<u>Teorema</u>: Se D é um domínio de Ideais Principais então D é domínio de Fatoração Única (DIP $\Rightarrow$ DFU)

<u>Prova</u>: Seja D D.I.P e suponhamos que D não é DFU, isto é, existe $a \in D^* \setminus U(D)$ que <u>não</u> se pode escrever como "produto" de irredutíveis
(pode ser só um fator)

Logo em particular a não é irredutível.

assim $a = a_1 b_1$ com $a_1, b_1 \notin U(D)$

Se a_1 e b_1 são produto de irredutíveis então a seria produto de irredutíveis
Podemos supor sem perda de generalidade que a_1 Não é produto de irredutíveis,
pelo mesmo argumentos $a_1 = a_2 b_2$
com $a_2\ b_2 \notin U(D)$ e $\underline{a_2}$ não é produto de irredutíveis

Indutivamente $\underline{a_i = a_{i+1}}\ b_{i+1}$ com

$a_{i+1}, b_{i+1} \notin U(D)$ e a_{i+1} não é produto de irredutíveis ...

Com isto construímos uma sequencia $\{a_j\}$ a_{j+1} divide a_j $\forall i$

Considemos o ideal $I = \langle \underbrace{a_1, a_2, a_3, \dots}_{\text{Sequencia infinita, enumerável}} \rangle$

I está formado exatamente pelas combinações lineares FINITAS dos $\{a_j\}$

$I \subset D$ Logo I é um ideal principal

desta forma $c \in D$ tal qe $I = \langle c \rangle$

$c \in I = \langle a_1, a_2, \dots \rangle$ desta forma

$$\boxed{c = t_1 a_1 + t_2 a_2 + t_3 a_3 + \dots + t_n a_n}$$

para alguns t_j $j = 1, \dots n$

$$\boxed{a_{i+1} \text{ divide } a_i \Rightarrow a_i \in \langle a_{i+1} \rangle}$$

$\Downarrow$

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \dots \subseteq \langle a_n \rangle \subseteq \dots$$

$$\underbrace{a_1, a_2 \dots a_{n-1}, a_n}\in \langle a_n \rangle$$

Logo $c = t_1 a_1 + t_2 a_2 + \dots + t_n a_n \in \langle a_n \rangle$

$\Rightarrow \langle c \rangle \subseteq \langle a_n \rangle$

$$a_{n+1} \in I = \langle c \rangle \subseteq \langle a_n \rangle \Rightarrow \boxed{a_{n+1} = a_n d}$$

$$a_n \in \langle a_{n+1} \rangle \Rightarrow \boxed{a_n = a_{n+1} b_{n+1}}$$

$$a_n = (a_n d) b_{n+1} \Rightarrow a_n (1 - d b_{n+1}) = 0$$

Como estamos em um dominio e $\underline{a_n \neq 0}$

$$\Rightarrow d b_{n+1} = 1 \Rightarrow b_{n+1} \in \underline{U(D)}$$

contraditório.

Falta mostrar unicidade!!

Suponhamos que $\exists a \in D^* \setminus U(D)$

que se pode escrever como produto de irredutíveis de duas formas

$$a = P_1 P_2 \ldots P_s = Q_1 Q_2 \ldots Q_t \Leftarrow$$

com $s \leq t$

Logo P_1 divide $Q_1 Q_2 \ldots Q_t$

Em geral primo $\Rightarrow$ irredutível Se D é DIP então irredutível $\Rightarrow$ primo

Como P_1 é irredutível e D é DIP então

$\left\{\begin{array}{l} P_1 \text{ é } \underline{\text{primo}} \\ P_1 \text{ divide } Q_1 Q_2 \cdots Q_t \end{array}\right. \Rightarrow \exists\, i \in \{1 \ldots t\}$ tal que $\underline{P_1 \text{ divide } Q_i}$

mas Q_i é irredutível. Logo (Podemos supor reordenando que $i=1$)

$$Q_1 = \varepsilon_1 P_1 \qquad \varepsilon_1 \in U(D)$$

$$a = P_1 P_2 \cdots P_s = Q_1 \cdots Q_t = \varepsilon_1 P_1 Q_2 \cdots Q_t$$

$$\Downarrow$$

unidade

$$\boxed{P_2 \cdots P_s = \varepsilon_1 Q_2 \cdots Q_t}$$

de igual forma $Q_2 = \varepsilon_2 P_2 \qquad \varepsilon_2 \in U(D)$

$$P_3 P_4 \cdots P_s = \varepsilon_1 \varepsilon_2 Q_3 \cdots Q_t$$

aplicando o processo s vezes $\quad \underline{Q_i} = \varepsilon_i \underline{P_i}$

$$U(D) \ni 1 = \underbrace{\varepsilon_1 \cdots \varepsilon_s}_{U(D)} \underline{Q_{s+1} \cdots Q_t} \rightarrow \text{ é uma unidade}$$

Logo não pode sobrar nada.

