AULA

Algoritmo da divisão em $k[x]$ 2

META:

Introduzir um algoritmo de divisão para anéis de polinômios definidos sobre corpos.

OBJETIVOS:

Ao fim da aula os alunos deverão ser capazes de:

Aplicar o algoritmo da divisão para determinar o quociente e o resto na divisão entre polinômios.

Conceituar função polinomial e zeros de uma função polinomial.

Estabelecer a diferença entre polinômios e funções polinomiais.

Enunciar e provar o teorema do resto e do fator.

PRÉ-REQUISITOS

A estrutura de anel para polinômios. Embora não seja necessário, os conhecimentos do ensino médio sobre divisão de polinômios, funções polinomiais, teorema do resto e do fator e uma revisão sobre o algoritmo da divisão para os inteiros ajudariam num melhor rendimento desta aula.

2.1 Introdução

Nesta aula, partiremos do seu conhecimento do ensino médio e fundamental sobre divisão de polinômios e formalizaremos tal método em forma de um algoritmo. A unicidade do quociente e do resto e o fato do resto ser nulo ou possuir grau estritamente menor que o grau do divisor são as propriedades fundamentais deste algoritmo. A última propriedade é de extrema importância teórica e terá profundas consequências no estudo de polinômios. A primeira delas é o teorema do fator e do resto já conhecido por você do ensino médio. As outras veremos na aula seguinte. Convém lembrar que LT(g) denota o termo líder do polinômio g.

OBS 2.1. Ao longo deste curso, a menos que seja dito o contrário, usaremos a letra k para denotar um corpo.

2.2 O Algoritmo da divisão em $k[x]$

Sejam $f(x) = 3x^5 + 2x^4 + 2x^3 + 4x^2 + x - 2$ e $g(x) = 2x^3 + 1$ dois polinômios em $\mathbb{Q}[x]$. Para dividir f por g, obtemos o primeiro termo do quociente $\dfrac{3x^5}{2x^3} = \dfrac{3}{2}x^2$. Este é o resultado da divisão dos termos dominantes de f e g. A diferença

$$f(x) - \frac{3}{2}x^2 g(x) = r_1(x) = 2x^4 + 2x^3 + \frac{5}{2}x^2 + x - 2$$

nos fornece o primeiro resto parcial. Repetindo este procedimento para $r_1(x)$ no lugar de $f(x)$ obtemos o segundo resto parcial

$$r_2(x) = r_1(x) - xg(x) = 2x^3 + \frac{5}{2}x^2 - 2.$$

Note que deg $f(x) >$ deg $r_1(x) >$ deg $r_2(x)$. Podemos aplicar este procedimento enquanto o grau do resto for menor do que o grau de $g(x)$. Ao fazer isto, obtemos uma sequência de restos $r_1, r_2, r_3, \ldots$ na qual

$$\deg r_1 > \deg r_1 > \deg r_2 > \deg r_3 > \dots$$

Se deg $f >$ deg g então, após no máximo $k = \deg f - \deg g + 1$ passos, devemos ter deg $r_k <$ deg g. Assim, $f(x) = g(x).q(x) + r(x)$ com $r(x) = r_k(x)$ satisfazendo as condições $r(x) = 0$ ou $0 \geq \deg r(x) < \deg g(x)$. Se deg $f(x) <$ deg $g(x)$ podemos fazer $r(x) = f(x)$ e obter, ainda, $f(x) = g(x).0 + r(x)$ com $r(x) = 0$ ou $0 \geq \deg r(x) < \deg g(x)$. Em forma de algoritmo o que temos é o seguinte:

Input: g, f $\quad (g \neq 0)$

Output: q, r.

