal, isto é, sem valor prático, de natureza

abstrata, deixa nosso conhecimento matemático com um pequeno vazio, algo que certamente perturba as mentes dos estudantes mais exigentes.

O objetivo deste trabalho é introduzir uma definição precisa do conceito de polinômios com coeficientes num anel e responder a pergunta: quem é o x da questão dos polinômio? Também definiremos uma adição e uma multiplicação no conjunto $A[x]$, formado por todos dos polinômios com coeficientes em anel A e mostraremos que tal conjunto é um anel. Finalmente, provaremos que se A é um corpo, então vale o Algoritmo da Divisão de Euclides em $A[x]$ e mostraremos a crucial diferença entre polinômios e funções polinomiais. Iremos mostrar que tais conceitos são totalmente distintos. Finalizamos o trabalho apresentando algumas aplicações deste algoritmo para a obtenção de resultados realmente curiosos sobre polinômios.

Capítulo 1

Anéis e Domínios

1.1 Definições e Exemplos

No primeiro capítulo, vamos introduzir alguns conceitos e resultados que serão necessários para o desenvolvimento do próximo capítulo, que é o enfoque principal deste mini-curso. O leitor que já cursou um curso básico de estruturas algébricas pode avançar este capítulo.

Começamos esta seção definindo o conceito de anel.

Definição 1.1 *Um anel é um conjunto não vazio A munido com duas operações internas denotadas por $+$ (chamada adição) e $\cdot$ (chamada multiplicação) que satisfazem as seguintes condições para quaisquer $a, b, c \in A$:*

(A.1) A adição é associativa, i.é, $(a + b) + c = a + (b + c)$;

(A.2) A adição é comutativa, i.é, $a + b = b + a$;

(A.3) Existe um elemento neutro da adição, i.é, existe um elemento em A, denotado por 0_A, tal que $0_A + a = a + 0_A = a$, para todo $a \in A$;

(A.4) Todo elemento de A possui um simétrico com respeito a adição, i.é, para todo $a \in A$, existe um elemento em $a' \in A$ tal que $a + a' = a' + a = 0_A$;

(M.1) A multiplicação é associativa, i.é, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*;*

(M.2) A multiplicação é distributiva em relação a adição, i.é, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ *e* $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$*;*

Quando um conjunto A é um anel, dizemos também que A possui ou admite uma estrutura algébrica de anel.

Muitas vezes a palavra **produto** é usada para disignar a operação de multiplicação, assim como a palavra **soma** é usada para disigar a operação de adição. Isto não é correto. A adição e a multiplicação são as operações internas de um conjunto. O resultado da adição de dois elementos é chamado *soma*, enquanto que o resultado da mulplicação de dois elementos é chamado de *produto*.

A condição (A.3) da definição anterior, garante a existência de **um** elemento neutro da adição. Se 0_A e $0'_A$ forem dois elementos neutros da adição de um anel A, então, em particular, $0_A = 0_A + 0'_A = 0'_A$. Isto mostra que o elemento neutro da adição é único num anel. Tal elemento é chamado *zero* do anel A e sempre que não houver possibilidade de confusão, ele será denotado simplesmente por 0.

A condição $(A.4)$ da Definição 1.1 garante que todo elemento a de um anel A admite **pelo menos um** elemento simétrico em relação a adição. Suponha que $a' \in A$ e $a'' \in A$ sejam simétricos de $a \in A$ em relação a adição. Temos:

$$\begin{aligned} a' &= a' + 0 && \text{por } (A.3) \\ &= a' + (a + a'') && \text{pois } a'' \text{ é simétrico de } a \\ &= (a' + a) + a'' && \text{por } (A.1) \\ &= 0 + a'' && \text{pois } a' \text{ é o simétrico de } a \\ &= a'' && \text{por } (A.3). \end{aligned}$$

Isto significa que o simétrico a' de a em relação a adição é único e será denotado por $-a$. Assim, $a + (-a) = (-a) + a = 0_A$.

Antes de darmos exemplos, vamos definir mais alguns conceitos importantes.

Se a multiplicação $\cdot$ em um anel A for comutativa, i.é, se $a \cdot b = b \cdot a$, para quaisquer $a, b \in A$, diremos que A é um *anel comutativo*.

Pode acontecer algumas vezes, as vezes não, de existir um elemento u num anel A tal que $a \cdot u = u \cdot a = a$ para todo $a \in A$. Quando isso acontece, diremos que o anel A é um *anel com unidade*. Em outras palavras, um anel com unidade é um anel que possui um elemento neutro para a multiplicação. De maneira análoga ao que foi feito para o elemento neutro da adição, mostra-se que, quando existe, o elemento neutro da multiplicação de um anel é único e será denotado por 1_A (ou simplesmente 1 quando não houver possibilidade de confusão). Tal elemento é chamado a *unidade* de A.

NOTAÇÃO: Se A é um anel com operação de multiplicação $\cdot$ e $a, b \in A$, escreveremos muitas vezes ab no lugar de $a \cdot b$.

Sejam A um anel e $a, b \in A$. Como $-b \in A$, definimos $a - b$ por $a - b = a + (-b)$. Isto induz uma nova operação sobre A, chamada *subtração* e denotada por $-$. O resultado da subtração de dois elementos é chamada de *diferença*. Também, se n é um número inteiro positivo, definimos a^n como sendo $a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n \ \ vezes}$. Quando A tem unidade 1, definimos $a^0 = 1$.

Vamos dar uma pequena pausa nas definições para darmos alguns exemplos. Eles nos motivarão a definir outros tipos de aneis "especiais".

Exemplo 1.2 *O conjunto dos números inteiros $\mathbb{Z}$ é um anel comutativo com unidade com a adição $+$ e multiplicação $\cdot$ usuais.*

Exemplo 1.3 *O conjunto dos números inteiros pares, denotado por $2\mathbb{Z}$, é um anel comutativo com a adição $+$ e multiplicação $\cdot$ usuais. Porém, $2\mathbb{Z}$ não é um anel com unidade.*

Exemplo 1.4 *O conjunto dos números naturais com a adição e multiplicação usuais $\mathbb{N}$* ***não é um anel*** *pois em geral a propriedade $(A.4)$ da Definição 1.1 não é válida. De fato, todo número natural não nulo não possui um simétrico com respeito a adição.*

Exemplo 1.5 *O conjunto dos números racionais $\mathbb{Q}$, bem como o conjunto dos números reais $\mathbb{R}$ com as operações usuais de adição e multiplicação são anéis comutativos com unidade.*

Exemplo 1.6 *Considere o conjunto $M_2(\mathbb{R})$ de todas as matrizes 2×2 com entradas reais, i.é,*

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} : a_{11}, a_{12}, a_{21}, a_{22} \in \mathbb{R} \right\}.$$

Definimos a adição e multiplicação de duas matrizes $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ *e* $\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ *pertencentes a* $M_2(\mathbb{R})$ *da seguinte forma:*

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \oplus \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

e

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \odot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

Fica como exercício para o leitor provar que as operações de adição $\oplus$ *e multiplicação* $\odot$ *definidas acima dão ao conjunto* $M_2(\mathbb{R})$ *uma estrutura de anel com unidade. Observe que o elemento neutro da adição é a matriz* $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$*, chamada matriz nula, e a matriz* $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *é a unidade de* $M_2(\mathbb{R})$*, chamada matriz identidade.*

