AULA

3

Teoria da divisibilidade Em $k[x]$

META:

Obter a propriedade de fatoração única para anéis de polinômios definidos sobre corpos.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:

Estabelecer os principais conceitos da teoria de divisibilidade para anéis de polinômios: unidades, divisores, divisor de zero, associados, irredutíveis, primos, máximo divisor comum e elementos relativamente primos.

Descrever a estrutura dos ideais em $k[x]$.

Usar os fatos de $k[x]$ ser DIP e DFU na solução de problemas na teoria de polinômios.

Aplicar o algoritmo de Euclides no cálculo de MDC de polinômios.

Expressar o MDC$(f(x), g(x))$ como combinação linear de $f(x)$ e $g(x)$.

Relacionar o MDC$(f(x), g(x))$ e o gerador do ideal gerado por $f(x)$ e $g(x)$.

PRÉ-REQUISITOS

Algoritmo da divisão em $k[x]$. Uma revisão da teoria da divisibilidade em $\mathbb{Z}$ ajudaria na compreensão desta aula.

3.1 Introdução

Prezado aluno, você deve estar familiarizado com a aritmética dos inteiros. A aritmética de $k[x]$, k corpo, é notavelmente semelhante à de $\mathbb{Z}$. Ambos admitem um algoritmo de divisão, máximo divisor comum e fatoração única em primos.

O "'set up"' da aritmética de um anel A reside na noção de divisibilidade: dados $a, b \in A$ dizemos que b divide a se existe $c \in A$ tal que $a = bc$. Desta noção, define-se: unidades, divisores de zero, elementos associados, elementos irredutíveis, elementos primos, mínimo múltiplo comum e máximo divisor comum. Por isso, num nível mais elementar a aritmética é, por vezes, chamada teoria de divisibilidade. Por outro lado, qualquer noção fundamentada na definição de divisibilidade pode ser interpretada via a noção de ideais principais. Para se ter uma idéia, um elemento a é dito associado a $b \overset{\text{def}}{\leftrightarrow} a|b$ e $b|a \leftrightarrow (a) = (b)$ onde $(x) = \{ax \mid a \in A\}$ denota o ideal principal gerado por x. Assim, em DIP's, aritmética, teoria de divisibilidade e estudo dos ideais principais são equivalentes e o uso de um dos termos depende apenas do ponto de vista. O primeiro reflete o da teoria dos números enquanto que o último o da álgebra abstrata. Esta aula trata justamente da teoria de divisibilidade do anel de polinômios em uma indeterminada sobre um corpo k. A idéia central é fazer um paralelo com a teoria já conhecida dos inteiros.

Na seção 3.2 são apresentadas as definições necessárias para a leitura do capítulo corrente. Sem tê-las em mente fica impossível compreender as idéias contidas neste capítulo. É aconselhável que num primeiro contato com álgebra, a cada palavra que remonte à uma definição, o aluno pare a leitura e relembre mentalmente a definição a fim de certifica-se que sua leitura esteja sendo ativa e

não meramente como a de um romance.

Na seção 3.3 descreveremos a estrutura dos ideais em $k[x]$. Mostraremos que todo ideal em $k[x]$ é principal, isto é, $k[x]$ é DIP. Finalmente, na seção 3.4 mostraremos a existência de MDC em $k[x]$ através do algoritmo de Euclides também conhecido como algoritmo das divisões sucessivas. Tal algoritmo ainda nos permite escrever o MDC como uma combinação dos fatores.

3.2 Glossário

1. **Divisibilidade:** um elemento $b \in A$ divide um elemento $a \in A$ em A se existe $c \in A$ tal que $a = bc$. Neste caso, diz-se também que a é múltiplo de b, b é divisor de a ou b é um fator de a.

