D é dominio de ideais principais

$\Downarrow$

D[x] so é DIP no caso que D é corpo

<u>Teorema</u>: Se D e dominio de fatorização única (DFU) então D[x] é <u>DFU</u>.

"Ferramentas" para provar este teorema

<u>Lema</u>: Se D e domínio então

$$U(D[x]) = U(D)$$

<u>Prova</u>: Se $f(x) \in U(D[x])$ logo existe

$g(x) \in D[x]$ $\quad f(x)g(x) = 1$

$\text{grau}(f(x)g(x)) = \text{grau}(f(x)) + \text{grau}(g(x)) = 0$

$\Rightarrow \text{grau}(f(x)) = \text{grau}(g(x)) = 0 \Rightarrow f(x)$ é constante $\square$

Def: Dizemos que um polinomio $f(x)$ é primitivo em $D[x]$ se sempre que $f(x) = c\,g(x)$ com $c \in D$ e $g(x) \in D[x]$ então $c \in \mathcal{U}(D)$

Exemplo: em $\mathbb{Z}[x]$ o polinomio $\boxed{2x^2+6x+10}$ não é primitivo pois

$$2x^2+6x+10 = 2(\underbrace{x^2+3x+5}_{\text{primitivo}}) \quad e \quad 2 \notin \mathcal{U}(\mathbb{Z})$$

Observemos que se $f(x)$ é primitivo e $f(x) = c\,g(x) \Rightarrow c \in \mathcal{U}(D)$

mas se $g(x) = d\,h(x) \Rightarrow$

$$f(x) = (cd)h(x) \Rightarrow \underline{cd} \in \mathcal{U}(D)$$

$\Rightarrow d \in \mathcal{U}(D) \Rightarrow g(x)$ tambem é primitivo

Lema: Se $f(x) \in D[x]$ com D DFU então existem $c \in D$ e $g(x) \in D[x]$

tal que $\quad \bullet\ f(x) = c\,g(x)$

$\bullet\ g(x)$ é primitivo

Prova: $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

com $a_n \neq 0$. Como D e DFU então

$a_n = u\,p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ onde $p_1 \dots p_s$ são irredutíveis em D e $\alpha_j > 0$ $\boxed{s \geq 0}$

Seja $C = p_1^{u_1} p_2^{u_2} \cdots p_s^{u_s}$

onde

$u_j = \max\{ l \in \mathbb{N} \mid$ tal que p_j^l divide a_i para todo $i = 0, 1, 2 \dots n \}$

Em particular c divide a_i para $i = 0, 1, 2 \dots n$

$a_i := b_i c$

$$f(x) = c\,(\underbrace{b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0}_{g(x)})$$

falta mostrar que $g(x)$ é primitivo. Suponhamos que não é primitivo $\Rightarrow g(x) = d\,h(x)$ com $d \notin \mathcal{U}(x) \Rightarrow d = Q_1^{\beta_1} \cdots Q_t^{\beta_t}$ $\beta_i \geq 1$, $t \geq 1$

$\Rightarrow Q_1$ divide b_n (que divide a_n)

$\Rightarrow Q_1$ deve ser algum P_j (Podemos supor que é P_1)

P_1 divide $b_0, b_1, \ldots, b_n$

$$\Rightarrow a_j = c \cdot b_j = P_1^{u_1}(\ldots)\, b_j$$
$$= P_1^{u_1}(\ldots)\, P_1(\ldots)$$

$\Rightarrow$ todos os coeficientes a_j são divisíveis por $P_1^{u_1+1}$ ← contraditório

$\square$

<u>Teorema</u>: Seja D DFU. Então todo elemento $f(x) \in D[x] \setminus \mathcal{U}(D[x])$ pode-se

escrever como produto de Irredutíveis.
(É mais fraco porque não pedimos unicidade)

<u>Prova</u>: Por contradição suponhamos que existe Um $f(x) \in D[x]$ que não é produto de irredutíveis. e vamos supor $f(x)$ de grau mínimo. Sabemos que

$f(x) = c\, g(x)$ com $c \in D$ e $g(x) \in D[x]$ primitivo. como $c \in D$ então

$c = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ com p_j irredutíveis de D.

