Domínio

DE $\Rightarrow$ DIP

($\Leftarrow$) existem contraexemplo

$\mathbb{Z}$, $K[x]$ são domínios euclideanos

$\Rightarrow$ também são domínios de ideais principais

Exemplo de D que NÃO é DIP

$\mathbb{Z}[x]$

$I_1 = (2)$ → polinomios com coeficientes pares

$I_2 = (x)$ → polinomios com coeficiente independente igual a zero

$I_1, I_2 \subseteq (2, x)$ → polinomios com coeficiente independente par

mas este ideal NÃO é principal

ie. NÃO existe $f(x) \in \mathbb{Z}[x]$ que gere $(2, x)$

pois nesse caso $(2, x) = (f(x))$ em particular

- $f(x)$ divide 2 $\qquad f =$ constante $= d$
- $f(x)$ divide x $\qquad x = d \cdot \frac{x}{d} \in \mathbb{Z}[x]$

Logo $c=1 \Rightarrow f(x)=1 \Rightarrow (f(x)) = \mathbb{Z}[x]$.

Em geral, se A // domínio que não é um corpo $\Rightarrow$ $A[x]$ não é de ideais principais

elementos invertíveis

Basta pegar $a \in A^* \setminus U(A)$

e considerar o ideal $I = (a, x)$. a prova que I não é principal é similar à anterior

Domínio ✓
que NÃO é DIP ✓

D.E

$$K[x_1] \twoheadrightarrow K[x_1, x_2] \twoheadrightarrow K[x_1, x_2, x_3] \twoheadrightarrow$$

Domínios de Fatoração Única (D.F.U)

Def: Dado D domínio. Dizemos que $a \in D$ é irredutível se sempre que $a = bc$ com $b, c \in D$ então ou $b \in U(D)$ ou $c \in U(D)$

Def: Dado D domínio Dizemos que $a \in D$ é um primo em D se sempre que a divide bc então a divide b ou a divide c

~~**Prop:** Todo irredutível é primo~~

~~Seja $a \in D$ irredutível e suponhamos que a divide $b \cdot c$.~~

~~Suponhamos que a não divide b~~

~~Consideremos $I = \langle a, b \rangle$~~

Primo $\Rightarrow$ Irredutível (Vale para todo Domínio)

$a \in D$ primo e suponhamos que a não é irredutível $\Rightarrow a = bc$

Logo a divide bc Logo

a divide b ou a divide c } Podemos supor sem perda de generalidade $a \mid b$

$$b = ad \xrightarrow{\text{mult por } c} bc = adc$$

$bc = a$

Como é domínio $a(\underline{1 - dc}) = 0$

$a=0$ ou $1-dc=0 \Rightarrow c \in \mathcal{U}(D)$

Teorema: Seja D um D.I.P. Então todo irredutível é primo.

Prova: Seja $a \in D$ irredutível e suponhamos por contradição que a não é primo, i.e. existem $b, c \in D$ tais que a divide bc, mas a não divide b nem c.

Considere o ideal $I=(a,b)$

Como D é DIP $\Rightarrow I=(d)$

$\Rightarrow$ d divide a $\Rightarrow a = de$ (irredutível) logo

• $d \in \mathcal{U}(D)$ ou • $e \in \mathcal{U}(D)$

• Se $d \in \mathcal{U}(D) \Rightarrow I=(d)=D \ni 1$

$\Rightarrow 1 = at + bs$ com $t, s \in D$

$$c = act + bcs \Rightarrow c \in (a)$$

$act \in (a)$, $bcs \in (a)$

$\Updownarrow$

a divide c ✓

Contraditório

- $e \in U(D) \Rightarrow I = (d) = (ae^{-1}) = (a)$

e^{-1}: unidade

Logo $(a) = (a, b) \ni b \Rightarrow b \in (a)$

$\Rightarrow$ a divide b contradição.

Exemplo: $\mathbb{Z}[\sqrt{-5}]$ não é D.I.P.

$\mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{-5}\, b \mid a, b \in \mathbb{Z}\}$

$I = (2, 1 + \sqrt{-5})$.

I não é principal. Suponhamos

$I = (a + \sqrt{-5}\, b) \Rightarrow$ $a + \sqrt{-5}\, b$ divide 2
$a + \sqrt{-5}\, b$ divide $1 + \sqrt{-5}$

$$2 = (a + \sqrt{-5}\, b) \cdot (c + \sqrt{-5}\, d)$$

$$2 = \underbrace{ac - 5bd}_{=2} + \sqrt{-5}\,(\underbrace{bc + ad}_{=0})$$

$$\begin{cases} ac - 5bd = 2 \\ bc + ad = 0 \end{cases} \qquad \begin{pmatrix} a & -5b \\ b & a \end{pmatrix}\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$$

$$c = \frac{2a}{a^2+5b^2} \in \mathbb{Z} \qquad d = \frac{-2b}{a^2+5b^2} \in \mathbb{Z}$$

Se $b \neq 0$ $\quad a^2+5b^2 \geq a^2+5 > 2a$ quocente não é inteiro

Logo $b=0$ $\quad c = \frac{2}{a}$ $\quad d=0$ $\quad a = 1$ ou 2

Concluímos que 2 é inredutível

$a + \sqrt{-5}\, b = \pm 1$ ou ± 2 $\quad \rightarrow (\pm 1) = \mathbb{Z}[\sqrt{-5}]$

$\rightarrow (\pm 2)$

- $(2) = (2, 1+\sqrt{-5}) \Rightarrow$ 2 divide $1+\sqrt{-5}$

$$1+\sqrt{-5} = 2(f+\sqrt{-5}\,g) \Rightarrow \begin{matrix} 2f = 1 \\ 2g = 1 \end{matrix} \quad \times$$