2. **Unidade:** divisor da identidade; elemento $a \in A$ tal que $ab = 1_A$ para algum $binA$; elemento $a \in A$ para o qual a equação $ax = 1_A$ admite solução em A. Em um anel não trivial ($1_A \neq 0_A$) toda unidade é não nula. Pode-se mostrar que o elmento $b \in A$ tal que $ab = 1_A$ é único. Este elemento é chamado inverso de a e denotado por a^{-1}. Denotaremos por $\mathbb{U}(A)$ ao conjunto das unidades em A. (Exemplo: $\mathbb{U}(\mathbb{Z}_n) = \{\overline{x} \ : mdc(x, n) = 1\}$)

3. **Inversível:** o mesmo que unidade.

4. **Divisor de zero:** elemento $a \in A$ tal que existe elemento não nulo $b \in A$ tal que $ab = 0$; elemento $a \in$ para o qual a equação $ax = 0$ admite solução não trivial ($\neq 0$); elemento $a \in A$ tal que o endomorfismo $A \to A$, $x \mapsto ax$ admite núcleo não trivial (equivalentemente, é não injetivo).

5. **Nilpotente:** elemento $a \in A$ para o qual existe inteiro positivo n tal que $a^n = 0$. O menor inteiro positivo n tal que $a^n = 0$ é chamado *índice de nilpotência*.

6. **Elementos associados:** elementos $a, b \in A$ tais que $a|b$ e $b|a$. Em domínios, isto é equivalente a dizer que $a = ub$ para alguma unidade $u \in A$.

7. **Divisor trivial:** unidades e associados à um elemento.

8. **Divisor próprio:** divisor não trivial de um elemento. Exemplo: $\mathbb{U}(\mathbb{Z}_{12}) = \{1, 5, 7, 11\}$. Logo, 2 é um divisor trivial de 10 pois é um de seus associados. Por outro lado, 3 é divisor próprio de 6 pois 3|6 com 3 não unidade e nem associado de 6.

9. **Elemento irredutível:** elemento não unidade $a \in A$ cujos divisores são seus associados ou unidades.

10. **Elemento redutível:** elemento não unidade que não é irredutível. Em outras palavras, elemento que possui divisores próprios.

11. **Elemento primo:** elemento não unidade $p \in A$ para o qual vale a seguinte propriedade: $p|ab \Rightarrow p|a$ ou $p|b$.

12. **Máximo divisor comum (MDC):** o máximo divisor comum de $a_1, \ldots, a_r \in A$ (não todos nulos) é um elemento $d \in A$ tal que

    i) $d|a_i$ para todo i, $1 \leq i \leq r$.

    ii) Se $c \in A$ divide cada a_i então $c|d$.

13. **Elementos relativamente primos:** Elementos cujo MDC é 1.

14. **Domínio de fatoração única (DFU):** domínio A no qual todo elemento não nulo e não unidade $a \in A$ satisfaz as seguintes condições:

    i) $a = p_1, \cdots p_r$, $p_i \in A$ irredutível para todo i, $1 \leq i \leq r$.

    ii) Se $a = q_1 \cdots q_s$ é uma outra fatoração com cada q_i irredutível então $r = s$ e, a menos de uma reordenação nos índices, p_i é associado à q_i para cada i, $1 \leq i \leq r$.

15. **Domínio de ideais principais (DIP):** domínio no qual todo ideal é principal.

16. **Domínio Euclidiano:** domínio A no qual está definido uma função $\delta : A^* \to \mathbb{Z}_{\geq 0}$ satisfazendo as seguintes propriedades:

    i) Se $a, b \in A$ são não nulos então $\delta a \leq \delta(ab)$.

    ii) Se $a, b \in A$ e $b \neq 0$ então existem $q, r \in A$ tais que $a = bq + r$ com $r = 0$ ou $0 \leq \delta(r) \leq \delta(b)$. Exemplo: a função módulo juntamente com o algoritmo da divisão em $\mathbb{Z}$ define em $\mathbb{Z}$ uma estrutura de domínio euclidiano. A notação A^* indica o conjunto dos elementos não nulos de A e $\mathbb{Z}_{\geq 0}$ é o conjunto dos inteiros não negativos.