Considere agora as matrizes $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ *e* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *de* $M_2(\mathbb{R})$*. Temos:*

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \odot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$$

e

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \odot \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

Portanto, $M_2(\mathbb{R})$ *com as operações* $\oplus$ *e* $\odot$ *definidas acima é um anel com unidade, mas não é comutativo. Fica como exercício generalizar o exemplo anterior para o conjunto* $M_n(\mathbb{R})$ *de todas as matrizes* $n \times n$ *com entradas reais.*

Exemplo 1.7 *Considere o conjunto* $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \,|\, a, b \in \mathbb{Z}\}$*. Para quaisquer elementos* $a + b\sqrt{3}, c + d\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ *definimos:*

(1) $(a+b\sqrt{3}) \oplus (c+d\sqrt{3}) = (a+c)+(b+d)\sqrt{3}$

(2) $(a+b\sqrt{3}) \odot (c+d\sqrt{3}) = (ac+3bd)+(ad+bc)\sqrt{3}$

Não é difícil (é apenas trabalhoso) mostrar que o conjunto $\mathbb{Z}[\sqrt{3}]$ *munido com as operações de adição* $\oplus$ *e multiplicação* $\odot$ *definidas acima é um anel comutativo com unidade. O zero deste anel é o elemento* $0+0\sqrt{3}$*, enquanto que a unidade é o elemento* $1+0\sqrt{3}$*.*

O leitor pode se inspirar no que acabamos de fazer para mostrar que para qualquer número inteiro m, o conjunto $\mathbb{Z}[\sqrt{m}]$ admite uma estrutura algébrica de anel comutativo com unidade. A adição e uma multiplicação em $\mathbb{Z}[\sqrt{m}]$ são definidas de maneira análoga ao que foi feito acima.

Observe que em $\mathbb{Z}$, $2\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{Z}[\sqrt{3}]$ apresentados acima, a multiplicação de quaisquer dois elementos não nulos é sempre um elemento não nulo. O mesmo não ocorre com $M_2(\mathbb{R})$, pois

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \odot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Para destacar a diferença entre tais anéis, temos a seguinte definição.

Definição 1.8 *Um anel comutativo com unidade* A *é dito ser um domínio de integridade ou domínio (simplesmente) se vale a seguinte sentença:*

$$\forall a, b \in A, \text{ se } a \neq 0 \text{ e } b \neq 0 \text{ então } a \cdot b \neq 0.$$

Logicamente, isto é equivalente a dizer que se a *e* b *são elementos de* A *tais que* $a \cdot b = 0$ *então* $a = 0$ *ou* $b = 0$*.*

Conforme vimos antes, os anéis $\mathbb{Z}$, $2\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{Z}[\sqrt{3}]$ são domínos de integridade enquanto que $M_2(\mathbb{R})$ não é domínio de integridade. Veremos adiante mais exemplos de anéis que não são domínios de integridade.

Note que se $x \neq 0$ é um elemento em um domínio de integridade D e $y, z \in D$, então

$$x \cdot y = x \cdot z \Longrightarrow y = z \text{ (verifique!)}$$

Tal propriedade é chamada *lei do corte à esquerda*. Analogamente temos a *lei do corte à direita*.

Exemplo 1.9 *Os conjuntos dos números racionais $\mathbb{Q}$ e dos números reais $\mathbb{R}$ são anéis comutativos com unidade com as operações de usuais de adição e multiplicação. Note que além disso, todo número racional (real) não nulo admite um inverso multiplicativo, i.é, para todo $x \in \mathbb{Q} - \{0\}$, $(x \in \mathbb{R} - \{0\})$ existe $y \in \mathbb{Q}$ $(y \in \mathbb{R})$ tal que $xy = 1$. Anéis que satizfazem esta última propriedade recebem um nome especial.*

Definição 1.10 *Um anel com unidade (não necessariamente comutativo) A é dito ser um anel com divisão se todo elemento não nulo de A admite um inverso multiplicativo, i.é, para todo $x \in A - \{0\}$, existe $y \in A$ tal que $x \cdot y = 1_A$.*

Pode-se mostrar que num anel com divisão A o inverso multiplicativo de $0 \neq x \in A$ é único. Tal elemento é denotado por x^{-1}.

Um anel com divisão e comutativo é chamado de *corpo*. Em outras palavras, um corpo é um anel comutativo com unidade cujos elementos não nulos admitem um inverso multiplicativo.

Os anéis $\mathbb{Q}$ e $\mathbb{R}$ são corpos. O conjunto dos números complexos

$$\mathbb{C} = \{a + bi \,:\, a, b \in \mathbb{R}\}$$

com adição e multiplicação usuais é um corpo. O inverso de um elemento não nulo $a+bi$ é o número complexo $\dfrac{a}{a^2+b^2} - \dfrac{b}{a^2+b^2}i$.

Outros corpos muito importante na matemática são construídos da seguinte forma: considere o conjunto $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} \,|\, a, b \in \mathbb{Q}\}$, onde p é um número inteiro primo. Para quaisquer elementos $a + b\sqrt{p}, c + d\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$ definimos:

(1) $(a + b\sqrt{p}) \oplus (c + d\sqrt{p}) = (a + c) + (b + d)\sqrt{p}$

(2) $(a + b\sqrt{p}) \odot (c + d\sqrt{p}) = (ac + pbd) + (ad + bc)\sqrt{p}$

O conjunto $\mathbb{Q}[\sqrt{p}]$ com as operações acima é um corpo. O inverso de $a + b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$ é o elemento $\dfrac{a}{a^2 - pb^2} - \dfrac{b}{a^2 - pb^2}\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$

1.2 Subanéis e Homomorfismos

Esta será uma breve seção para introduzirmos dois conceitos que necessitamos, mas que serão mencinados minimamente no próximo capítulo. Para maiores detalhes, o leitor poderá procurar em **??**.

Sejam A um anel com adição $+$ e multiplicação $\cdot$ e B um subconjunto não vazio de A. Se B com estas operações for um anel, diremos que B é um subanel de A.

Vamos agora dar um critério para decidir se um subconjunto de um anel é ou não um subanel.

Proposição 1.11 *Sejam A um anel com adição $+$ e multiplicação $\cdot$ e B um subconjunto de A. Então, B é um subanel de A se e somente se as seguintes condições são verificadas:*

(i) $0 \in B$;

(ii) $x, y \in B \Longrightarrow x - y \in B$;

(iii) $x, y \in B \Longrightarrow x \cdot y \in B$.

A demonstração é relativamente fácil e por isso será deixada a cargo do leitor.

Vamos usar a notação $B \leq A$ para indicar que B é um subanel de A.

Exemplo 1.12 *Conforme vimos na seção anterior temos os seguintes exemplos:*

(i) $2\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{R} \leq \mathbb{C}$;

(ii) $\mathbb{Z} \leq \mathbb{Z}[\sqrt{p}] \leq \mathbb{Q}[\sqrt{p}] \leq \mathbb{R}$.

Sejam A e B dois anéis. Por comodidade vamso denotar as oprerações destes dois anéis por $+$ e $\cdot$ simplesmente. Uma função $f : A \longrightarrow B$ é dita ser um *homomorfismo* de A em B se F satisfaz as seguintes condições:

(i) $f(x + y) = f(x) + f(y), \ \forall\, x, y \in A$;

(ii) $f(x \cdot y) = f(x) \cdot f(y), \ \forall\, x, y \in A$.