$\Rightarrow s = t$ salvo unidades e ordem a fatoração é única.

$$12 = (-2)(-3)\,2 = 2 \cdot 2 \cdot 3$$

30 Pag 371

ⓐ $1+i \in \mathbb{Z}[i]$

Mostrar que é irredutível

$$(1-i) = (a+ib)(c+id)$$

$$= ac-bd + i(ad+bc)$$

$$\begin{cases} 1 = ac-bd \\ -1 = bc+ad \end{cases} \qquad \boxed{c\ d}$$

$$\Rightarrow \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} \Leftarrow$$

$$\begin{pmatrix} c \\ d \end{pmatrix} = \frac{1}{a^2+b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$= \frac{1}{a^2+b^2} \begin{pmatrix} a-b \\ -b-a \end{pmatrix} \Rightarrow \begin{cases} c = \frac{a-b}{a^2+b^2} \\ d = -\frac{a+b}{a^2+b^2} \end{cases}$$

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

Se $a \neq 0 \Rightarrow$

$$a^2+b^2 \geq 1+b^2 \geq |2b|$$

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

$$\Rightarrow \frac{2b}{a^2+b^2} \leq 1$$

$$\Rightarrow a = \pm 1 \ \text{e} \ b = \pm 1$$

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

$$a = b \Rightarrow c = 0 \quad d = \pm 1 \Rightarrow c+id = \pm i \in \mathcal{U}(\mathbb{Z}[i])$$

$$a = -b \Rightarrow c = \pm 1 \quad d = 0 \Rightarrow c+id = \pm 1 \in \mathcal{U}(\mathbb{Z}[i])$$

Logo $c+id$ é unidade em todo caso

Se $a=0 \Rightarrow c=d$

$$\underbrace{c+d}_{\text{par}} = -\frac{2b}{b^2} = -\frac{2}{b} \Rightarrow \underline{\underline{b=\pm 1}} \text{ ou } \cancel{\pm 2}$$

$a+ib = \pm i$ unidade.

Segunda solução

$$\begin{cases} 1-i = (a+ib)(c+id) \\ 1+i = (a-ib)(c-id) \end{cases}$$ conjugado

$$2 = (a^2+b^2)(c^2+d^2) \in \mathbb{Z}$$

Norma

2 é irredutível em $\mathbb{Z}$

então algum dos fatores é ± 1

Como $a^2+b^2, c^2+d^2 \geq 0 \Rightarrow$ então

podemos supor qe $a^2+b^2 = 1$

mas isso só tem 4 soluções $(\pm 1, 0)$ $(0, \pm 1)$

então $a+ib \in \{\pm 1, \pm i\}$ logo unidade.

Provamos que $1+i$ e $1-i$ são irredutíveis em $\mathbb{Z}[i]$ então $2=(1+i)(1-i)$ OK!! ☺

$$\mathbb{Z}[\sqrt{n}] \xrightarrow{N} \mathbb{Z}$$
$$a+\sqrt{n}b \longmapsto |a^2-nb^2| \Leftarrow$$

$$U(\mathbb{Z}[\sqrt{n}]) = \{a+\sqrt{-n}b \mid N(a+\sqrt{n}b)=1\}$$

$$U(\mathbb{Z}[i]) = \{\pm 1 \ \pm i\}$$

$$U(\mathbb{Z}[\sqrt{-2}]) = \{\pm 1\}$$

$$a^2+2\underline{b}^2=1 \to b=0 \quad a^2=1$$

$$U(\mathbb{Z}[\sqrt{3}]) = \{a+\sqrt{3}b \mid \underbrace{a^2-3b^2=\pm 1}_{\text{Equação de Pell}}\}$$

$$\underbrace{(2-\sqrt{3})}^{j} \in U(\mathbb{Z}[\sqrt{3}]) \quad \forall j \in \mathbb{Z}$$

→ todas as unidade são desta forma!

$U(\mathbb{Z}[\sqrt{n}])$ com n positivo e não quadrado contém infinitas soluções

$$\| $$

$$\{(x_0+\sqrt{-n}\,y_0)^j \mid j\in\mathbb{Z}\}$$

Teorema!!

solução fundamental

$$(1+i)(1-i)=2 \qquad (1+i)\cdot\left(\frac{1-i}{2}\right)=1$$

$$\Rightarrow (1+i)\cdot\left(\frac{1}{2}-\frac{1}{2}i\right)=1$$

$$\cancel{A}\in\mathbb{C} \qquad \mathbb{Z}[i]\subseteq\mathbb{C}$$

$$\mathbb{Z}[i]$$

anel, corpo

$$A\subseteq K$$

$$a\in A \qquad a\in K \qquad ab=1$$

$$c\in A \text{ tq } ac=1 \Rightarrow \boxed{c=b}$$

Logo basta verificar que se $b\in A$

3. Falso ou verdadeiro

(a) $\underbrace{a \mid b}_{b = at}$ e $\underbrace{c \mid d}_{d = cs}$ $\Rightarrow$ $ac \mid bd$

$\Rightarrow (bd) = atcs = (ac)ts$

Verdadeiro.

(b) $a \mid b$ $\quad c \mid d$ $\Rightarrow$ $(a+c) \mid b+d$

$\mathbb{Z}$ $\quad 1 \mid 2, \; 1 \mid 3 \Rightarrow (1+1) \mid (2+3)$

↑ falso

Aula de Dúvidas

Segunda 19:30 Teams!!

//

D anel com identidade (com unidade) $\Rightarrow \mathcal{U}(D) = \left\{ a \in D \;\middle|\; \begin{array}{l} \exists b \in D \\ ab = ba = 1 \end{array} \right\}$

i.e. com elemento neutro para o produto

$\mathcal{U}(\mathbb{Z}) = \{\pm 1\}$ $\qquad \mathcal{U}(\mathbb{R}) = \mathbb{R}^*$

em geral $\mathbb{K}$ corpo $\qquad \mathcal{U}(\mathbb{K}) = \mathbb{K}^*$