10.5 Factoração única de polinomios sobre domínio

- Se A é DFU $\Rightarrow$ $A[x]$ é DFU.

- Aneis Noetheriano: Anel tal que todo ideal é finitamente gerado

Se $I_1 \subseteq I_2 \cdots \subseteq I_n \subseteq \cdots$ então $\exists N$ tal que $I_N = I_{N+1} = \cdots$

- Teorema da Base de Hilbert:

Se A é Noetheriano $\Rightarrow$ $A[x]$ é Noetheriano

Corolario A é Noetheriano $\Rightarrow$ $A[x_1, x_2 \ldots x_n]$ é Noetheriano

$$S = \{(x_1 \ldots x_n) \in A^n \mid f_j(x_1 \ldots x_n) = 0,\ j \in J\}$$

$$\Updownarrow$$

$\exists$ $f_{i_1}(x_1 \ldots x_n) \ldots$ $f_{i_s}(x_1 \ldots x_n)$

S coincide com o conjunto de soluções $\begin{cases} f_{i_1}(x_1, \dots x_n) \equiv 0 \\ \vdots \\ f_{i_s}(x_1, \dots x_n) \equiv 0 \end{cases}$

$$I = \langle f_1, \dots, f_k \rangle \subseteq A[x_1, \dots x_n]$$

Dado $g \in A[x_1, \dots, x_n]$, determinar de forma algorítmica se $g \in I$?!

$$I \subseteq \underline{\underline{K[x]}} \qquad K \in \text{corpo}$$

Se $g \in K[x]$ como determinar se $g \in I$

$\to$ $K[x]$ é um D.E. $\Rightarrow$ DIP

$\Rightarrow$ $I = (f)$ e nesse caso

Para $g \in I$ precisamos que g seja divisível por f.

Se $K[x,y]$ NÃO é domínio de ideais principais $\Rightarrow$ Não é DE

$I = \langle x, y \rangle$ precisa de 2 geradores

$$J = \langle P(x,y), Q(x,y) \rangle$$

$$= \{ a(x,y)P(x,y) + b(x,y)Q(x,y) \mid a, b \in K[x,y] \}$$

$g(x,y) \in K[x,y]$ ¿ $g(x,y) \in J$?

Não temos algoritmo da divisão para tentar dividir $g(x,y)$ por $P(x,y)$ e depois o resto dividir por $Q(x,y)$

$g(x,y) = x^5 + 3x^4y^2 + 5x^3y^4$ | $ax^n + \cdots$ | $bx^m + \cdots$

$\frac{a}{b}x^{n-m}$

$P(x,y) = x^2 + 2xy^2 + y^5$

$gra_x(g(x,y)) = 5$

$gra_y(g(x,y)) = 4$

$grau_T(g(x,y)) = 7$

$I \subset K[x_1, \ldots, x_n]$ e definimos uma ordem dos monomios (adequado) então existem $P_1\ P_2 \ldots P_s \in I$ tal que $I = \langle P_1 \ldots P_s \rangle$

e para todo $g \in K[x_1, \ldots, x_n]$ podemos aplicar um "algoritmo da divisão" que me permite determinar se $g \in I$ ou não

o conjunto $P_1 \ldots P_n$ com a ordem é chamado de Base de Grobner de I

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} \preccurlyeq x_1^{\beta_1} \cdots x_n^{\beta_n}$$

Possíveis ordem:

- Ordem lexicografica = Ordem do diccionio $\circledast$

$$\begin{cases} \alpha_1 < \beta_1 \\ \text{ou} \\ \alpha_1 = \beta_1 \text{ e } \alpha_2 < \beta_2 \\ \text{ou} \\ \alpha_1 = \beta_1, \alpha_2 = \beta_2, \text{ e } \alpha_3 \leq \beta_3 \\ \vdots \\ \alpha_1 = \beta_1 \cdots \alpha_{n-1} = \beta_{n-1} \text{ e } \alpha_n < \beta_n \end{cases}$$

- Ordem lexicografico ponderado

se $\alpha_1 + \cdots + \alpha_n < \beta_1 + \cdots + \beta_n$

ou $\alpha_1 + \cdots \alpha_n = \beta_1 + \cdots + \beta_n$ e $\circledast$

Para $\preccurlyeq$ ser uma ordem deve cumprir se $\vec{\alpha} \preccurlyeq \vec{\beta} \Rightarrow \vec{\alpha} + \vec{\gamma} \preccurlyeq \vec{\beta} + \vec{\gamma}$

transitivo
- $\vec{\alpha} \preccurlyeq \vec{\beta}$ e $\vec{\beta} \preccurlyeq \vec{\gamma} \Rightarrow \vec{\alpha} \preccurlyeq \vec{\gamma}$