Quando um homomorfismo f de um anel A em um anel B é injetor (resp. sobrejetor), diremos que f é um *monomorfismo* (resp. *epimorfismo*). Quando f é um monomorfismo, podemos "identificar"cada elemento $a \in A$ com $f(a) \in B$ e, usando um abuso de linguagem, podemos considerar A contido em B. Se f é um homomorfismo bijetor (ou seja, inversível), diremos que f é um *isomorfismo*.

1.3 O Anel $\mathbb{Z}_m$

Fixe um número inteiro m e considere a relação R definida sobre $\mathbb{Z}$ da seginte maneira:

$$\begin{aligned} \forall\, a, b \in \mathbb{Z}, aRb &\iff m|a-b \\ &\iff a-b \text{ é múltiplo de } m \\ &\iff a-b = km, \text{ para algum } k \in \mathbb{Z} \\ &\iff a = km+b, \text{ para algum } k \in \mathbb{Z}. \end{aligned}$$

Não é muito difícil de mostrar que R é uma relação de equivalência. Assim, temos as classes de equivalência módulo R. Se $n \in \mathbb{Z}$, sua classe de equivalência módulo R, denotada por $\bar{n}$, é dada por

$$\bar{n} = \{a \in \mathbb{Z} \,|\, aRn\} = \{a \in \mathbb{Z} \,|\, a = km+n, k \in \mathbb{Z}\} = \{km+n \,|\, k \in \mathbb{Z}\}.$$

Em outras palavras, $\bar{n}$ é o conjunto de todos os números inteiros a cujo resto da divisão de a por m é n. Disso resulta que as únicas classes de equivalência módulo R são:

$\bar{0} = \{a \in \mathbb{Z} \,|\, aR0\} = \{a \in \mathbb{Z} \,|\, a = km, k \in \mathbb{Z}\} = \{km \,|\, k \in \mathbb{Z}\}.$

$\bar{1} = \{a \in \mathbb{Z} \,|\, aR1\} = \{a \in \mathbb{Z} \,|\, a = km+1, k \in \mathbb{Z}\} = \{km+1 \,|\, k \in \mathbb{Z}\}.$

$\bar{2} = \{a \in \mathbb{Z} \,|\, aR2\} = \{a \in \mathbb{Z} \,|\, a = km+2, k \in \mathbb{Z}\} = \{km+2 \,|\, k \in \mathbb{Z}\}.$

$\vdots$

$\overline{m-1} = \{a \in \mathbb{Z} \,|\, aR(m-1)\} = \{a \in \mathbb{Z} \,|\, a = km+(m-1), k \in \mathbb{Z}\} = \{km+(m-1) \,|\, k \in \mathbb{Z}\}$

O conjunto quociente de $\mathbb{Z}$ por R é o conjunto de todas as classes de equivalência módulo R. Tal conjunto é denotado por $\mathbb{Z}_m$. Simbolicamente, $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}$.

Em $\mathbb{Z}_m$ podemos definir uma operação interna de adição $\oplus$ e uma operação interna de multiplicação $\odot$ da seguinte forma:

(1) $\forall\ \bar{i}, \bar{j} \in \mathbb{Z}_m$, $\bar{i} \oplus \bar{j} = \overline{i+j} = \bar{k}$, onde k é o resto da divisão de $i + j$ por m.

(2) $\forall\ \bar{i}, \bar{j} \in \mathbb{Z}_m$, $\bar{i} \odot \bar{j} = \overline{i \cdot j} = \bar{k}$, onde k é o resto da divisão de $i \cdot j$ por m.

Um bom exercício é mostrar que estas operações estão bem definidas e que $\mathbb{Z}_m$ com tais operações é um anel comutativo com unidade.

Para facilitar a escrita, de agora em diante escreveremos simplesmente $\bar{i} + \bar{j}$ no lugar de $\bar{i} \oplus \bar{j}$ e $\bar{i}\ \cdot \bar{j}$ no lugar de $\bar{i} \odot \bar{j}$.

Observamos que para $m \in \mathbb{Z}$ fixado, $\mathbb{Z}_m$ é um anel finito que tem exatamente m elementos. O Z_6, por exemplo, tem 6 elementos. São eles: $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$ e $\bar{5}$. Observe que neste caso, $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$. Isto mostra que $\mathbb{Z}_6$ não um domínio de integridade e portanto não é um corpo. Deixamos para o leitor mostrar que Z_m é um corpo se e somente se m é um número primo.

Embora pareça que estes anéis estejam muito distantes da nossa vida cotidiana, um olhar um pouco mais crítico nos leva a conclusão do contrário. De fato, imagine um enfermeira que começa seu turno as 8 horas da noite, ou melhor, as 20 horas e que tem uma jornada de trabalho de 6 horas. Que horas esta enfermeira para de trabalhar? As 26 horas, ou as 2 horas? A resposta certa é 2 horas (da madrugada se preferir). Isto ocorre porque um dia tem 24 horas. As horas terrestres são: a hora 0, a hora 1, a hora 2, $\cdots$, a hora 23. Assim sendo, nenhum relógico digital do mundo é capaz de contar a hora 24. Portanto, a grosso modo, podemos pensar que as horas do dia terrestre funcionam mais ou menos como o $\mathbb{Z}_{24}$.

Capítulo 2

Polinômios em uma Indeterminada

2.1 Introdução

Neste capítulo vamos introduzir uma definição precisa do conceito de polinômios em uma indeterminada com coeficientes em um anel e responder a pergunta: quem é o x da questão dos polinômio? Também definiremos uma adição e uma multiplicação no conjunto $A[x]$, formado por todos dos polinômios com coeficientes em anel A, e mostraremos que tal conjunto é um anel. Finalmente, provaremos que se A é um corpo, então vale o Algoritmo da Divisão de Euclides em $A[x]$ e mostraremos a crucial diferença entre polinômios e funções polinomiais. Finalizamos o capítulo dando algumas aplicações do Algoritmo da Divisão de Euclides.

2.2 Sequências e Polinômios

Seja A um conjunto qualquer. Uma *sequência* em A é uma função $a : \mathbb{N} \longrightarrow A$, ou seja, uma sequência nada mais é do que um função a cujo domínio é $\mathbb{N}$ e o contra-domínio é A. Afim de simplificarmos a notação, para todo $n \in \mathbb{N}$, denotaremos a imagem de n pela

função a por a_n e não por $a(n)$ como estamos acostumados. É comum representarmos uma sequência em A por $(a_n)_{n\in\mathbb{N}}$, ou simplesmente (a_n), ou ainda $(a_0, a_1, a_2, a_3, \cdots)$. Numa sequência $(a_0, a_1, a_2, a_3, \cdots)$, cada termo a_i é chamado de *coeficiente*. O índice i indica a posição do coeficiente na sequência.

Seja $\mathbb{A}$ um anel com elemento neutro da adição 0. Dada uma sequência $p = (a_n)_{n\in\mathbb{N}}$ em A, definimos o *suporte* de a como sendo o seguinte conjunto:

$$sup(p) = \{i \in \mathbb{N} \,:\, a_i \neq 0\}$$

Observe que $sup(p)$ é um subconjunto de $\mathbb{N}$ e não do anel $\mathbb{A}$.