3.3 Ideais em $k[x]$

Um ideal de um anel A é um subconjunto $I \subset A$ tal que $(I, +)$ é subgrupo aditivo de $(A, +)$ e $ax \in I$ sempre que $a \in A$ e $x \in I$. Um ideal $I \subset A$ é dito principal se $I = (a)$ para algum $a \in A$ onde $(a) = \{ax : x \in A\}$.

Teorema 3.1. *$k[x]$ é DIP.*

Prova: Seja $I \subset k[x]$ um ideal. Se $I = (0)$ é o ideal nulo nada temos a provar. Suponhamos I não nulo. Considere o conjunto

$$S = \{ \deg f \ : \ f \in I\}$$

Desde que $I \neq 0$, existe $f \in I$, $f \neq 0$. Então, $S \subset \mathbb{Z}_{\geq 0}$ é não vazio. Pelo Princípio da Boa Ordem existe $f(x) \in I$ tal que deg f é mínimo dentre os graus de todos os polinômios em I. Vamos mostrar que $I = (f(x))$. A inclusão $(f(x)) \subset I$ segue da definição de ideal visto que $f(x) \in I$. Seja $g(x) \in I$. Pelo algoritmo da divisão, existem $q(x), r(x) \in k[x]$ tais que

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

com $r(x) = 0$ ou $0 \leq \deg\ r(x) < \deg\ f(X)$. Ora, se $r(x) \neq 0$ então $r(x) = g(x) - q(x)f(x) \in I$ (pois $g(x), q(x)f(x) \in I$) com deg $r(x) <$ deg $f(x)$. Isto contradiz a minimalidade de deg $f(x)$. Logo, $r(x) = 0$ e $g(x) = q(x)f(x) \in (f(x))$. Assim, $I \subset (f(x))$ donde $I = (f(x))$.

3.4 MDC em $k[x]$

A existência de MDC em $k[x]$ é uma consequência direta do fato de $k[x]$ ser DIP.

Teorema 3.2. (Existência de MDC) *Sejam $f(x), g(x) \in k[x]$. Então, MDC$(f(x), g(x))$ existe e é único a menos de um produto por uma constante não nula em k.*

Prova: Considere $(f(x), g(x)) \subset k[x]$ o ideal gerado por $f(x)$ e $g(x)$. Desde que $k[x]$ é DIP, existe $d(x) \in k[x]$ tal que $(d(x)) = (f(x), g(x))$. Vamos mostrar que $d(x) = \text{MDC}(f(x), g(x))$. Primeiramente, $d(x)|f(x)$ e $d(x)|g(x)$ pois, $f(x), g(x) \in (f(x), g(x)) =$

$(d(x))$. Suponha $h(x) \in k[x]$ tal que $h(x)|f(x)$ e $h(x)|g(x)$. Então, $f(x) = h(x)q_1(x)$ e $g(x) = h(x)q_2(x)$. Desde que $d(x) \in (f(x), g(x))$ existem $r(x), s(x) \in k[x]$ tais que $d(x) = r(x)f(x) + s(x)g(x)$. Logo,

$$\begin{aligned} d(x) &= r(x)f(x) + s(x)g(x) \\ &= r(x)h(x)q_1(x) + s(x)h(x)q_2(x) \\ &= h(x)\left[r(x)q_1(x) + s(x)q_2(x)\right] \end{aligned}$$

donde $h(x)|d(x)$. Resta mostrar a unicidade a menos de uma multiplicação por uma constante não nula. Suponham $d_1(x), d_2(x)$ sob as condições de serem um máximo divisor comum de $f(x)$ e $g(x)$. Por definição de MDC segue que $d_1(x)|d_2(x)$ e $d_2(x)|d_1(x)$. Logo, $d_1(x) \sim d_2(x)$ donde $d_1(x) = ud_2(x)$ com $u \in \mathbb{U}(k[x]) = k \setminus 0$. □