Logo $(2) \neq (2, 1+\sqrt{-5})$

- $(1) = \mathbb{Z}[\sqrt{-5}] = (2, 1+\sqrt{-5}) \ni 1$

$$1 = 2(s+\sqrt{-5}\,t) + (1+\sqrt{-5})(x+\sqrt{-5}\,y)$$

$$= 2s + \sqrt{-5}(2t) + x - 5y + \sqrt{-5}(x+y)$$

$$\begin{cases} 1 = 2s + x - 5y \\ 0 = 2t + x + y \end{cases}$$

$$\underbrace{1}_{\text{Impar}} = \underbrace{2s + 2t + 2x - 4y}_{\text{Par}}$$

Logo NÃO pode existir solução

$\mathbb{Z}[\sqrt{-5}]$ não é de ideais principais.

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

2 divide $\underbrace{(1+\sqrt{-5})(1-\sqrt{-5})}$ $= 1^2 - (\sqrt{-5})^2$

mas 2 não divide nem $(1+\sqrt{-5})$ nem $(1-\sqrt{-5})$

$a_1 a_2 \ldots a_e \in A$

$I := (a_1 \ldots a_e) = \{a_1 t_1 + \ldots + a_e t_e \mid t_j \in A\}$

é ideal

$\mathbb{N}$ não precisa ser enumerável

$\{a_i\}_{i\in\mathbb{N}} \subseteq A$

somas finitas

$$I(\{a_i\}_{i\in\mathbb{N}}) := \left\{ \sum_{j=1}^{s} a_{i_j} t_{i_j} \;\middle|\; \begin{array}{l} s \in \mathbb{N} \\ i_1 \ldots i_s \in \mathbb{N} \\ t_{i_j} \in A \end{array} \right\} \subseteq A$$

Exemplo de ideal que

$\mathbb{R}[x_1\, x_2\, x_3 \, \ldots \, x_n \ldots]$ → é um ideal que precisa de infinitos geradores

$\cup$

$a_i = x_i^i$ $\quad I = (\{a_i\}_{i \in \mathbb{N}})$

Logo $2 \in \mathbb{Z}[\sqrt{-5}]$ é irredutível mas NÃO é primo.

$\{\theta_i\}_{i \in M}$ irracionais que sejam "polinomialmente independentes"

$\mathbb{Q}[\{\theta_i\}_{i \in M}] \subseteq \mathbb{C}$ "variáveis θ_i"

Def: Dizemos que D domínio é domínio de fatoração única se para todo $a \in D^* \setminus U(D)$ existem $b_1\, b_2 \ldots b_s$ irredutíveis tais que

$a = b_1 b_2 \ldots b_s$

Além disso se $a = c_1 \ldots c_t$ com c_j irredutíveis então $t = s$ e existe uma permutação dos fatores de tal forma que $b_j = c_j e_j$ com $e_j \in U(D)$

$\mathbb{Z}[\sqrt{-5}]$ NÃO é DFU

Pois $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

Teorema: Todo DIP é DFU

O contrario não necessariamente é verdadeiro

Pensar: $\mathbb{Z}[x]$ e DFU mas não é DIP

$$\boxed{DE \Rightarrow DIP \Rightarrow DFU.}$$

$\mathbb{Z}[\sqrt{-5}]$

$x^5 + y^5 = z^5$

Pag 330 Ex.4.: c e d associados ($c = de$, $e \in U(D)$) em D $\Leftrightarrow$ c divide b, d divide c

$(\Rightarrow)$ $c = de$ $\Rightarrow$ d divide c

$c \underset{D}{e^{-1}} = d$ $\Rightarrow$ c divide d

(⇐) d divide c $\Rightarrow$ $c = de$

c divide d $\Rightarrow$ $d = cf$

$$c = cfe \Rightarrow c(1-fe) = 0$$

Como D é domínio $\Rightarrow$ $c = 0 \Rightarrow d = 0$

ou

$1 - fe = 0 \Rightarrow f, e \in U(D)$

$\Rightarrow c = d(\overset{\text{unidade}}{e})$ $\Rightarrow$ c e d são associados.

Pag 167 Exe 18: $\underset{\text{ideal}}{P \subsetneq R}$ R comutativo

P é $\overset{\text{ideal}}{\text{primo}}$ $\Leftrightarrow$ $\forall A, B$ ideais com $AB \subseteq P \Rightarrow$ $A \subseteq P$ ou $B \subseteq P$

$\boxed{P \text{ é ideal primo se sempre } ab \in P \Rightarrow a \in P \text{ ou } b \in P}$

(⇒) P primo e suponhamos que existem A, B ideais com $AB \subseteq P$ mas $A \nsubseteq P$ e $B \nsubseteq P$

$\Rightarrow \exists\, a \in A \setminus P$ $b \in B \setminus P$

mas $ab \in AB \subseteq P \Rightarrow ab \in P \Rightarrow$ $a \in P$ ou $b \in P$ contraditório

$(\Leftarrow)$ Seja $ab \in P \Rightarrow (a)(b) \subseteq P$

$(a)(b) = \{at\, bs \mid t, s \in D\} = \{ab(ts) \mid t, s \in D\}$
$= (ab)$

$\Rightarrow$ ou $(a) \subseteq P$ $\quad a \in (a) \subseteq P \Rightarrow a \in P$
ou ou
ou $(b) \subseteq P$ $\quad b \in (b) \subseteq P \Rightarrow b \in P$