A sequência $(0, 0, 0, 0, \cdots)$ cujos coeficientes são todos nulos tem suporte vazio. Tal sequência é chamada *sequência nula*.

De agora em diante, $\mathbb{A}$ denotará um anel comutativo com unidade 1.

Definição 2.1 *Seja $\mathbb{A}$ um anel comutativo com unidade 1. Um polinômio numa indeterminada sobre $\mathbb{A}$, ou simplesmente um polinômio sobre $\mathbb{A}$, é uma sequência $(a_n)_{n\in\mathbb{N}}$ cujo suporte é finito.*

Em outras palavras, um polinômio em uma indeterminada sobre $\mathbb{A}$ é uma sequência $(a_n)_{n\in\mathbb{N}}$ em $\mathbb{A}$ que tem apenas um número finito de coeficientes são não nulos. Assim, a partir de um certo índice m teremos $a_{m+1} = a_{m+2} = \cdots = 0$.

Por simplificação, muitas vezes diremos simplesmente *um polinômio sobre* $\mathbb{A}$ ou ainda *um polinômio com coeficientes em* $\mathbb{A}$ para nos referirmos a um polinômio numa indeterminada sobre $\mathbb{A}$

Note que a sequência nula é um polinômio por ter suporte vazio, portanto finito. Este polinômio é chamado *polinômio nulo*. Como $\mathbb{A}$ tem 1, a sequência $(1, 0, 0, \cdots)$ também é um polinômio cujo suporte é $\{0\}$. Já as sequências $(0, 1, 0, \cdots)$ e $(1, 1, 0, \cdots)$ também são polinômios cujos suportes são, respectivamente, iguais a $\{1\}$ e $\{0, 1\}$.

Dizemos que dois polinômios $p = (a_0, a_1, a_2, \cdots)$ e $q = (b_0, b_1, b_2, \cdots)$ sobre $\mathbb{A}$ são *iguais* se e somente se $a_i = b_i$ em $\mathbb{A}$, para todo $i \in \mathbb{N}$.

Dado um polinômio não nulo $p = (a_0, a_1, a_2, \cdots)$ sobre $\mathbb{A}$, definimos o *grau* de p como sendo o maior número natural pertencente a $sup(p)$. Denotamos o grau de um polinômio não nulo p por $gr(p)$. Como o polinômio nulo tem suporte vazio, seu grau não é definido.

Note que $gr(1,0,0,\cdots)=0$, enquanto que $gr(0,1,\cdots)=gr(1,1,0,\cdots)=1$.

Note também que se $p=(a_0,a_1,a_2,\cdots)$ é um polinômio sobre $\mathbb{A}$ e $gr(p)=n$, então $a_m=0$ para todo $m>gr(p)$.

Um polinômio de grau zero é chamado *polinômio constante*. Explicitamente, os polinômios constantes são da forma $(a_0,0,0,\cdots)$, onde $a_0\in\mathbb{A}$.

Se $p=(a_0,a_1,a_2,\cdots)$ é um polinômio sobre $\mathbb{A}$ com $gr(p)=n$, o coeficiente a_n é chamado *coeficiente líder* de p. Um polinômio é dito ser *mônico* se seu coeficiente líder igual a 1.

Seja $\mathcal{A}$ o conjunto de todos os polinômios em uma ideterminada sobre $\mathbb{A}$. Vamos definir uma operação de soma $\oplus$ e um operação de multiplicação $\odot$ no conjunto $\mathcal{A}$.

Sejam $p=(a_0,a_1,a_2,\cdots)$ e $q=(b_0,b_1,b_2,\cdots)$ dois polinômios de $\mathcal{A}$. Definimos

$$\begin{aligned} p\oplus q= &\ (a_0+b_0,a_1+b_1,a_2+b_2,\cdots,a_k+b_k,\cdots)\\ &\ \text{e}\\ p\odot q= &\ (c_0,c_1,c_2,\cdots,c_k,\cdots), \end{aligned}$$

onde

$$\begin{cases} c_0=a_0b_0\\ c_1=a_0b_1+a_1b_0\\ c_2=a_0b_2+a_1b_1+a_2b_0\\ \vdots\\ c_k=a_0b_k+a_1b_{k-1}+a_2b_{k-2}+\cdots+a_{k-1}b_1+a_kb_0=\displaystyle\sum_{i=0}^{k}a_ib_{k-i}\\ \vdots \end{cases}$$

É fácil ver que $sup(p\oplus q)\subseteq sup(p)\cup sup(q)$, e portanto $sup(p\oplus q)$ é finito. Logo, $p\oplus q\in\mathcal{A}$. Para mostrar que $p\odot q\in\mathcal{A}$, suponha que $gr(p)=n$ e $gr(q)=m$. Se $k>n+m$, então $k>n$, $k>m$ e $k-n>m$. Disso segue que $a_{n+1}=a_{n+2}=\cdots a_k=0$ e $b_k=b_{k-1}=\cdots=b_{k-n}=0$, e portanto

$$c_k=\underbrace{a_0b_k+a_1b_{k-1}+\cdots+a_nb_{k-n}}_{=0}+\underbrace{a_{n+1}b_{k-n-1}+\cdots+a_kb_0}_{=0}=0.$$

Isto mostra que para todo $k>n+m$, $c_k=0$, ou seja, $sup(p\odot q)$ é finito.

Deste modo, $p \oplus p$ e $p \odot q$ são elementos de $\mathcal{A}$, i.é, $\oplus$ e $\odot$ são operações internas de $\mathcal{A}$, chamadas adição e multiplicação de polinômios, respectivamente.

Como a adição $+$ em $\mathbb{A}$ é associativa e comutativa, segue facilmente que a adição de polinômios também é associativa e comutativa. O polinômio nulo é o elemento neutro da adição, enquanto que o simétrico aditivo do polinômio $p = (a_0, a_1, a_2, \cdots)$ é o polinômio $(-a_0, -a_1, -a_2, \cdots)$ denotado por $-p$.

Para a multiplicação temos o polinômio $(1, 0, 0, \cdots)$ como sendo o elemento neutro. Além disso, a comutatividade da multiplicação segue diretamente da comutatividade da multiplicação em $\mathbb{A}$ e da maneira como foi definida multiplicação de polinômios acima.

A associatividade da multiplicação e a distributividade da mesma em relação a adição são um pouco mais sofisticadas e deixamos como exercício para o leitor.

Logo, concluímos que o conjunto $\mathcal{A}$ munido com as operações de adição e multiplicação definidas acima é um anel comutativo com unidade, chamado *anel de polinômios em uma indeterminada com coeficintes* $\mathbb{A}$ ou, por simplificação, *anel de polinômios sobre* $\mathbb{A}$.

Proposição 2.2 *Seja* $\mathbb{A}$ *um anel comutativo com unidade* 1 *e* $\mathcal{A}$ *o anel de polinômios sobre* $\mathbb{A}$. *O conjunto* $A_0 = \{(a_0, 0, 0, \cdots) : a_0 \in \mathbb{A}\}$ *é um subanel de* $\mathcal{A}$ *isomorfo a* $\mathbb{A}$.