OBS 3.1. O teorema acima nos mostra que o MDC de dois polinômios $f, g \in k[x]$ é um gerador do ideal (f, g). Embora este resultado tenha relevância teórica ele não nos ensina como obter o MDC de $f(x)$ e $g(x)$. A rigor, deveríamos determinar o polinômio de menor grau escrito como combinação linear de $f(x)$ e $g(x)$. Na prática, isto torna-se impraticável. Felizmente, existe um algoritmo clássico, conhecido como Algoritmo Euclidiano, para computar o MDC de dois polinômios. Este algoritmo é fundamentado no resultado a seguir.

Lema 3.1. *Sejam $f(x), g(x) \in k[x]$. Se $f(x) = q(x)g(x) + r(x)$ com $q(x), r(x) \in k[x]$ então $MDC(f(x), g(x)) = MDC(g(x), r(x))$.*

Prova: Usaremos noções de ideais e a verificação das inclusões ficarão como exercícios. A relação $f(x) = q(x)g(x) + r(x)$ fornece-nos as inclusões de ideais $(f) \subset (g, r)$ e $(r) \subset (f, g)$. Logo,

$(f,g) \subset (g,r) \subset (f,g)$. Assim, $(\text{MDC}(f,g)) = (f,g) = (g,r) = (\text{MDC}(g,r))$ donde $\text{MDC}(f,g) = \text{MDC}(g,r)$. $\square$
Eis o Algoritmo Euclidiano para computar $\text{MDC}(f,g)$:

Input: f, g
Output: h
$h := f$
$s := g$
Enquanto $s \neq 0$ faça

$r :=$ resto (h, s)

$h := s$

$s := r$

Caso o leitor não tenha visualizado, este algoritmo é aquele visto no ensino fundamental e chamado método das divisões sucessivas. De fato, dados $f, g \in k[x]$, $g \neq 0$, o algoritmo nos fornece:

Passo	Resultado
0	$h_0 = f$, $s_0 = g$ e $f = q_0 g + r_0$, $r_0 = \text{resto}(f,g)$.
1	$h_1 = s_0 = g$, $s_1 = r_0$ e $g = q_1 r_0 + r_1$, $r_1 = \text{resto}(g, r_0)$.
2	$h_2 = r_0$, $s_2 = r_1$ e $r_0 = q_2 r_1 + r_2$, $r_2 = \text{resto}(r_0, r_1)$.
3	$h_3 = r_1$, $s_3 = r_2$ e $r_1 = q_3 r_2 + r_3$, $r_3 = \text{resto}(r_1, r_2)$.
	$\vdots$

Pela propriedade do resto, tem-se uma sequência estritamente decrescente de inteiros não negativos

$$\deg r_0 > \deg r_1 > \deg r_2 > \ldots.$$

Usando o princípio da boa ordem pode-se mostrar (verifique!) que em algum passo, necessariamente, deveremos ter um resto nulo, digamos no passo $n+1$. Deste modo,

Passo	Resultado
n	$h_n = r_{n-2}$, $s_n = r_{n-1}$ e $r_{n-2} = q_n r_{n-1} + r_n$.
$n+1$	$h_{n+1} = r_{n-1}$, $s_{n+1} = r_n$ e $r_{n-1} = q_{n+1} r_n + 0$.

onde $r_{n+1} = \text{resto}(r_{n-1}, r_n) = 0$. Pelo Lema 3.1, $\text{MDC}(f,g) = \text{MDC}(g, r_0) = \text{MDC}(r_0, r_1) = \ldots = \text{MDC}(r_{n-1}, r_n) = \text{MDC}(r_n, 0) = r_n$.