Antisimetrica
- $\vec{\alpha} \preccurlyeq \vec{\beta}$ e $\vec{\beta} \preccurlyeq \vec{\alpha} \Rightarrow \vec{\alpha} = \vec{\beta}$

Reflexiva
- $\vec{\alpha} \preccurlyeq \vec{\alpha} \Rightarrow$

C.C.A: o Anel A cumpre a condição da cadeia ascendente se para toda cadeia ascendente de ideais

$$I_1 \subseteq I_2 \subseteq I_3 \cdots \subseteq I_n \subseteq \cdots \subseteq A$$

existe $N \in \mathbb{N}$ tal que $I_N = I_{N+1} = I_{N+2} = \cdots$

Se A tem um # finito de ideais $\Rightarrow$ trivialmente A cumpre CCA

Se A cumpre CCA $\Leftrightarrow$ A é noetheriano

Def: Dado $I \subset A \rightarrow$ Dominio definimos

$$\sqrt{I} := \{a \in A \mid \exists n \in \mathbb{N} \text{ tal que } a^n \in I\}$$

$\hookrightarrow$ radical do ideal I

Provar que $\sqrt{I}$ é um ideal

- $a, b \in \sqrt{I} \Rightarrow \exists n \in \mathbb{N}$ tal que $a^n \in I$
  $\exists m \in \mathbb{N}$ tal que $b^m \in I$

Queremos mostrar $a+b \in \sqrt{I}$

isto é queremos mostrar $\exists l \in \mathbb{N}$ tal que $(a+b)^l \in I$

Pegaremos $l = m+n$

$$\underbrace{(a+b)^{m+n}}_{\cap\, I} = \overbrace{\underset{\cap\, I}{a^{m+n}} + \underset{\cap\, I}{\binom{m+n}{1}} a^{m+n-1}b + \cdots + \underset{\cap\, I}{\binom{m+n}{m}}}^{a^n} \overbrace{a^n b^m + \cdots \underset{\cap\, I}{\binom{m+n}{m+n-1} a b^{m+n-1}}}^{b^m} + \underset{\cap\, I}{b^{m+n}}$$

$c \in A \Rightarrow ca \in \sqrt{I}$ pois $c^n a^n \in I$ ✓

$$a \in \sqrt{I} \Rightarrow \overset{\exists n}{a^n} \in I \Rightarrow a^{2n} \in I \Rightarrow (-a)^{2n} \in I$$

$$\Downarrow$$

$$-a \in \sqrt{I}$$

$\mathbb{Z} \supset (2400)$ $\quad 2400 = 2^5 \cdot 3 \cdot 5^2$

$\sqrt{(2400)} \ni a \iff \exists n$ tal que $a^n \in (2^5 \cdot 3 \cdot 5^2)$

$$\Rightarrow 2^5 \cdot 3 \cdot 5^2 \mid a^n \Rightarrow \left.\begin{array}{l} 2 \mid a \\ 3 \mid a \\ 5 \mid a \end{array}\right\} \Rightarrow 30 \mid a$$

$$\sqrt{(2400)} \supseteq (30)$$

$a \in (30) \Rightarrow a = 2 \cdot 3 \cdot 5 \cdot b \Rightarrow a^5 = 2^5 \cdot 3^5 \cdot 5^5 \cdot b^5 \in (2400)$

$\Rightarrow a \in \sqrt{(2400)}$

$(n) \subseteq \mathbb{Z} \Rightarrow \sqrt{(n)} = (p_1 p_2 \dots p_k)$

$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$

Problema: A anel Noetheriano e $J = \sqrt{(0)}$ nilradical

ie, $\boxed{a \in J \Leftrightarrow \exists n \text{ tal que } a^n = 0}$

Então existe $N \geq 1$ tal que

$$\underbrace{J \cdot J \cdots J}_{N \text{ vezes}} = 0$$

Lembrando: $I \cdot J = \langle ab \mid a \in I, b \in J \rangle$

Como A é noetheriano então

J é finitamente gerado

$J = \langle u_1, u_2 \ldots, u_s \rangle = \sqrt{(0)}$

$\forall u_j \Rightarrow \exists n_j \in \mathbb{N}$ tal que $u_j^{n_j} = 0$

Seja $a \in J$ logo existem

$c_1\ c_2 \ldots c_s \in A$ tal que

$$a = c_1 u_1 + c_2 u_2 + \ldots + c_s u_s$$

$$a^{n_1+n_2+\ldots+n_s} = (c_1 u_1 + c_2 u_2 + \quad + c_s u_s)^{\overbrace{n_1+\ldots+n_s}^{N}}$$

$$= \sum_{l_1+\ldots+l_s=N} \binom{N}{l_1, l_2 \ldots l_s} c_1^{l_1} u_1^{l_1} c_2^{l_2} u_2^{l_2} \ldots c_s^{l_s} u_s^{l_s}$$