Demonstração: Para provarmos este resultado, vamos usar a Proposição 1.11. Claramente, $(0, 0, 0, \cdots) \in A_0$. Agora, sejam $p = (a_0, 0, 0, \cdots)$ e $q = (b_0, 0, 0, \cdots)$ elementos de A_0. Neste caso, temos $a_i = b_i = 0$ para todo $i \in \mathbb{N}, i > 0$. Note que, $-q = (-b_0, 0, 0, \cdots) \in A_0$ e $p \oplus (-q) = (a_0 + (-b_0), 0+0, 0+0, \cdots) = (a_0 - b_0, 0, 0, \cdots) \in A_0$. Além disso, $p \odot q = (c_0, c_1, c_2, \cdots)$ onde

$$\begin{cases} c_0 = a_0 \cdot b_0 \\ c_1 = a_0 b_1 + a_1 b_0 = a_0 \cdot 0 + 0 \cdot b_0 = 0 \\ c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 = a_0 \cdot 0 + 0 \cdot 0 + 0 \cdot b_0 = 0 \\ \vdots \\ c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \cdots + a_{k-1} b_1 + a_k b_0 = a_0 \cdot 0 + 0 \cdot 0 + \cdots + 0 \cdot b_0 = 0 \\ \vdots \end{cases}$$

Portanto, $p \odot q = (a_0 b_0, 0, 0, \cdots) \in A_0$ o que mostra que A_0 é um subanel de $\mathcal{A}$.

Seja $\varphi : \mathbb{A} \longrightarrow A_0$ definida por $\varphi(a) = (a, 0, 0, \cdots)$, para todo $a \in \mathbb{A}$. É fácil ver que φ é um homomorfismo de anéis cuja inversa é a função $\psi : A_0 \longrightarrow \mathbb{A}$ definida por $\psi(a_0, 0, 0, \cdots) = a_0$, para todo $(a_0, 0, 0, \cdots) \in A_0$. Logo, φ é um isomorfismo de anéis. $\square$

A proposição anterior diz que o conjunto dos polinômios constantes sobre $\mathbb{A}$ é subanel de $\mathcal{A}$ que é isomorfo ao anel $\mathbb{A}$. Isto nos será bastante útil mais adiante.

A seguintes propriedades dos polinômios também são notáveis.

Lema 2.3 *Seja $\mathbb{A}$ um anel comutativo com unidade 1 e $\mathcal{A}$ o anel de polinômios sobre $\mathbb{A}$. Então, as seguintes identidades são válidas:*

(i) $(a_0, a_1, a_2, \cdots) \odot (0, 1, 0, 0, \cdots) = (0, a_0, a_1, a_2, \cdots)$, $\forall\, a_i \in \mathbb{A}, i \in \mathbb{N}$.

(ii) $(a, 0, 0, \cdots) \odot (0, 1, 0, \cdots)^n = (0, 0, \cdots, \underbrace{a}_{pos.\ n}, 0, \cdots), \forall a \in \mathbb{A}$.

Demonstração: (i) Para simplificarmos a notação, sejam $p = (a_0, a_1, a_2, \cdots)$ e $q = (b_0, b_1, b_2, \cdots)$ tal que $b_1 = 1$ e $b_i = 0$ para todo $i \in \mathbb{N}, i \neq 1$. Então, $p \odot q = (c_0, c_1, c_2, \cdots)$, onde

$$\begin{cases} c_0 = a_0 b_0 = a_0 0 = 0 \\ c_1 = a_0 b_1 + a_1 b_0 = a_0 1 + a_1 0 = a_0 \\ c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 = a_0 0 + a_1 1 + a_2 0 = a_1 \\ \vdots \\ c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0 = a_0 0 + a_1 0 + \cdots + a_{k-1} 1 + a_k 0 = a_{k-1} \\ \vdots \end{cases}$$

Logo, $p \odot q = (a_0, a_1, a_2, \cdots) \odot (0, 1, 0, 0, \cdots) = (0, a_0, a_1, \cdots)$.

(ii) Faremos a prova por indução sobre n.

Como $(0, 1, 0, \cdots)^0 = (1, 0, 0, \cdots)$, temos

$$(a, 0, 0, \cdots) \odot (0, 1, 0, \cdots)^0 = (a, 0, 0, \cdots) \odot (1, 0, 0, \cdots) = (a, 0, 0, \cdots)$$

e portanto a a afirmação vale para $n = 0$.

Suponha que $(a, 0, 0, \cdots) \odot (0, 1, 0, \cdots)^n = (0, 0, \cdots, \underbrace{a}_{\text{pos. } n}, 0, \cdots)$ para algum $n \in \mathbb{N}$.

Então,

$$\begin{aligned}(a,0,0,\cdots)\odot(0,1,0,\cdots)^{n+1} &= (a,0,0,\cdots)\odot(0,1,0,\cdots)^{n}\odot(0,1,0,0\cdots)\\ &= (0,0,\cdots,\underbrace{a}_{\text{pos. } n},0,\cdots)\odot(0,1,0,0,\cdots)\\ &= (0,0,\cdots,\underbrace{a}_{\text{pos. } n+1},0,\cdots),\ \text{pelo item } (ii)\end{aligned}$$

□

Considere um polinômio $p=(a_0,a_1,a_2,a_3,\cdots,a_n,0,0,\cdots)$ com coeficientes em um anel comutativo com unidade $\mathbb{A}$, como $a_n\neq 0$. Então, pelo item (ii) do lema anterior, temos:

$$\begin{aligned}p &= (a_0,0,0,\cdots)\oplus(0,a_1,0,\cdots)\oplus(0,0,a_2,0,\cdots)\oplus\cdots\oplus(0,0,\cdots,0,a_n,0\cdots)\\ &= (a_0,0,0,\cdots)\odot(0,1,0,\cdots)^0\oplus[(a_1,0,0,\cdots)\odot(0,1,0,0,\cdots)^1]\\ &\quad\oplus[(a_2,0,0,\cdots)\odot(0,1,0,0,\cdots)^2]\oplus[(a_3,0,0,\cdots)\odot(0,1,0,0,\cdots)^3]\\ &\quad\oplus\cdots\oplus[(a_n,0,0,\cdots)\odot(0,1,0,0,\cdots)^n]\end{aligned}$$

Observe que pela Proposição 2.2, o conjunto dos polinômios constantes sobre $\mathbb{A}$ é subanel de $\mathcal{A}$ que é isomorfo ao anel $\mathbb{A}$. Assim, podemos identificar a_i com $(a_i,0,0,\cdots)$ e portanto, podemos escrever a_i no lugar de $(a_i,0,0,\cdots)$, para todo $i\in\mathbb{N}$. Deste modo, o símbolo a_i será usado para designar duas coisas distintas: o elemento $a_i\in\mathbb{A}$, quando este for o caso, e o elemento $(a_i,0,0,\cdots)\in\mathcal{A}$, quando estivermos estudando polinômios. Logo, o polinômio $p=(a_0,a_1,a_2,a_3,\cdots,a_n,0,0,\cdots)$ será escrito como

$$\begin{aligned}p &= a_0\odot(0,1,0,\cdots)^0\oplus[a_1\odot(0,1,0,0,\cdots)^1]\oplus[a_2\odot(0,1,0,0,\cdots)^2]\\ &\quad\oplus[a_3\odot(0,1,0,0,\cdots)^3]\oplus\cdots\oplus[a_n\odot(0,1,0,0,\cdots)^n].\end{aligned}$$

Por razões práticas, vamos denotar o polinômio $(0,1,0,0,\cdots)$ pelo símbolo x. Então, como $x^0=1$ e $x^1=x$, podemos escrever qualquer polinômio $p=(a_0,a_1,a_2,a_3,\cdots,a_n,0,0,\cdots)$ da seguinte forma:

$$p=a_0\oplus(a_1\odot x)\oplus(a_2\odot x^2)\oplus(a_3\odot x^3)\oplus\cdots\oplus(a_n\odot x^n).$$

Para simplificar ainda mais a notação, vamos escrever $+$ no lugar de $\oplus$ e $\cdot$ no lugar de $\odot$.

