Pag 341 - 1, $a, b \neq 0$ D domínio

$a \notin U(D)$. Mostrar $(ab) \subsetneq (b)$

$ab \in (b) \Rightarrow (ab) \subseteq (b)$

Verifiquemos que $b \notin (ab)$. Suponhamos falso, existe $c \in D$ tal que $b = (ab)c$

$acb = b \quad (ac-1)\underbrace{b}_{\neq 0} = 0 \Rightarrow ac - 1 = 0$

$ac = 1 \Rightarrow a \in U(D)$ contradição

Logo $b \notin (ab) \Rightarrow (ab) \subsetneq (b)$.

---

(14) p primo $R = \{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \} \subseteq \mathbb{Q}$

(a) R domínio.

- $\underset{\underset{R}{\Uparrow}}{\frac{a_1}{b_1}} + \underset{\underset{R}{\Uparrow}}{\frac{a_2}{b_2}} = \frac{a_1b_2 + a_2b_1}{b_1b_2}$

Com $p \nmid b_1$ e $p \nmid b_2$ $\Rightarrow p \nmid b_1b_2$

$\Rightarrow \frac{a_1b_2 + a_2b_1}{b_1b_2} \in R$

$p \mid b_1$ e $p \mid b_2$ $\Rightarrow p \mid b_1b_2$

- $\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1a_2}{b_1b_2} \in R$

- $\frac{a_1}{b_1} + \frac{-a_1}{b_1} = 0 = \frac{0}{1}$

ⓑ Se $\frac{a}{b} \in R$ e $p \nmid a$ $\Rightarrow$ $\frac{a}{b} \in U(R)$

$\frac{b}{a} \in \mathbb{Q}$ e $p \nmid a$ $\Rightarrow$ $\frac{b}{a} \in R$ e

$\frac{a}{b} \cdot \frac{b}{a} = 1$ $\Rightarrow$ $\frac{a}{b}$ tem inverso em R.

ⓒ $I \subsetneq R$ então $p^t \in I$ para algum $t \geq 0$

Seja $\frac{a}{b} \in I \setminus \{0\}$ $\Rightarrow$ $\underbrace{\frac{a}{b}}_{\in I} \cdot \underbrace{\frac{b}{1}}_{\in R} = a \in I$

$a = p^t \cdot c$ $\Longrightarrow$ $\overset{\in I}{a} \cdot \overset{\in R}{\frac{1}{c}} = p^t \in I$

$(p,c) = 1$ $t \geq 0$

Suponhamos que $t = 0$ $\Rightarrow$ $p^0 = 1 \in I$

$\Rightarrow I = (1) = R$ I não é ideal próprio

Logo $t > 0$

$\Rightarrow$ todo ideal de R é da forma (p^t) para algum $t > 0$

(d) R é DIP

$I \trianglelefteq R \Rightarrow \exists t > 0$ tal que $p^t \in I$ ⊛

e escolhemos t mínimo com esta ⊛ propriedade $(p^t) \subseteq I$

Queremos mostrar que $I = (p^t)$

Suponhamos $I \setminus (p^t) \neq \emptyset$

$\frac{c}{d} \in I \setminus (p^t)$ $\qquad c = p^u c'$

$\frac{c}{d} = p^u \cdot \frac{c'}{d} \Rightarrow$ $\mathrm{mdc}(c', p) = 1$, $\mathrm{md}(d, p) = 1$

$\Rightarrow \overset{\in I}{\frac{c}{d}} \cdot \overset{\in R}{\frac{d}{c'}} = p^u \in I$

mas $p^u \notin (p^t)$ pois caso contrario

$p^u \cdot \overset{\in R}{\frac{c'}{d}} = \frac{c}{d} \in (p^t)$

$\Rightarrow p^u \in I \setminus (p^t) \Rightarrow p^t \nmid p^u$

$\Rightarrow$ $u < t$ contraditório

logo $I = (p^t) \Rightarrow R$ é

um domínio de ideais principais.