$q := 0$; $r = f$

Enquanto $r \neq 0$ e LT(g) dividir LT(r) faça

$$q := q + \text{LT}(r)/\text{LT}(g)$$

$$r := r - [\text{LT}(r)/\text{LT}(g)]\, g$$

O grau do dividendo r, em cada passo, é estritamente menor que o grau do dividendo do passo anterior. Assim, o algoritmo termina no máximo em deg $f -$ deg $g + 1$ passos. Isto mostra a existência de q e r tais que

$$f = qg + r$$

com $r = 0$ ou $0 \leq \deg r \leq \deg g$. Podemos, ainda, mostrar que o quociente $q(x)$ e o resto $r(x)$, assim obtidos, são únicos. De fato, suponham q_1, q_2 dois quocientes e r_1, r_2 dois restos para uma mesma divisão de f por g com os restos satisfazendo as condições acima. Então,

$$q_1 g + r_1 = f = q_2 g + r_2$$

donde $(q_1 - q_2)g = r_2 - r_1$. Se $q_1 \neq q_2$, então, $q_1 - q_2 \neq 0$. Assim,

$$\deg r_2 - r_1 = \deg\,(q_1 - q_2)g = \deg\,(q_1 - q_2) + \deg\, g \geq \deg\, g$$

e isto é uma contradição, pois, ambos r_1 e r_2 têm graus menor do que o grau de g. Logo, $q_1 = q_2$ e, portanto,

$$r_1 - r_2 = (q_1 - q_2)g = 0g = 0$$

donde $r_1 = r_2$. O resultado que acabamos de provar é chamado *algoritmo da divisão*. Segue o enunciado em forma de teorema.

Teorema 2.1. *(Algoritmo da divisão) Seja k um corpo e $f(x), r(x) \in k[x]$ com $g(x) \neq 0$. Então, existem únicos polinômios $q(x), r(x) \in k[x]$ tais que*

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

com $r(x) = 0$ ou $0 \leq$ deg $r(x) <$ deg $g(x)$. □

Prezado aluno, caso você não tenha se convencido da existência de q e r em forma de algoritmo, segue a prova convencional.

Prova: (Existência) Se $f(x) = 0$ ou deg $f <$ deg $g(x)$ faça $r(x) = f(x)$ e $q(x) = 0$. Suponha deg $f(x) \geq$ deg $g(x)$. Neste caso, procederemos por indução em deg $f(x)$. O polinômio $h(x) = f(x) - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)}g$ tem grau menor que o polinômio f (seus termos dominantes são iguais). Por hipótese indutiva, existem $q'(x), r'(x) \in k[x]$ tais que

$$h(x) = f(x) - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)}g = q'(x)g(x) + r'(x)$$

com $r'(x) = 0$ ou $0 \leq$ deg $r'(x) <$ deg $g(x)$. Assim,

$$f(x) = \left(q'(x) + \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)}\right)g + r'(x).$$

Então, $q(x) = q'(x) + \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)}$ e $r(x) = r'(x)$ satisfazem as propriedades requeridas.

Exemplo 2.1. Vamos determinar o quociente e o resto da divisão

de $f(x) = 3x^4 - 2x^3 + 6x^2 - x + 2$ por $g(x) = x^2 + x + 1$ em $\mathbb{Q}[x]$.

$$\begin{array}{ll} 3x^4 - 2x^3 + 6x^2 - x + 2 & \underline{\mid x^2 + x + 1} \\ \underline{-3x^2 - 3x^3 - 3x^2} & 3x^2 - 5x + 8 \\ -5x^3 + 3x^2 - x + 2 & \\ \underline{5x^3 + 5x^2 + 5x} & \\ 8x^2 + 4x + 2 & \\ \underline{-8x^2 - 8x - 8} & \\ -4x - 6 & \end{array}$$

Resposta: Quociente: $3x^2 - 5x + 8$; Resto: $-4x - 6$.