Logo, com todas as convensões que acabamos de propor, todo polinômio $p = (a_0, a_1, a_2, a_3, \cdots, a_n, 0, 0, \cdots)$ é igual a soma $a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n$, onde a_ix^i denota $a_i \cdot x^i$. Deste modo,

$$\mathcal{A} = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \,|\, a_i \in \mathbb{A} \text{ e } n \in \mathbb{N}\} = \left\{\sum_{i=1}^{n} a_ix^i \mid a_i \in \mathbb{A} \text{ e } n \in \mathbb{N}\right\},$$

e as operações deste deste anel são aquelas apresentadas anteriormente e que são simplesmente aquelas que estamos (ou deveriamos estar) acostumados.

A partir de agora, o *anel de polinômios em uma indeterminada* sobre um anel comutativo com unidade $\mathbb{A}$ será denotado por $\mathbb{A}[x]$. Um elemento de $\mathbb{A}[x]$ será denotado por $f(x)$, ou $p(x)$, ou $q(x)$, etc. O polinômio nulo é o polinômio $0 + 0x + 0x^2 + \cdots + 0x^n$ que será denotado simplesmente por 0. A unidade de $\mathbb{A}[x]$ é o polinômio $1+0x+0x^2+\cdots+0x^n$ que é denotado por 1.

Observação 2.4 *Com toda construção que fizemos acima, fica explicado quem é o x que aparece no anel de polinômios.*

Vamos agora enunciar as definições que vimos anteriomente sobre polinômios, mas usando a nova notação.

Definição 2.5 *Sejam $\mathbb{A}$ um anel comutativo com unidade e $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{A}[x]$, com $a_n \neq 0$. Cada a_i é chamado coeficiente de $p(x)$. O número natural n é chamado grau de $p(x)$. O coeficiente a_n é chamado coeficiente lider de $p(x)$. Quando o coeficiente líder é 1, o polinômio é dito mônico.*

Proposição 2.6 *Sejam $\mathbb{A}$ um domínio e $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, $q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \in \mathbb{A}[x]$ tais que $a_n \neq 0$ e $b_m \neq 0$, i.é, $gr(p(x) = n$ e $gr(q(x) = m$. Então:*

(i) $gr(p(x) + q(x)) \leq max\{n, m\}$, *sempre que* $gr(p(x) + q(x)) \neq 0$.

(ii) $gr(p(x)q(x)) = m + n = gr(p(x)) + gr(q(x))$

Demonstração: Faremos somente a prova do item (ii). Como sabemos, $p(x)q(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n+m}x^{n+m}$, onde

$$\begin{cases} c_0 = a_0b_0 \\ c_1 = a_0b_1 + a_1b_0 \\ c_2 = a_0b_2 + a_1b_1 + a_2b_0 \\ \vdots \\ c_{n+m} = a_0b_{n+m} + a_1b_{n+m-1} + \cdots + a_nb_m + a_{n+1}b_{m-1} + \cdots + a_{n+m-1}b_1 + a_{n+m}b_0 \end{cases}$$

Note que $c_{n+m} = a_nb_m$ e $= a_nb_m \neq 0$, pois $\mathbb{A}$ é um domínio. Logo, $gr(p(x)q(x)) = m + n = gr(p(x)) + gr(q(x))$. □

2.3 Polinômios e Funções Polinomiais

Um erro grave cometido por muitos estudantes da área de ciências exatas é pensar que não há diferença entre os conceitos de polinômio em uma indeterminada sobre um anel $\mathbb{A}$ e função polinomial (em uma variável) sobre o mesmo anel $\mathbb{A}$. Porém, a construção feita acima possibilita entender melhor a diferença entre tais conceitos.

Sejam $\mathbb{A}$ um anel comutativo com unidade e $a_0, a_1, \cdots a_n \in \mathbb{A}$ elementos quaisquer. Uma *função polinomial* (em uma variável) sobre $\mathbb{A}$ é uma função $f : \mathbb{A} \longrightarrow \mathbb{A}$ que associa a cada $x \in \mathbb{A}$ um único $y = a_0 + a_1x + \cdots a_nx^n \in \mathbb{A}$. Tal y, por ser único, é denotado por $f(x) = a_0 + a_1x + \cdots a_nx^n \in \mathbb{A}$. Uma função polinomial $f : \mathbb{A} \longrightarrow \mathbb{A}$ é dita identicamente nula se $f(x) = 0$ para todo $x \in \mathbb{A}$.

Informalmente, podemos imediatamente perceber que polinômio e função polinomial não são a mesma coisa, pois em um polinômio o "x"é uma sequência específica em $\mathbb{A}$, enquanto que o "x"de uma função polinomial é qualquer elemento de $\mathbb{A}$.

Formalmente, vemos a diferença de polinômios e função polinomial da seguinte forma: considere o corpo $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ e a função polinomial $f : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$ definida por $f(x) = x + x^2$. Então,

$$f(\bar{0}) = \bar{0} + \bar{0}^2 = \bar{0} \text{ e } f(\bar{1}) = \bar{1} + \bar{1}^2 = \bar{2} = \bar{0},$$

ou seja, f é a função polinomial identicamente nula. Mas é claro que pela nossa definição de polinômio em uma indeterminada x, o polinômio $p(x) = x+x^2 \in \mathbb{Z}_2[x]$ não o polinômio nulo. Em termos de sequências, esse polinômio seria $(\bar{0}, \bar{1}, \bar{1}, \bar{0}, \bar{0}, \cdots)$.

2.4 Algoritmo da Divisão de Euclides

Em termos técnicos, um algoritmo é uma sequência lógica, finita e definida de instruções que devem ser seguidas para resolver um problema ou executar uma tarefa. Em uma linguagem mais simples, um algoritmo nada mais é do que uma receita que mostra passo a passo os procedimentos necessários para a resolução de uma tarefa. Ele não responde a pergunta "o que fazer?", mas sim "como fazer".

Um algoritmo em matemática muito útil é o chamado Algoritmo da Divisão de Euclides. Embora ele seja mais abrangente, nós o enunciaremos e provaremos para o caso de polinômios sobre um corpo.

Teorema 2.7 (***Algoritmo da Divisão de Euclides***)
Seja $\mathbb{K}$ um corpo. Se $f(x), g(x) \in \mathbb{K}[x]$ com $g(x) \neq 0$, então existem únicos $q(x), r(x) \in \mathbb{K}[x]$ tais que

$$f(x) = g(x)q(x) + r(x),$$

onde $r(x) = 0$ ou $gr(r(x)) < gr(g(x))$.