Se $l_1 + \ldots + l_s = n_1 + \ldots + n_s$ então $\exists i$ tal que $l_j \geq n_j \Rightarrow \underline{\underline{u_j^{l_j} = 0}}$ logo

todos os somandos são 0

$$\Rightarrow J^N = 0$$

$$a_1 \cdots a_N \in J$$

$$a_i = \sum_{j=1}^{s} c_{ij} u_j$$

$$\underset{\substack{\cap \\ J^N}}{a_1 a_2 \cdots a_N} = \prod_{i=1}^{N} \left(\sum_{j=1}^{s} c_{ij} u_j \right)$$

$\exists\ l_j \geq n_j$ mesmo argumento

$$= \sum_{l_1 + l_2 + \cdots + l_s = N} d_{l_1 \cdots l_s}\, u_1^{l_1} \cdots u_s^{l_s}$$

<u>Problema</u>: A noetheriano $\phi : A \twoheadrightarrow A$ é homomorfismo sobrejetor

Mostrar que ϕ é isomorfismo.

Suponhamos que não é injetora $\Rightarrow$

$\ker(\phi) \neq (0)$ $\qquad \ker(\phi) \subseteq A$ ideal

$\Rightarrow$ $\ker(\phi)$ é finitamente gerado

$$\ker(\phi) = \langle u_1, u_2, \ldots, u_s \rangle$$

$$\mathbb{R}[x_1, x_2 \ldots x_n \ldots] \xrightarrow{\psi} \mathbb{R}[x_1 \ldots x_n \ldots]$$

$$x_1 \longmapsto 0$$

$$x_{i+1} \longmapsto x_i$$

é um homomorfismo sobre mas não é injetivo pois $x_1 \in Ker(\psi)$

$$R[x,y] = I = (x^n, x^{n-1}y, x^{n-2}y^2, \ldots, xy^{n-1}, y^n)$$

tem n+1 geradores

$Ker(\psi) \neq \{0\}$

$$\boxed{\frac{A}{Ker(\psi)} \simeq A}$$

Teorema de isomorfismo

$Ker(\psi) = \{a \in A \mid \psi(a) = 0\}$

<u>Teorema</u>: Dada A anel existem ideais maximais (Lema de Zorn)

$$\underset{I_0}{(0)} \subseteq \underset{I_1}{\psi^{-1}(0)} = Ker(\psi) \subseteq \underset{I_2}{\psi^{-1}(I_1)}$$

Em geral $I_j = \underbrace{\psi^{-1}(\psi^{-1}(\psi^{-1} \cdots \psi^{-1}}_{j \text{ vezes}}(0)))\ldots$

Afirmação $I_j \subseteq I_{j+1}$ prova por indução

$I_0 \subseteq I_1$ ✓

Se $I_j \subseteq I_{j+1} \Rightarrow \psi^{-1}(I_j) \subseteq \psi^{-1}(I_{j+1})$

$$\begin{array}{ccc} \psi^{-1}(I_j) & \subseteq & \psi^{-1}(I_{j+1}) \\ \parallel & & \parallel \\ I_{j+1} & \subseteq & I_{j+2} \end{array}$$

$I_0 \subseteq I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots\ldots$

Como A é noetheriano $\exists N$ tal que $\underline{I_N = I_{N+1}} = \psi^{-1}(I_N)$

$$\begin{array}{ccc} \psi(I_N) & = & \psi(I_{N+1}) \\ \parallel & & \\ I_{N-1} & = & I_N \end{array}$$

aplicando N vezes

Chegamos $I_1 = I_0$

$$\underset{\text{Ker}(\varphi)}{\overset{\shortparallel}{}} = (0) \quad \text{injetivo.}$$

Problema: A domínio Noetheriano

A é DIP $\iff$ todos os ideais primos são principais.

$$\boxed{\begin{array}{l}\underline{\textbf{Def}}: I \subset A \text{ é ideal primo se} \\ \text{sempre que } ab \in I \text{ então } a \in I \text{ ou } b \in I\end{array}}$$

Falso - verdadeiro

- Todo subanel de um anel noetheriano é noetheriano
- Todo anel noetheriano é DFU ??