Polinômios

Prof. Dr. Vinícius Wasques

Universidade Estadual Paulista "Júlio de Mesquita Filho" - Campus Rio Claro

13 de julho de 2020

Polinômios

Dado um anel comutativo K, definimos o anel comutativo $K[x]$ cujos elementos são da forma

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$$

com $a_i \in K$, por *polinômios* com coeficientes em K.

A soma e o produto em $K[x]$ são definidos da maneira usual:

$$f(x) + g(x) = \sum_i (a_i + b_i)x^i$$

$$f(x) \cdot g(x) = \sum_k \sum_{i+j=k} (a_ib_j)x^k$$

Definimos o grau $deg\ f(x)$ de um polinômio

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdot + a_n x^n$$

como sendo o maior valor i tal que $a_i \neq 0$.

Temos então as seguintes identidades para todos os polinômios $f(x), g(x) \in K[x]$:

$$deg\ (f(x).g(x)) = deg\ f(x) + deg\ g(x) \quad \text{e}$$

$$deg\ (f(x) + g(x)) \leq \max\{deg\ f(x), deg\ g(x)\}$$

Observação: Definimos o grau do polinômio nulo 0 por $-\infty$.

O coeficiente do termo de maior grau de um polinômio é chamado de coeficiente líder.

Um polinômio cujo coeficiente líder é igual a 1 é chamado de *mônico*.

Dado um polinômio $f(x) \in K[x]$, qualquer $c \in K$ tal que $f(c) = 0$ é chamado de raiz ou zero de $f(x)$.

Divisibilidade entre polinômios

Podemos definir divisibilidade de polinômios de maneira completamente análoga ao que fizemos para os números inteiros:

$d(x)|f(x)$ em $K[x]$ se, e só se, existe $g(x) \in K[x]$ tal que $f(x) = d(x) \cdot g(x)$.

Temos também uma generalização da divisão euclidiana:

Algoritmo da divisão para polinômios

Seja K um corpo. Dados polinômios $f(x), g(x) \in K[x]$, com $g(x) \neq 0$, existem $q(x), r(x) \in K[x]$ chamados respectivamente de quociente e resto da divisão de $f(x)$ por $g(x)$, unicamente determinados, tais que

$$f(x) = q(x) \cdot g(x) + r(x) \quad \text{com} \quad deg\ r(x) < deg\ g(x)$$

Dem: Exercício

Corolário

Seja K um corpo, $f(x) \in K[x]$ e $a \in K$. Então

$$x - a | f(x) \Leftrightarrow f(a) = 0.$$

Veja que para verificar esse fato, basta notar que como $deg(x-a) = 1$, dividindo f(x) por $x - a$ temos que

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

com $r \in K$.

Logo, substituindo x por a, temos que $f(a) = r$ podendo assim concluir o resultado.

Proposição

Seja K um corpo. Um polinômio $f(x) \in K[x]$ não nulo de grau n tem no máximo n raízes em K.

Dem: Utilize o princípio de indução para provar esse fato.

Seja K um corpo. Podemos considerar também congruências de polinômios em K[x]:

Sejam $a(x), b(x), m(x) \in K[x]$. Escrevemos

$$a(x) \equiv b(x) \ (mod \ m(x)) \Leftrightarrow m(x)|a(x) - b(x).$$

As mesmas demonstrações do caso dos números inteiros mostram que as congruências módulo m(x) definem uma relação de equivalência em $K[x]$ compatível com as operações de soma, subtração e produto.

Assim, podemos formar o anel quociente

$$\frac{K[x]}{(m(x))}$$

cujos elementos são da forma

$$\overline{a(x)} = \{b(x) \in K[x] | b(x) \equiv \ a(x) \ (mod \ m(x))\}$$

e as operações no anel quociente são dadas por

$$\overline{f(x)} + \overline{g(x)} = \overline{f(x) + g(x)} \quad \text{e}$$

$$\overline{f(x)} \cdot \overline{g(x)} = \overline{f(x) \cdot g(x)}$$

sendo independentes das escolhas dos representantes de classe f(x) e g(x).

Exemplo:

Determine o resto da divisão de $(x+1)^{2010}$ por x^2+x+1 em $\mathbb{Q}[x]$.

Exemplo:

Determine o resto da divisão de $(x+1)^{2010}$ por x^2+x+1 em $\mathbb{Q}[x]$.