2.3 O teorema do resto e do fator

Seja $A \subset B$ uma extensão de anéis. Uma função $f : A \to B$ é dita polinomial se existem $a_0, a_1, \ldots, a_n \in A$ tais que

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

para todo $a \in A$. Um elemento $a \in A$ tal que $f(a) = 0$ é chamado zero da função f. Seja

$$p(x) = a_0 + a_1 x + \cdots a_n x^n \in A[x]$$

o polinômio associado à função polinomial f. A relação entre polinômios e funções polinomiais é sultil e merece algum comentário. Para todo polinômio

$$q(x) = b_0 + b_1 x + \cdots b_m x^m \in A[x]$$

está associado uma função polinomial $f\ A \to A$ definida por $f(a) = q(a)$ onde $q(a)$ denota a operação $b_0 + b_1 a + \cdots b_m a^m$ em A. Assim, $q(a) = b_0 + b_1 a + \cdots b_m a^m$ equivale a substituir a no lugar de x em $q(x)$ (tal operação não está definida no anel de polinômios).

Um elemento $a \in A$ tal que $q(a) = 0$ é chamado *raiz* do polinômio $q(x)$. A sultileza aqui é que funções polinomiais e polinômios são objetos distintos. A correspondência

$$\{\text{polinômios em } A[x]\} \overset{\Psi}{\leftrightarrow} \{\text{Funções polinomiais}\}$$

embora seja sempre sobrejetiva não é em geral injetiva. É o que mostra o exemplo abaixo.

Exemplo 2.2. Em $\mathbb{Z}_2[x]$ o polinômio $f(x) = x^2 + 1$ não é nulo, mas a função polinomial $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ é a função nula.

Exemplo 2.3. Os polinômios $p(x) = x^4+x+1, q(x) = x^3+x^2+1 \in \mathbb{Z}_3[x]$ definem as funções polinomiais $f : \mathbb{Z}_3 \to \mathbb{Z}_3$, $f(r) = r^4+r+1$ e $g : \mathbb{Z}_3 \to \mathbb{Z}_3$, $g(t) = t^3 + t^2 + 1$. Tem-se $f(0) = 1 = g(0)$, $f(1) = 0 = g(1)$ e $f(2) = 1 = g(2)$. Assim, $f(r) = g(r)$ para todo $r \in \mathbb{Z}_3$. Logo, f e g definem a mesma função em $\mathbb{Z}_3$ embora, como polinômios, sejam distintos.

Teorema 2.2. (Teorema do resto) *O resto da divisão de um polinômio $f(x) \in k[x]$ por $x - a$ é $f(a)$.*

Prova: Existem únicos $q(x), r(x) \in k[x]$ tais que

$$f(x) = q(x)(x - a) + r(x)$$

com $r(x) = 0$ ou $0 \leq \deg r(x) < \deg (x - a) = 1$. Então, $r(x) = 0$ ou $\deg r(x) = 0$. Assim, $r(x)$ necessariamente é uma constante $c \in k$. Da igualdade acima segue a igualdade

$$f(a) = q(a)(a - a) + c = c = r(x). \quad \square$$

Teorema 2.3. (Teorema do fator) *Seja $f(x) \in k[x]$. Um elemento $a \in k$ é uma raiz de $f(x)$ se e somente se $x - a$ divide $f(x)$.*

Prova: Seja $r(x)$ o resto da divisão de $f(x)$ por $x - a$. Pelo teorema do resto, tem-se $r(x) = f(a)$. Assim, a é raiz de $f(x) \Leftrightarrow f(a) = r(x) = 0 \Leftrightarrow x - a$ divide $f(x)$. $\square$

2.4 Conclusão

Nesta aula, implementamos um algoritmo de divisão em $k[x]$ semelhante àquele dos números inteiros. Como consequência imediata, obtivemos a relação fundamental entre os zeros de uma função polinomial e os fatores lineares da forma $x-a$ do polinômio que a define; a saber: o teorema do resto e do fator. A respeito do que diz estes resultados, podemos extrair duas importantes conclusões. Primeira, um polinômio admite sempre um número finito de raízes tendo seu grau como cota superior. Segunda, a existência de raízes para um polinômio é relativa ao anel de coeficientes em que se considera o polinômio. Por exemplo, x^2+1 não possui raízes reais, mas admite duas raízes em $\mathbb{C}$.