OBS 3.2. Outra propriedade também importante de tal algoritmo é que nos permite expressar o $\text{MDC}(f,g)$ como uma combinação linear entre f e g. De fato, basta retroceder aos passos do algoritmo para determinar $r, s \in k[x]$ tais que $\text{MDC}(f,g) = rf + sg$. Vejamos um exemplo para ilustrar tais idéias.

Exemplo 3.1. Vamos calcular o MDC entre $f(x) = x^4 - x^3 - x^2 + 1$ e $g(x) = x^3 - 1$ e expressá-lo como uma combinação linear de $f(x)$ e $g(x)$. Seguindo os passos do algoritmo obtém-se:

$$x^4 - x^3 - x^2 + 1 = (x-1)(x^3-1) - x^2 + x \quad (3.1)$$

$$x^3 - 1 = (-x-1)(-x^2+x) + x - 1 \quad (3.2)$$

$$-x^2 + x = -x(x-1) \quad (3.3)$$

Assim, $\text{MDC}\,(f(x), g(x)) = x - 1$. Vamos agora expressar o MDC obtido como combinação linear de $f(x)$ e $g(x)$. Isolando $x - 1$ na equação 3.2 tem-se:

$$x - 1 = x^3 - 1 - (-x-1)(-x^2+x) \quad (3.4)$$

Por outro lado, isolando $-x^2 + x$ na equação 3.1 e substituindo na equação 3.4 obtém-se:

$$\begin{aligned} x-1 &= x^3-1-(-x-1)(-x^2+x) \\ &= x^3-1-(-x-1)\left[x^4-x^3-x^2+1-(x-1)(x^3-1)\right] \\ &= [1+(-x-1)(x-1)]\,(x^3-1)- \\ &\quad (-x-1)(x^4-x^3-x^2+1) \\ &= (-x^2+2)(x^3-1)+(x+1)(x^4-x^3-x^2+1) \end{aligned}$$

3.5 MDC $\not\Rightarrow$ DIP

Em geral, todo DIP admite MDC. Neste exemplo, mostraremos que a recíproca não é verdadeira por exibir um anel com MDC que não é DIP. Considere $\mathbb{Z}[x]$ e $2, x \in \mathbb{Z}[x]$. Vamos mostrar que o ideal $(2, x)$ não é principal. Suponha, por absurdo, que existe $p(x) \in \mathbb{Z}[x]$ tal que $(2, x) = (p(x))$. Então, existiriam $r(x), s(x) \in \mathbb{Z}[x]$ tais que

$$p(x) = r(x).2 + s(x).x$$

Por outro lado $2 \in (2, x) = (p(x))$ donde $2 = p(x)q_1(x)$. Assim, $0 = \deg 2 = \deg p(x) + \deg q_1(x)$ donde $\deg p(x) = 0$. Logo, $p(x) = c \in \mathbb{Z}$ é um polinômio constante. Analogamente, $x = p(x)q_2(x)$ para algum $q_2(x) \in \mathbb{Z}[x]$. Assim, $1 = \text{LC } x = c.\text{LC } q_2(x)$ (onde LC denota o coeficiente líder). Conclusão: $c \in \mathbb{U}(\mathbb{Z}) = \{\pm 1\}$ (onde $\mathbb{U}(A)$ denota o conjunto das unidades de A). Podemos considerar $c = 1$ (Por quê?). Assim,

$$1 = p(x) = r(x).2 + s(x).x$$

Isto é um absurdo (você sabe por quê?). Logo, tal $p(x)$ não existe.

OBS 3.3. O domínio $\mathbb{Z}[x]$ não é um DIP. Mas, pode-se mostrar se A é DFU então $A[x]$ é DFU (a prova disto está além das pretensões

deste texto!). Como $\mathbb{Z}$ é DFU então $\mathbb{Z}[x]$ é DFU. Logo, admite MDC. Seja $d(x) = \text{MDC } (2, x)$ (você saberia mostrar que $d(x) = 1$?). Por definição de MDC, $(2, x) \subset (d(x)) = (1) = \mathbb{Z}[x]$ mas $d(x) = 1 \notin (2, x)$, pois $(2, x)$ não é principal. Assim, MDC $(2, x)$ não pode ser escrito como combinação linear de 2 e x.