---

(19) Dizemos que R satisfaz a condição da cadeia descendente (CCD) sobre ideais se $R \supseteq I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots \supseteq I_n \supseteq \cdots$

então $\exists n$ tal que $I_j = I_n \ \forall j \geq n$

(a) Mostrar que $\mathbb{Z}$ não satisfaz CCD

$(2) \supsetneq (4) \supsetneq (8) \supsetneq (16) \supsetneq (32) \supsetneq \cdots \supsetneq (2^n) \supsetneq \cdots$

$(2) \supsetneq (2 \cdot 3) \supsetneq (2 \cdot 3 \cdot 4) \cdots \supsetneq (n!) \supsetneq \cdots$

(b) R domínio de integridade

R é corpo $\Longleftrightarrow$ R satisfaz CCD

$(\Rightarrow)$ trivial pois os únicos "ideais" são $(0) = \{0\}$ e R

($\Leftarrow$) Suponha que R satisfaz CCD

$a \in R^*$

$(a) \supseteq (a^2) \supseteq (a^3) \supseteq (a^4) \cdots \supseteq$

Como R satisfaz CCD então existe n tal que $(a^{n+j}) = (a^n)$ $\forall j \geq 0$

$j=1$ $\quad (a^{n+1}) = (a^n)$

$a^n \in (a^{n+1}) \Rightarrow \exists\, b \in R$ tal que

$a^n = a^{n+1} \cdot b \Rightarrow a^n \cdot (1 - ab) = 0$

Como R é domínio $\to a^n = 0 \Rightarrow$ impossível ("$a \cdot a^{n-1}$")

$\to 1 - ab = 0$ $\quad ab = 1$

$\Rightarrow$ b é o inverso de a

Logo R é corpo.

---

(10) D DIP Provar que (a) é maximal

$\Leftrightarrow$ a é irredutível

($\Rightarrow$) Suponhamos (a) maximal mas a é redutível

$a = b \cdot c$ onde $b, c \notin U(D)$.

$(a) \subseteq (b)$

- Como $b \notin U(D) \Rightarrow (b) \neq D$
- Como (a) é maximal

$\Rightarrow (a) = (b) \Rightarrow b \in (a) \Rightarrow \exists d$

tal que $b = ad$

$a = (ad)c \Rightarrow a(1 - dc) = 0$

Como $a \neq 0 \Rightarrow dc = 1 \Rightarrow c \in U(D)$

Contraditório $\Rightarrow$ a é irredutível!.

($\Leftarrow$) Suponhamos a irredutível e queremos mostrar (a) é maximal

Seja I $\quad (a) \subseteq I \subsetneq D$

Como D é PIP $\Rightarrow \exists\, b \in D$ tq $I = (b)$

$\Rightarrow (a) \subseteq (b) \subsetneq D$

Em particular $a \in (b)$, logo existe $c \in D$ tal que $a = bc$

Como a é irredutível $\Rightarrow$ $b \in U(D)$ ~~X~~ ou $c \in U(D)$

$c \in U(D) \Rightarrow ac^{-1} = b \Rightarrow b \in (a)$
$(b) \subseteq (a)$

$\Rightarrow (a) = (b) \Rightarrow (a)$ é maximal

$D = \mathbb{Z}[x] \rightarrow 2$ é irredutível mas (2) não é maximal pois $(2) \subsetneq (2, x)$

Pag (351) 6 $\Rightarrow$ 5 é irredutível? em

b $\mathbb{Z}[i]$ $\quad 5 = (1+2i)(1-2i)$ Não é

c $\mathbb{Z}[\sqrt{-2}]$ $\quad a + \sqrt{-2}\, b \mid 5$

$$\Rightarrow N(a + \sqrt{-2}\, b) \mid N(5) = 25$$
$$\shortparallel$$

$(a+\sqrt{-2}b)(a-\sqrt{-2}b) = a^2 + 2b^2$ divide 25

$$a^2 + 2b^2 = 1 \text{ ou } 5 \text{ ou } 25$$

- $a^2+2b^2=1 \Rightarrow a=\pm 1 \quad b=0$

  $a+\sqrt{-2}\,b=1$

- $\underbrace{a^2+2b^2}=\underset{\sim}{5} \Rightarrow$ Impossível

- $a^2+2b^2=25 \qquad a,b\geq 1$

  $a^2<25$

  $|a|<5$

  $2b^2\leq 25$

  $|b|<\sqrt{\frac{25}{2}}=3,\ldots$

$\Rightarrow b=1,2,3$

$b=1 \Rightarrow a^2=23$ ✗

$b=2 \Rightarrow a^2=17$ ✗

$b=3 \Rightarrow a^2=7$ ✗

Logo 5 é irredutível em $\mathbb{Z}[\sqrt{-2}]$

Teorema. Seja $a+\sqrt{n}\,b\in\mathbb{Z}[\sqrt{n}]$ tal que $N(a+\sqrt{n}\,b)$ é um número primo de $\mathbb{Z}$, Então $a+\sqrt{n}\,b$ é irredutível em $\mathbb{Z}[\sqrt{n}]$

$\Leftarrow$ Não necessariamente vale!