Demonstração: Suponha que $f(x) = a_0 + a_1x + \cdots a_nx^n$ e $g(x) = b_0 + b_1x + \cdots b_mx^m$, com $gr(g(x)) = m$.

Existência:

Se $f(x) = 0$, basta tomar $q(x) = r(x) = 0$.

Suponha que $f(x) \neq 0$ e que $gr(f(x)) = n$. Se $n < m$, tome $q(x) = 0$ e $r(x) = f(x)$. Portanto, resta considerar o caso em que $n \geq m$.

A idéia é multiplicar $g(x)$ por um polinômio apropriado e subtrair o resultado de $f(x)$ a fim de conseguirmos um outro polinômio de grau menor que o grau de $f(x)$.

Multiplicamos $g(x)$ por $a_n b_m^{-1} x^{n-m}$. Subtraindo este resultado de $f(x)$ obtemos um outro polinômio $f_1(x)$, i.é,

$$f(x) - a_n b_m^{-1} x^{n-m} g(x) = f_1(x).$$

Como

$$\begin{aligned} a_n b_m^{-1} x^{n-m} g(x) &= (a_n b_m^{-1} x^{n-m})(b_0 + b_1 x + \cdots b_m x^m) \\ &= a_n b_m^{-1} b_0 x^{n-m} + a_n b_m^{-1} b_1 x^{n-m+1} + \cdots + a_n b_m^{-1} b_m x^{n-m+m} \\ &= a_n b_m^{-1} b_0 x^{n-m} + a_n b_m^{-1} b_1 x^{n-m+1} + \cdots + a_n x^n, \end{aligned}$$

temos que $gr(f_1(x)) = gr(f(x) - a_n b_m^{-1} x^{n-m} g(x)) < gr(f(x)$.

Se $f_1(x) = 0$, então tomamos $q(x) = a_n b_m^{-1} x^{n-m}$ e $r(x) = 0$.

Se $gr(f_1(x)) < gr(g(x))$, então tomamos $q(x) = a_n b_m^{-1} x^{n-m}$ e $r(x) = f_1(x)$.

Se $gr(f_1(x)) \geq gr(g(x))$, então executamos o processo anterior colocando $f_1(x)$ no lugar de $f(x)$. Ou seja, se $f_1(x) = c_0 + c_1 x + \cdots + c_p x^p$, com $c_p \neq 0$ e $p \geq m$, então multiplicamos $g(x)$ por $c_p b_m^{-1} x^{p-m}$ e subtraindo este resultado de $f_1(x)$ obtendo um outro polinômio $f_2(x)$ dado por

$$f_1(x) - c_p b_m^{-1} x^{p-m} g(x) = f_2(x).$$

Novamente, $gr(f_2(x)) < gr(f_1(x))$.

Substituindo $f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$ na igualdade anterior obtemos

$$\begin{aligned} f_2(x) &= f(x) - a_n b_m^{-1} x^{n-m} g(x) - c_p b_m^{-1} x^{p-m} g(x) \\ &= f(x) - [a_n b_m^{-1} x^{n-m} + c_p b_m^{-1} x^{p-m}] g(x). \end{aligned}$$

Se $f_2(x) = 0$, tomemos $q(x) = a_n b_m^{-1} x^{n-m} g(x) + c_p b_m^{-1} x^{p-m}$ e $r(x) = 0$.

Se $gr(f_2(x)) < gr(g(x))$, tomemos $q(x) = a_n b_m^{-1} x^{n-m} + c_p b_m^{-1} x^{p-m}$ e $r(x) = f_2(x)$.

Se $gr(f_2(x)) \geq gr(g(x))$, repetimos o processo anterior. Ora, a cada passo o grau do polinômio $f_i(x)$ encontrado diminui estritamente, de modo que após um número finito de passos (n passos no máximo), obteremos $f_i(x) = 0$, ou $gr(f_i(x)) < gr(g(x))$. Neste momento tomaremos $r(x) = f_i(x)$ e $q(x)$ conforme acima.

Unicidade:

Suponha que existam $q_1(x), q_2(x), r_1(x), r_2(x) \in \mathbb{K}[x]$ tais que $f(x) = q_1(x)g(x)+r_1(x)$ e $f(x) = q_2(x)g(x) + r_2(x)$, onde $r_i(x) = 0$ ou $gr(r_i(x)) < gr(g(x))$, $i = 1, 2$. Então,

$$q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x) \Rightarrow r_1(x) - r_2(x) = [q_2(x) - q_1(x)]g(x).$$

Se $q_1(x) \neq q_2(x)$, então

$$gr(r_1(x) - r_2(x)) = gr((q_1(x) - q_2(x))g(x) = gr((q_1(x) - q_2(x)) + gr(g(x)) \geq gr(g(x)).$$

Porém, como $gr(r_i(x)) < gr(g(x))$, temos que $gr(r_1(x)-r_2(x)) < max\{gr(g(x)), gr(g(x))\} = gr(g(x))$, contradição.

Logo, $q_1(x) = q_2(x)$. Neste caso, claramente também temos $r_1(x) = r_2(x)$.

Nomenclatura: Na notação do teorema anterior, $f(x)$ é chamado *dividendo*, $g(x)$ é chamado *divisor*, $q(x)$ é chamado *quociente* e $r(x)$ é chamado de *resto*. □

Exemplo 2.8 *Considere $f(x) = 12x^3 + 4x^2 - 8x$ e $g(x) = 4x$ pertencentes a $\mathbb{R}[x]$. Determine o quociente e o resto da divisão de $f(x)$ por $g(x)$ usando o algoritmo da divisão.*

Solução: Note que o $gr(f(x)) = 3$, $gr(g(x)) = 1$ e os conficientes lideres de $f(x)$ e $g(x)$ são, respectivamente, 12 e 4. Pelo algoritmo da divisão temos:

$$f_1(x) = f(x) - 12 \cdot 4^{-1}x^{3-1} \cdot g(x) = (12x^3 + 4x^2 - 8x) - (3x^2) \cdot 4x = 4x^2 - 8x.$$

Como $gr(f_1(x)) \geq gr(g(x))$, vamos repetir o processo anterior.

$$f_2(x) = f_1(x) - 4 \cdot 4^{-1}x^{2-1} \cdot g(x) = (4x^2 - 8x) - (x) \cdot 4x = -8x.$$

Como $gr(f_2(x)) \geq gr(g(x))$, vamos repetir o processo anterior.

$$f_3(x) = f_2(x) - (-8) \cdot 4^{-1}x^{1-1} \cdot g(x) = (-8x) - (-2) \cdot 4x = 0.$$

Como $f_3(x) = 0$, temos do algoritmo da divisão que $q(x) = 3x^2 + x - 2$ e $r(x) = 0$.