3.6 Irredutíveis e Fatoração única em $k[x]$

Seja A um anel. Lembramos que um elemento $a \in A$ é dito irredutível se não admite divisores próprios. Em outras palavras, se $b|a$ então ou b é unidade ou $b \sim a$. No caso de domínios, $a \sim b$ se e somente se $a = ub$ com u uma unidade. Em nosso caso, $k[x]$ é domínio. Então, dizer que $p(x)$ é associado a $q(x)$ é equivalente a dizer que $p(x) = cq(x)$ para algum $c \in k$, isto é, $p(x)$ e $q(x)$ diferem por uma constante. Comecemos por investigar os elementos irredutíveis de $k[x]$. Mostraremos que polinômios irredutíveis são elementos primos em $k[x]$ - esta é uma condição básica para um anel ser DFU. Precisaremos do seguinte fato elementar visto em Estruturas Algébricas I: em um domínio euclidiano A (ou em que vale o algoritmo euclidiano) se $a|bc$ e MDC $(a, b) = 1$ então $a|c$ (você sabe provar isto?).

Lema 3.2. *Irredutíveis em $k[x]$ são elementos primos.*

Prova: Seja $p(x) \in k[x]$ irredutível. Pela definição de elemento primo, devemos mostrar que se $p(x)|f(x)g(x)$ então $p(x)|f(x)$ ou $p(x)|g(x)$. Suponha $p(x)|f(x)g(x)$ com $p(x) \not| f(x)$. Por definição de irredutível, o fato de $p(x)$ não dividir $f(x)$ implica que $p(x)$ e $f(x)$ são relativamente primos. Assim, $p(x)|f(x)g(x)$ com MDC $(p(x), f(x)) = 1$. Então, $p(x)|g(x)$ como queríamos demonstrar. □

OBS 3.4. Pelo lema acima, se $p(x)$ é irredutível e $p(x)$ divide o produto $q_1(x)\cdots q_r(x)$ então $p(x)$ divide um dos fatores $q_i(x)$ para algum i, $1 \leq i \leq r$ (pode-se provar isto usando-se recursivamente o lema ou por indução no número de fatores). Deste modo, sempre que tivermos $p_1(x), \ldots, p_r(x)$ e $q_1(x), \ldots, q_s(x)$ irredutíveis com

$$p_1(x)\cdots p_r(x) = q_1(x)\cdots q_s(x)$$

poderemos supor $p_1|q_1$ a menos de uma permutação nos índices.

Teorema 3.3. *(Fatoração única em $k[x]$) Seja k um corpo. Todo polinômio não constante $f(x) \in k[x]$ é um produto de polinômios irredutíveis em $k[x]$. Esta fatoração é única a menos de uma constante não nula, isto é, se*

$$f(x) = p_1(x)\cdots p_r(x) \quad e \quad f(x) = q_1(x)\cdots q_s(x)$$

são duas fatorações em irredutíveis de $f(x)$ então $r = s$ e, a menos de uma permutação nos índices, $p_i = u_i q_i$ com $u_i \in k$, $u_i \neq 0$, para todo i, $1 \leq i \leq r$.