Primeiro note que multiplicando por $x-1$ a congruência $x^2+x+1 \equiv 0 \ (mod\ x^2+x+1)$, obtemos

$$x^3-1 \equiv 0 \ (mod\ x^2+x+1) \quad \Rightarrow x^3 \equiv 1 \ (mod\ x^2+x+1).$$

Assim, temos o seguinte:

$$\begin{aligned} (x+1)^2 &\equiv x \ (mod\ x^2+x+1) \\ \Rightarrow (x+1)^{2010} &\equiv x^{1005} = (x^3)^{335} \ (mod\ x^2+x+1) \\ \Rightarrow (x+1)^{2010} &\equiv 1 \ (mod\ x^2+x+1) \end{aligned}$$

Portanto, o resto da divisão de $(x+1)^{2010}$ por x^2+x+1 é 1.

mdc entre polinômios

Definimos o mdc de f(x) e g(x) como sendo o polinômio mônico de maior grau que divide f(x) e g(x), simultaneamente.

Exemplo: $mdc(2x^2 - 2, x^2 + 2x + 1) = x + 1$

Note que

$$2x^2 - 2 = (2x - 2)(x + 1)$$

e

$$x^2 + 2x + 1 = (x + 1)(x + 1).$$

mmc entre polinômios

Definimos o mmc de f(x) e g(x) como sendo o polinômio mônico de menor grau que é divisível tanto por f(x) como por g(x).

Exemplo: $mmc(2x+4, x^2-1) = x^3+2x^2-x-2$

Note que a multiplicação entre $f(x)$ e $g(x)$ não necessariamente produz o mmc, como é o caso acima.

Qualquer função $h(x) = p(x)(x^3+2x^2-x-2)$ é um múltiplo de $f(x)$ e $g(x)$, em particular para $p(x) = 2$ que é exatamente o produto entre $f(x)$ e $g(x)$.

Teorema de Bachet-Bézout para polinômios

Seja d(x) o máximo divisor comum de dois polinômios f(x) e g(x). Então existem dois polinômios m(x) e n(x) tais que

$$f(x)m(x) + g(x)n(x) = d(x).$$

Dem: Exercício.

Dica: Utilize os mesmos passos do Teorema de Bachet-Bézout para os números inteiros, sendo $d(x)$ o polinômio mônico de menor grau no conjunto

$$I(f, g) = \{f(x)m(x) + g(x)n(x) | m(x), n(x) \in K[x]\}.$$

Polinômio irredutível

Seja K um corpo. Dizemos que um polinômio não constante $f(x) \in K[x]$ é *irredutível* em K[x] se f(x) não é o produto de dois polinômios em K[x] de graus estritamente menores do que $deg\ f(x)$.

Polinômios irredutíveis fazem o papel de números primos para polinômios.

Exemplo:

O polinômio $x^2+1 \in \mathbb{R}[x]$ é irredutível em $\mathbb{R}[x]$, pois caso contrário poderia ser escrito como produto de polinômios de grau 1 em $\mathbb{R}[x]$, contradizendo o fato de $x^2+1=0$ não possuir raízes reais.

Observação: Note que x^2+1 é *redutível* em $\mathbb{C}[x]$ já que $x^2+1=(x-i)(x+i)$. Portando, irredutibilidade é um conceito que depende do anel de polinômios sobre o qual estamos trabalhando.

Corpo algebricamente fechado

Os exemplos mais evidentes de polinômios irredutíveis em K[x] são os da forma $x - a, a \in K$.

Quando estes são os únicos polinômios irredutíveis em K[x] dizemos que o corpo K é *algebricamente fechado*.

Teorema

Seja K um corpo e f(x) um polinômio irredutível em K[x]. Então

$$\frac{K[x]}{(f(x))}$$

é um corpo.

Demonstração

Aqui mostraremos apenas que todo $\overline{a(x)} \neq 0$ é invertível em $\frac{K[x]}{(f(x))}$.

Por hipótese temos que $mdc(a(x), f(x)) = 1$ uma vez que f(x) é irredutével em $k[x]$ e, além disso, f(x) não divide a(x), pois caso contrário teríamos $\overline{a(x)} = 0$.

Logo, pelo teorema de Bachet-Bézout, existem $r(x), s(x) \in K[x]$ tais que

$$a(x)r(x) + f(x)s(x) = 1 \Leftrightarrow a(x)r(x) \equiv 1 \ (mod\ f(x))$$

Portanto $\overline{r(x)}$ é o inverso multiplicativo de $\overline{a(x)}$.

Exemplo:

Seja $K = \mathbb{Z}_2$ e $f(x) = x^2 + x + \overline{1} \in K[x]$.

Temos que f(x) é irredutível pois ele tem grau 2 e não possui raízes em K.

Assim, $\frac{K[x]}{(f(x))}$ é um corpo, que possui os seguintes elementos:

$$\frac{K[x]}{(f(x))} = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$$

Polinômios primitivos

Um polinômio não nulo $f(x) \in \mathbb{Z}[x]$ é dito primitivo se o mdc de seus coeficientes é 1.

Exemplo: $f(x) = x^2 + 10x - 3$ é um polinômio primitivo, pois seus coeficientes são primos dois a dois.