Agora $g(x)$ tem duas possibilidades

- $g(x)$ é unidade de $D[x] \Rightarrow g(x) \in U(D)$ ✓

ou

- $g(x)$ Não é uma unidade de $D[x]$
  - Se $g(x)$ é irredutível de $D[x]$ acabou
  - Caso $g(x)$ não seja redutível

$\Rightarrow$ $g(x) = h_1(x)\, h_2(x)$ onde $h_1(x)$ e $h_2(x)$ não são unidades, e além disso $h_1(x)$ e $h_2(x)$ Não são constantes, pois $g(x)$ é primitivo -

$$\text{grau}(g(x)) = \text{grau}(h_1(x)) + \text{grau}(h_2(x))$$

$\geq 1 \qquad \geq 1$

$$\Rightarrow \begin{array}{l} 0 < \text{grau}(h_1(x)) < \text{grau}(g(x)) \\ 0 < \text{grau}(h_2(x)) < \text{grau}(g(x)) \end{array}$$

Como $f(x)$ era o contraexemplo de grau mínimo $\Rightarrow$ $h_1(x)$ e $h_2(x)$ podem se escrever como produto de inedutíveis

$\Rightarrow$ $f(x) = c\,\underbrace{h_1(x) h_2(x)}$ e' produto de inedutíveis (contraditorio) $\square$

Lema: Sejam $g(x)\, h(x) \in D[x]$ D.F.U

e seja $p \in D$ inedutível tal que p divide $g(x) \cdot h(x)$. Então p divide $g(x)$ ou p divide $h(x)$

Prova: Supohamos que p não divide $g(x)$

$g(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$, logo existe $0 \le i \le n$ tal que p não divide a_i e vamos supor i mínimo com esta propriedade (Logo p divide a_j $\forall j < i$) $\Leftarrow$

Se $h(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_0$

$$g(x)h(x) = (a_n x^n + \dots + a_1 x + a_0)(b_m x^m + \dots + b_0)$$

$$= a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \dots + (a_i b_0 + a_{i-1} b_1 + \dots + a_0 b_i)x^i + \dots$$

→ é divisível por p. ⇒ cada coeficiente é divisível por p, em particular

$a_i b_0 + a_{i-1} b_1 + \dots\ a_1 b_{i-1} + a_0 b_i$ é divisível por p

$$a_i b_0 + \underbrace{a_{i-1} b_1 + \dots\ a_1 b_{i-1} + a_0 b_i}_{\text{é divisível por } p}$$

⇒ p divide $a_i b_0$ mas p não divide a_i ⇒ p divide b_0

A prova continua por indução mostrando que todos os coeficientes b_j são divisíveis por p

- $j=0$ está provado

HI: Suponhamos que p divide $b_0, \dots, b_{\ell-1}$

Queremos mostrar que p divide b_ℓ

No produto $g(x)h(x)$ o coeficiente de $x^{\ell+i}$ é

$$\underbrace{b_{\ell+i} a_0 + b_{\ell+i-1} a_1 + \dots}_{\text{são divisíveis por } p} + a_i b_\ell + \underbrace{a_{i+1} b_{\ell-1} + \dots + a_{\ell+i} b_0}_{\text{Por HI são divisíveis por } p}$$

Logo $a_i b_e$ é divisível por p $\Rightarrow$
p divide $\underline{b_e}$ ✓

Portanto todos os coeficientes de $h(x)$ são divisíveis por p.

<u>Lema de Gauss</u>: Seja D DFU então o produto de polinomios primitivos é polinomio primitivo

<u>Prova</u>: Suponhamos por contradição que $f(x), g(x) \in D[x]$ são primitivos MAS

$f(x)g(x)$ não é primitivo $\Rightarrow$

$f(x)g(x) = \underline{c}\, h(x)$ com $\underline{c} \notin U(D)$

$\Rightarrow$ $\exists\, p \in D$ irredutível que divide c.

$\Rightarrow$ p divide $f(x)g(x)$ e pelo Lema anterior p divide $f(x)$ ou p divide $g(x)$

o que contraditório. $\square$

Teorema: Seja D DFU e $f(x), g(x) \in D[x]$ polinômios primitivos tais que

$$r f(x) = s g(x) \quad \text{para alguns } r, s \in D^*$$

então r e s são associados

$$\boxed{\begin{array}{l} r \text{ e } s \text{ são associados se } \exists u \in U(D) \\ \text{tal que } r = us \qquad \text{Exemplo } \mathbb{Z}[i] \; 2+3i \text{ e } 3-2i \text{ são associados} \end{array}}$$

Prova: • Se $r \in U(D) \Rightarrow f(x) = (r^{-1}s) g(x)$

mas como $f(x)$ é primitivo

então $r^{-1}s \in U(D) \Rightarrow r^{-1}s = u \Rightarrow \underline{s = ur}$

• Se $r \notin U(D) \Rightarrow \underbrace{r = P_1 P_2 \ldots P_k}$ $K \geq 1$

produto de irredutíveis

$\Rightarrow P_1 (P_2 \ldots P_k) f(x) = \underline{s\, g(x)}$ Logo $\underline{P_1}$

divide $\underline{s\, g(x)}$, mas P_1 não divide

$g(x)$, pois $g(x)$ é primitivo $s = P_1 s_1$

$$\underline{P_1} P_2 \ldots P_k f(x) = \underline{P_1} s_1 g(x)$$

$$\underline{P_2 \ldots P_k} f(x) = s_1 g(x)$$

Fazendo o mesmo processo com P_2 P_3 ...