Prova: (Existência) Seja $f(x) \in k[x]$ um polinômio não constante. Usaremos indução em $\deg f(x) = n \geq 1$. Se $\deg f(x) = 1$ então $f(x)$ é irredutível (todo polinômio de grau 1 é irredutível). Suponhamos o teorema verdadeiro para todo polinômio de grau $< n$. Se $f(x)$ é irredutível então nada temos a provar pois $f(x) = 1.f(x)$ que um produto de irredutíveis com somente um fator (permissível em nosso contexto). Se $f(X)$ é redutível então, por definição, $f(x) = g(x)h(x)$ com $\deg g(x) < n$ e $\deg h(x) < n$. Por hipótese indutiva, $g(x) = u_1 p_1 \cdots p_r$ e $h(x) = u_2 p_{r+1} \cdots p_k$ com $u_1, u_2 \in k$. Pondo $u = u_1 u_2$ temos $f(x) = u p_1 \cdots p_k$ como queríamos.
(Unicidade) Sejam $f(x) = u_1 p_1 \cdots p_r$ e $f(x) = u_2 q_1 \cdots q_s$ duas

fatorações de f em irredutíveis. Se $r \neq s$ podemos supor, sem perda de generalidade, $r < s$. Então, a menos de uma permutação nos índices, $p_1 \sim q_1$, $p_2 \sim q_2$, $\ldots$, $p_r \sim q_r$. Assim, $p_1 \cdots p_r = cq_1 \cdots q_r q_{r+1} \cdot q_s$ donde $q_{r+1} \cdots q_s = u \in k$ donde $q_{r+1}, \ldots, q_s$ são unidades. Isto contradiz a irredutibilidade de $q_{r+1}, \ldots, q_s$. Logo, $r = s$ e $p_i \sim q_i$ para todo i, $1 \leq i \leq r$. $\square$

3.7 Irredutibilidade *versus* raízes de funções polinomiais

As noções de irredutibilidade e zeros de funções polinomiais são antagônicas. Para que um polinômio (de grau > 1) seja irredutível sobre um corpo k não é suficiente mas é necessário que ele não admita raízes em k (teorema do fator). Em linguagem simbólica:

$$\text{irredutibilidade sobre } k \Rightarrow \text{ não existência de raízes em } k.$$

A recíproca não é verdadeira. Considere dois polinômios quadráticos $f(x), g(x) \in \mathbb{R}[x]$ sem raízes em $\mathbb{R}$. Então, $h(x) = f(x)g(x)$ não admite raízes reais e, no entanto, é redutível.
A não equivalência da implicação acima não a desfavorece teoricamente. Sua contrapositiva é de grande utilidade teórica e nos fornece um critério de redutibilidade para polinômios de grau ≤ 2. É importante também ressaltar que para polinômios de grau 2 e 3 a implicação acima torna-se uma equivalência. Todas estas observações são decorrentes dos teoremas do resto e do fator.

3.8 Conclusão

Estruturalmente, a teoria da divisibilidade em $k[x]$, k corpo, é idêndica à de $\mathbb{Z}$. Ambos são domínios euclidianos. Apenas a função

norma difere. Em $\mathbb{Z}$ é dada pela função módulo $a \mapsto |a|$ e em $k[x]$, pela função grau $f(x) \mapsto \deg f(x)$. Consequentemente, tanto a teoria de ideais quanto a existência e o cálculo do MDC também são idênticos. Em geral, todo domínio euclidiano é um DIP e admite MDC.

RESUMO

Ideais em $k[x]$

$$\boxed{I \subset k[x] \text{ ideal} \Rightarrow I = (f(x)) \text{ para algum } f(x) \in k[x]}$$

O elemento $f(x)$ que gera o ideal I é um polinômio de menor grau em I.

MDC em $k[x]$

$$\boxed{k[x] \text{ DIP} \Rightarrow \text{Existe MDC em } k[x]}$$

De fato, todo gerador de um ideal não nulo $(f(x), g(x))$ (existe pois $k[x]$ é DIP) é um MDC de $f(x)$ e $g(x)$. A recíproca é também verdadeira para domínios euclidianos. Deste modo, em domínios euclidianos, embora o MDC não seja único, quaisquer dois são associados. Assim, em $k[x]$, existe um único MDC mônico. Alguns textos definem o MDC em $k[x]$ como este representante mônico nesta classe de equivalência e garante, já na definição, a unicidade do MDC.