Prova: $a+\sqrt{n}\,b=z\cdot w \qquad z,w\in\mathbb{Z}[\sqrt{n}]$

$N(a+\sqrt{n}\,b)=N(z)\cdot N(w)$ é primo

$\Rightarrow N(z)$ ou $N(w)$ é $1 \Rightarrow z$ ou w é unidade

(11) Mostrar que $\mathbb{Z}[\sqrt{-6}]$ não é DFU

$$10 = 2 \cdot 5 = (2+\sqrt{-6})(2-\sqrt{-6})$$

Se $a+\sqrt{-6}\,b$ divide 2

$\Rightarrow a^2+6b^2$ divide 4 $\Rightarrow a = \pm 2$

$\Rightarrow$ 2 é irredutível

2 não divide $2+\sqrt{-6}$

Caso contrario $N(2)$ dividiria $N(2 \pm \sqrt{-6})$

$\Rightarrow$ 4 dividiria 10 contraditorio

Pag 330 - 13) R domínio euclideano

$k \in \mathbb{Z}$ $k > 0$ δ função euclideano

Dados $a, b \in R$ $b \neq 0$ $\exists\, q, r \in R$ tal que $a = qb + r$ com $r = 0$ ou $\Rightarrow \delta(r) < \delta(b)$

ⓐ Mostrar que R também é D.E. dado pela função $\theta(r) = \delta(r) + k$

Pegando ⊛ e somando k $\Rightarrow \underbrace{\delta(r)+k}_{\theta(r)} < \underbrace{\delta(b)+k}_{\theta(b)}$

$\theta(r) < \theta(b)$

$\theta : D \to \mathbb{N}$ ✓

$r_1, r_2 \in D^*$

$\theta(r_1 r_2) \overset{?}{\geq} \theta(r_1)$ ✓ ← queremos mostrar

$\theta(r_1 r_2) = \delta(r_1 r_2) + k \overset{?}{\geq} \delta(r_1) + k$ ✓

$\underbrace{\delta(r_1 r_2) \geq \delta(r_1)}$ ✓

ⓑ $\beta(r) = k\,\delta(r)$

$\delta(r_1 r_2) \geq \delta(r_1) \Rightarrow k\,\delta(r_1 r_2) \geq k\,\delta(r_1)$

$\beta(r_1 r_2) \geq \beta(r_1)$ ✓

$K[x] \ni f$ $\quad \deg(f)$

$\deg(fg) = \deg(f) + \deg(g) \geq \deg(f)$

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \supsetneq \mathbb{Z}[\sqrt{-19}]$ Não é domínio euclideano.

Def: Dado D domínio dizemos que $u \in D$ é um divisor universal se

- $u \notin U(D)$
- $\forall x \in D$ existe $y \in U(D) \cup \{0\}$ tal que u divide $x-y$

Lema: Seja D domínio (que não corpo) e não possui divisores universais então D Não é domínio euclideano.

Prova:

$\mathbb{Z}[\sqrt{-19}]$ Não possui divisores universais

$\downarrow$

$a+\sqrt{-19}\,b$ que é divisor universal

$U(\mathbb{Z}[\sqrt{-19}]) = \{\pm 1\}$

$x = 2 \in \mathbb{Z}[\sqrt{-19}] \Rightarrow$ u divide

algum entre $\underset{\underset{1}{\shortparallel}}{2-1}$ $\quad \underset{\underset{2}{\shortparallel}}{2-0}$ $\quad \underset{\underset{3}{\shortparallel}}{2+1}$

$a + \sqrt{-19}\, b$ divide 2 a 3

$a^2 + 19b^2$ divide 4 ou 9

$\swarrow$ $a = \pm 2$, $b = 0$

$\downarrow$ $a = \pm 3$, $b = 0$

Logo os possíveis divisores universais são 2 ou 3

Suponhamos 2 divisor universal

$$x = \frac{1+\sqrt{-19}}{2} \Rightarrow 2 \text{ divide } \begin{cases} \dfrac{1+\sqrt{-19}}{2} - 1 \\ \text{ou} \\ \dfrac{1+\sqrt{-19}}{2} \quad \times \\ \dfrac{1+\sqrt{-19}}{2} + 1 \end{cases}$$

3