Exemplo 2.9 *Considere $f(x) = 12x^3 - 19x^2 + 15x - 3$ e $g(x) = 3x^2 - x + 2$ pertencentes a $\mathbb{R}[x]$. Determine o quociente e o resto da divisão de $f(x)$ por $g(x)$ usando o algoritmo da divisão.*

Solução: Note que o $gr(f(x)) = 3$, $gr(g(x)) = 2$ e os coeficientes líderes de $f(x)$ e $g(x)$ são, respectivamente, 12 e 3. Pelo algoritmo da divisão temos:

$$f_1(x) = f(x) - 12 \cdot 3^{-1}x^{3-2} \cdot g(x) = (12x^3 - 19x^2 + 15x - 3) - (4x) \cdot (3x^2 - x + 2) = -15x^2 + 7x - 3.$$

Como $gr(f_1(x)) \geq gr(g(x))$, vamos repetir o processo anterior.

$$f_2(x) = f_1(x) - (-15) \cdot 3^{-1}x^{2-2} \cdot g(x) = (-15x^2 + 7x - 3) - (-5) \cdot (3x^2 - x + 2) = 2x + 7.$$

Como $gr(f_2(x)) < gr(g(x))$, temos do algoritmo da divisão que $q(x) = 4x - 5$ e $r(x) = 2x + 7$.

Observação 2.10 *O Algorítmo da Divisão de Euclides pode ser aplicado sobre $\mathbb{A}[x]$, onde $\mathbb{A}$ é um domínio de integridade, sempre que o coeficiente líder do divisor $g(x)$ é invertível em $\mathbb{A}$. Em particular, o Algorítmo da Divisão de Euclides pode ser aplicado quando o divisor $g(x)$ é um polinômio mônico.*

Exemplo 2.11 *Considere $f(x) = 2x^3 + 6x^2 + 7x - 1$ e $g(x) = x + 3$ pertencentes a $\mathbb{Z}[x]$. Determine o quociente e o resto da divisão de $f(x)$ por $g(x)$ usando o algoritmo da divisão.*

Solução: Mesmo que $\mathbb{Z}$ não é corpo, pela observação anterior, podemos aplicar o Algoritmo de Euclides, pois $g(x)$ é um polinômio mônico em $\mathbb{Z}[x]$.

Note que o $gr(f(x)) = 3$, $gr(g(x)) = 1$ e os coeficientes líderes de $f(x)$ e $g(x)$ são, respectivamente, 2 e 1. Pelo algoritmo da divisão temos:

$$f_1(x) = f(x) - 2 \cdot 1^{-1}x^{3-1} \cdot g(x) = (2x^3 + 6x^2 + 7x - 1) - 2x^2 \cdot (x + 3) = 7x - 1.$$

Como $gr(f_1(x)) \geq gr(g(x))$, vamos repetir o processo anterior.

$$f_2(x) = f_1(x) - (7) \cdot 1^{-1}x^{2-2} \cdot g(x) = (7x - 1) - 7 \cdot (x + 3) = -22.$$

Como $gr(f_2(x)) < gr(g(x))$, temos do algoritmo da divisão que $q(x) = 2x^2 + 7$ e $r(x) = -22$.

Definição 2.12 *Dados um polinômio* $f(x) = a_0 + a_1x + \cdots a_nx^n \in \mathbb{A}[x]$, *onde* $\mathbb{A}$ *é um anel comutativo com unidade, e um elemento* $\alpha \in \mathbb{A}$, *a substituição de* x *por* α *em* $f(x)$ *é um elemento de* $\mathbb{A}$ *dado por*

$$f(\alpha) = a_0 + a_1\alpha + \cdots a_n\alpha^n.$$

Se $f(\alpha) = 0$, *diremos que* α *é uma raiz de* $f(x)$ *em* $\mathbb{A}$.

Corolário 2.13 *Seja* $\mathbb{A}$ *um domínio de integridade. Se* $f(x) \in \mathbb{A}[x]$ *e* $\alpha \in \mathbb{A}$, *então o resto da divisão de* $f(x)$ *por* $x - \alpha$ *é* $f(\alpha)$. *Em particular,* α *é raiz de* $f(x)$ *se e somente se* $f(x) = (x - \alpha) \cdot q(x)$, *para algum* $q(x) \in \mathbb{A}[x]$.

Demonstração: Uma vez que $x-\alpha$ é mônico, podemos aplicar o Algoritmo de Euclides e obteremos polinômios $q(x), r(x) \in \mathbb{A}[x]$ tais que $f(x) = (x - \alpha) \cdot q(x) + r(x)$, onde $r(x) = 0$ ou $gr(r(x) < 1$. Em todo caso, $r(x) = a$, para algum $a \in \mathbb{A}$. Logo,

$$f(\alpha) = (\alpha - \alpha) \cdot q(\alpha) + r(\alpha) = a = r(x).$$

Em particular,

$$\alpha \text{ é raiz de } f(x) \Leftrightarrow f(\alpha) = 0 \Leftrightarrow r(x) = 0 \Leftrightarrow f(x) = (x - \alpha) \cdot q(x).$$

□

Corolário 2.14 *Seja* $\mathbb{A}$ *um domínio de integridade. Se* $f(x) \in \mathbb{A}[x]$ *é um polinômio não nulo de grau* n *então o número de raizes de* $f(x)$ *é menor ou igual a* n.

Demonstração: Faremos a demonstração por indução sobre $n = gr(f(x))$. Se $gr(f(x)) = 0$ então $f(x) = a$, com $0 \neq a \in \mathbb{A}$, e portanto o número de raízes de $f(x)$ é zero.

Suponha agora que o corolário vale para polinômios de grau $n - 1$. Vamos mostrar que vale para $f(x)$. Se $f(x)$ não possui raízes em $\mathbb{A}$, então o corolário segue. Porém, se $f(x)$ possui uma raiz $\alpha \in \mathbb{A}$ então, pelo corolário anterior, $f(x) = (x - \alpha) \cdot q(x)$, para algum $q(x) \in \mathbb{A}[x]$. Como $q(x)$ tem grau $n - 1$, segue da hipótese de indução que $q(x)$ tem no máximo $n - 1$ raízes. Mas toda raiz de $q(x)$ também é uma raiz de $f(x)$. Logo, $f(x)$ tem no máximo n raízes. □

Observação 2.15 *Sejam $\mathbb{K}$ e $\mathbb{L}$ dois corpos tais que $\mathbb{K} \subseteq \mathbb{L}$. O número de raízes de um polinômio $f(x) \in \mathbb{K}[x]$ pode aumentar se o considerarmos como um polinômio de $\mathbb{L}[x]$. Por exemplo, o polinômio $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ não possui raízes em $\mathbb{Q}$, possui uma raiz em $\mathbb{R}$ e possui três raízes em $\mathbb{C}$, a saber,*

$$\alpha_1 = 1,\ \alpha_2 = \sqrt[3]{2}\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right),\ \alpha_3 = \sqrt[3]{2}\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right).$$

Se retirarmos a hipótese de $\mathbb{A}$ ser um domínio de integridade então o corolário anterior é falso. Por exemplo, o polinômio de grau 2 $f(x) = x^2 + \bar{3}x + \bar{2} \in \mathbb{Z}_6[x]$ possui 4 raízes em $\mathbb{Z}_6$. São elas $\bar{1}$, $\bar{2}$, $\bar{4}$ e $\bar{5}$.

Bibliografia

[1] GONÇALVES, A.; *Introdução à Álgebra*. Projeto Euclides, IMPA-CNPq, 5ª ed., (2001).

[2] Garcia, A. e Lequain, I. *Elementos de Álgebra*. Projeto Euclides, IMPA-CNPq, (2002).

[3] www.campusitabaiana.ufs.br/matematica