Lema. O produto de dois polinômios primitivos é primitivo.

Proposição. Seja K um corpo. Então todo polinômio não nulo em $K[x]$ pode ser fatorado como um produto de polinômios irredutíveis em K[x]. Tal fatoração é única a menos da ordem dos fatores e multiplicação por constantes não nulas.

Demonstre o Lema e a Proposição acima.

Lema de Gauss

Seja $f(x) \in \mathbb{Z}[x]$ um polinômio primitivo não constante. Então f(x) é irredutível em $\mathbb{Q}[x]$ se, e somente se, f(x) é irredutível em $\mathbb{Z}[x]$.

Em outras palavras, o Lema de Gauss garante que não podemos escrever $f(x) = g(x)h(x)$ com $g(x), h(x) \in \mathbb{Z}[x]$ não constantes.

Demonstração

A implicação ($\Rightarrow$) é imediata, uma vez que $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$.

($\Leftarrow$) Reciprocamente, suponha por contradição que $f(x)$ seja irredutível sobre $\mathbb{Z}[x]$ mas que $f(x) = g(x)h(x)$ com $g(x), h(x) \in \mathbb{Q}[x]$, ambos não constantes.

Multiplicando esta última igualdade por um inteiro conveniente $d > 0$, podemos escrever

$$d \cdot f(x) = e \cdot g_0(x)h_0(x)$$

com $g_0(x), h_0(x) \in \mathbb{Z}[x]$ primitivos e $e \in \mathbb{N}$.

Pelo Lema anterior temos que $g_0(x)h_0(x)$ é um polinômio primitivo.

Como $f(x)$ também é primitivo, temos que d é o mdc dos coeficientes de $d \cdot f(x)$, enquanto que e é o mdc dos coeficientes de $e \cdot g_0(x)h_0(x)$.

Logo $d = e$ e assim $f(x) = g_0(x)h_0(x)$ é redutível sobre $\mathbb{Z}[x]$, chegando em uma contradição.

Portanto, segue que $f(x)$ seja irredutível sobre $\mathbb{Q}[x]$.

Critério de Eisenstein

Seja $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ um polinômio primitivo não constante. Suponha que exista um número primo p tal que

$p \nmid a_n$,

$p | a_j$ para todo $0 \leq j < n$

e $p^2 \nmid a_0$.

Então $f(x)$ é irredutível em $\mathbb{Z}[x]$.

Demonstração

Suponha por absurdo que $f(x)$ é redutível, isto é, existem $g(x), h(x) \in \mathbb{Z}[x]$ tais que $f(x) = g(x)h(x)$ com $0 < deg\ g(x), deg\ h(x) < n$.

Em $\mathbb{Z}_p$, temos $\overline{f(x)} = \overline{g(x)} \cdot \overline{h(x)}$.

Como $p|a_j$ para todo $0 \leq j < n$, segue que $\overline{f}(x) = \overline{a_n}x^n$ e portanto, pela fatoração única em $\mathbb{Z}_p$, devemos ter $g(x) = \overline{b}x^i$ e $h(x) = \overline{c}x^j$ com $0 < i, j < n$, $i + j = n$ e $\overline{b \cdot c} = \overline{a_n}$.

Mas isto significa que os coeficientes de x^0 em $g(x)$ e $h(x)$ são múltiplos de p, e portanto a_0 é múltiplo de p^2, uma vez que $f(x) = g(x)h(x)$. Chegamos então em um absurdo.

Observação

O Lema de Gauss nos diz que verificar a irredutibilidade de um polinômio primitivo em $\mathbb{Q}[x]$ é equivalente a verificar a irretubilidade do mesmo em $\mathbb{Z}[x]$.

Sendo assim, o critério de Eisenstein também pode ser utilizado para verificar a irredutibilidade de polinômios primitivos em $\mathbb{Q}[x]$.

Exemplo: Pelo critério de Eisenstein temos que o polinômio primitivo $f(x) = x^2 + x + 1$ é irredutível em $\mathbb{Z}[x]$. Pelo Lema de Gauss, garantimos que $f(x)$ também é irredutível em $\mathbb{Q}[x]$.

Referências

MARTINEZ, F.E.B; MOREIRA, C.G.T; SALDANHA, N.,T.; TENGAN, E. Teoria dos Números. Um passeio com Primos e outros Números Familiares pelo Mundo Inteiro. IMPA, 2013.

GRAHAM, R. L., KNUTH, D. E., PATASHNIK, O
Matemática Concreta. LTC, São Paulo, 1995

NIVEN, I. E.; ZUCKERMAN, N.S. An Introduction to the Theory of Numbers, NY, John Wiley & Sons, 1991.

Contato

Prof. Dr. Vinícius Wasques

email: viniciuswasques@gmail.com

Departamento de Matemática

site: `https://viniciuswasques.github.io/home/`