RESUMO

Algoritmo da divisão em $k[x]$

Input: g, f $\quad (g \neq 0)$
Output: q, r.
$q := 0$; $r = f$
Enquanto $r \neq 0$ e LT(g) dividir LT(r) faça

$$q := q + \text{LT}(r)/\text{LT}(g)$$
$$r := r - [\text{LT}(r)/\text{LT}(g)]\, g$$

Em forma de teorema:
Seja k um corpo e $f(x), r(x) \in k[x]$ com $g(x) \neq 0$. Então, existem únicos polinômios $q(x), r(x) \in k[x]$ tais que

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

Algoritmo da divisão em $k[x]$

com $r(x) = 0$ ou $0 \leq \deg r(x) < \deg g(x)$.

Funções polinomiais *versus* **polinômios**

Os polinômios $p(x) = x^4 + x + 1, q(x) = x^3 + x^2 + 1 \in \mathbb{Z}_3[x]$ são distintos mas estão associados à mesma função polinomial.

Análise	Álgebra	Geometria
Funções polinomiais	Polinômios	Gráfico
Zero	Raiz	Interseção com o eixo das abscissas

Teorema do resto

Resto$(p(x), x - a) = p(a)$.

Teorema do fator

$a \in k$ é raiz de $p(x) \in k[x] \iff x - a$ divide $p(x)$.

PRÓXIMA AULA

Na próxima aula estudaremos a aritmética do anel de polinômios $k[x]$. Por meio do algoritmo da divisão, mostraremos que $k[x]$ é um domínio de ideais principais (DIP), isto é, todo ideal de $k[x]$ é principal. Isto acarretará na existência de MDC em $k[x]$ e no fato de $k[x]$ ser um domínio fatorial (DFU).

ATIVIDADES

ATIV. 2.1. Enuncie o algoritmo da divisão em $k[x]$.

ATIV. 2.2. Aplique o algoritmo da divisão para determinar polinômios $q(x)$ e $r(x)$ tais que $f(x) = q(x)g(x) + r(x)$ com $r(x) = 0$ ou $0 \leq \deg r(x) \leq \deg g(x)$.

a) $f(x) = x^3 + x - 1$, $g(x) = x^2 + 1$ em $\mathbb{R}[x]$.

b) $f(x) = x^5 - 1$, $g(x) = x - 1$ em $\mathbb{R}[x]$.

c) $f(x) = x^5 - x^3 + 3x - 5$, $g(x) = x^2 + 7$ em $\mathbb{Q}[x]$.

d) $f(x) = x^5 - x^3 + 3x - 5$, $g(x) = x - 2$ em $\mathbb{Q}[x]$.

e) $f(x) = x^5 - x^3 + 3x - 5$, $g(x) = x + 2$ em $\mathbb{Z}_5[x]$.

f) $f(x) = x^5 - x^3 + 3x - 5$, $g(x) = x^3 + x - 1$ em $\mathbb{Z}_3[x]$.

ATIV. 2.3. Sejam $f(x), g(x) \in \mathbb{Z}[x]$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$ onde $b_m = 1$. Mostre que existem $q(x), r(x) \in \mathbb{Z}[x]$ tais que $f(x) = q(x)g(x) + r(x)$ onde $r(x) = 0$ ou $0 \leq \deg\,(r(x) \leq \deg\, g(x)$.

ATIV. 2.4. Enuncie e demonstre os teoremas do resto e do fator.

ATIV. 2.5. Seja $\phi : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$ a função definida do seguinte modo:

$$\phi(a_0 + a_1x + \cdots + a_nx^n) = \overline{a}_0 + \overline{a}_1x + \cdots + \overline{a}_nx^n.$$

Mostre que ϕ é um homomorfismo sobrejetivo de anéis.

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.