$S_1 = P_2 S_2 \qquad S_2 = P_3 S_3 \; \cdots$ podemo ir simplificando os P_j $j=1,\dots,K$ obtendo ao final

$$\underline{f(x)} = S_K\, g(x)$$

mas $f(x)$ é primitivo $\Rightarrow S_K \in \mathcal{U}(D)$

$$S = \underbrace{P_1 P_2 \cdots P_K}_{} S_K = r\, S_K$$

Logo S e r são associados $\square$

Prop: Dado um domínio D <u>existe</u> um F corpo mínimo que contém D

<u>Prova</u>: $F = \left\{ (a,b) \;\middle|\; \begin{array}{l} a,b \in D \\ b \neq 0 \end{array} \right\} \Big/ \sim$

$(a_1, b_1) \sim (a_2, b_2)$ se $\quad \dfrac{a_1}{b_1} = \dfrac{a_2}{b_2}$

$\hookrightarrow a_1 b_2 = a_2 b_1$

Com $\left\{ \begin{array}{l} (a,b) + (c,d) = (ad+bc,\; bd) \checkmark \\ (a,b)\cdot(c,d) = (ac,\; bd) \checkmark \end{array} \right.$

$\hookrightarrow$ F é corpo $\rightarrow$ chamado corpo de frações de D

$$\begin{array}{ccc} D & \hookrightarrow & F \\ a & \longmapsto & (a,1) \end{array}$$ insetivo

$(a,1)\cdot(1,a)$

$=(a,a)\sim(1,1)$

Corolario: Se D e DFU e F é seu corpo de frações e se $f(x)\in D[x]$ não constante.

Se $f(x)$ é iredutivel em $D[x]$ então $f(x)$ é irredutível em $F[x]$

Prova: Suponhamos falso Logo $\exists f(x)\in D[x]$ iredutível tal que

$$f(x)=g(x)h(x) \quad \text{com} \quad g(x),h(x)\in F[x]$$

e diferentes de constante.

Suponhamos que $d\in D^*$ tal que

$dg(x)\in D[x]$ e $e\in D^*$ talque

$eh(x)\in D[x]$

sabemos que existem $\tilde{d}\in D$ e $\tilde{e}\in D$

tal que $d g(x) = \tilde{d}\, \tilde{g}(x)$, e $h(x) = \hat{e}\, \hat{h}(x)$

com $\tilde{g}(x), \hat{h}(x) \in D[x]$ primitivos

$$\Rightarrow \quad f(x) = g(x)\, h(x)$$

$\swarrow$ inredutível

$$d e \underline{f(x)} = \underline{d g(x)}\; \underline{e h(x)}$$
$$= \tilde{d}\, \tilde{g}(x)\, \tilde{e}\, \hat{h}(x)$$

primitivos

$$(d e) f(x) = \tilde{d}\, \tilde{e}\, \tilde{g}(x)\, \hat{h}(x)$$

Logo de e $\tilde{d}\tilde{e}$ são associados

$$f(x) = u\, \underset{\overset{\uparrow}{D[x]}}{\tilde{g}(x)\, \hat{h}(x)}$$

Logo $f(x)$ redutível em $D[x]$ $\square$

Teorema: se D é DFU $\Rightarrow$ $D[x]$ é DFU

Prova: Falta a unicidade

$$\underbrace{c_1 c_2 \cdots c_m}\, \underbrace{p_1(x) \cdots p_k(x)} = \underbrace{d_1 d_2 \cdots d_n}\, \underbrace{q_1(x) \cdots q_\ell(x)}$$

Irredutíveis

Logo $c_1 \dots c_m$ e $d_1 \dots d$ são associados $\Rightarrow$ $\underline{c_1 \dots c_m} = u\, \underline{d_1 \dots d_n} \in D$

mas em $\underline{D}$ temos Fatoração única.

então $m = n$ $\underline{\underline{c_j = d_j u_j}}$ $u_j \in U(D)$

$$\underbrace{p_1(x)\, p_2(x) \dots p_k(x)}= \underbrace{q_1(x) \dots q_\ell(x)} \quad (**)$$

Irredutível $\Rightarrow$ $\underline{\text{primo}}$ $\underline{p_1(x)}$ divide $\underline{\underline{q_1(x) \dots q_\ell(x)}}$

então $\underline{p_1(x)}$ divide algum $\underline{q_j(x)}$

Como $q_j(x)$ é irredutível $\Rightarrow$

$$p_1(x) = v_1\, q_j(x)$$

Podemos "simplificar" esse fator em $(**)$ e continuar o mesmo processo.

Continuando $k = \ell$ e todos os fatores iguais $\square$