Algoritmo Euclidiano

Input: f, g

Output: h

$h := f$

$s := g$

Enquanto $s \neq 0$ faça

$r :=$ resto (h, s)

$h := s$

$s := r$

Quadro comparativo entre a teoria de divisibilidade de $\mathbb{Z}$, $k[x]$ e $\mathbb{Z}[x]$.

$\mathbb{Z}$	$k[x]$	$\mathbb{Z}[x]$
Comutativo	Sim	Sim
Com identidade	Sim	Sim
Domínio	Sim	Sim
Euclidiano	Sim	**Não**
DIP	Sim	**Não**
DFU	Sim	Sim
$\exists$ MDC	Sim	Sim
MDC pode ser escrito como combinação linear	Sim	**Não**

OBS 3.5. Em geral, tem-se as seguintes inclusões (todas próprias):

Domínios euclidianos $\subset$ DIP $\subset$ DFU.

Irredutibilidade *versus* raízes de funções polinomiais

irredutibilidade sobre $k \Rightarrow$ não existência de raízes em k.

A recíproca não é verdadeira: x^2+1 não possui raízes reais donde $(x^2+1)^2$ também não possui raízes reais, mas é redutível. Contudo, vale a recíproca para polinômios de grau 2 e 3.

Fatoração única em $k[x]$

$$k \text{ corpo } \Rightarrow k[x] \text{ DFU}$$

PRÓXIMA AULA

Focalizaremos o estudo de irredutibilidade no anel de polinômios definidos sobre o corpo dos racionais. Mostraremos que a irredutibilidade em $\mathbb{Z}[x]$ é suficiente para a irredutibilidade em $\mathbb{Q}[x]$.

ATIVIDADES

ATIV. 3.1. Classifique e caracterize os elementos em $k[x]$ quanto a cada definição dada no glossário.

ATIV. 3.2. Mostre que a noção de elementos associados define uma relação de equivalência em $k[x]$. Verifique que para cada classe de equivalência existe um único representante mônico.

ATIV. 3.3. Determine todos os polinômios irredutíveis de grau 2 e 3 em $\mathbb{Z}_2[x]$.

ATIV. 3.4. Calcule MDC $(f(x), g(x))$ em $\mathbb{Q}[x]$ para os pares de polinômios nos itens abaixo. Expresse o MDC como combinação linear entre os pares de polinômios dados.

a) $f(x) = x^3 - 6x^2 + x + 4$; $g(x) = x^5 - 6x + 1$.

b) $f(x) = x^2 + 1$; $g(x) = x^6 + x^3 + x + 1$.

ATIV. 3.5. Mostre que o MDC é único a menos de um fator constante não nulo. Em outras palavras, mostre que $d_1(x), d_2(x)$ são MDC de $f(x)$ e $g(x)$ se e somente se $d_1(x) \sim d_2(x)$. Deste modo, existe um único MDC mônico.

ATIV. 3.6. Verifique que a igualdade $1 = r(x)2 + s(x)x$ é um absurdo quaisquer que sejam $r(x), s(x) \in k[x]$

ATIV. 3.7. Mostre que se $p(x)|f(x)g(x)$ e MDC $(p(x), f(x)) = 1$ então $p(x)|g(x)$.

ATIV. 3.8. Mostre que se $p(x)$ é irredutível e $p(x) \not| f(x)$ então $p(x)$ e $f(x)$ são relativamente primos. Conclua que irredutíveis em $k[x]$ são primos.

ATIV. 3.9. Demonstre a implicação: irredutibilidade sobre $k \Rightarrow$ não existência de raízes em k. Mostre a recíproca para polinômios de grau 2 e 3.

ATIV. 3.10. Mostre que todo polinômio de grau 1 é irredutível sobre $k[x]$.

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.