$I \subseteq A$

$\downarrow$

ideal que não é primo

$\exists\, ab \in I$ mas $a, b \notin I$

$A \to \dfrac{A}{I}$ sobre

$a \mapsto \bar{a}$

Dominio de Ideais principais

$a \mapsto \bar{a} \neq \bar{0}$

$b \mapsto \bar{b} \neq \bar{0}$

$\bar{a}\bar{b} = \overline{ab} = \bar{0}$

$(4) \subseteq \mathbb{Z} \to \dfrac{\mathbb{Z}}{4\mathbb{Z}}$ ✓

Ideal não primo

A

$A \xrightarrow{\psi} B \setminus \{b\}$

$a \mapsto -b$

$-a \mapsto b$ X.

se ψ homo então

$\Rightarrow \psi(A)$ sempre é anel

$\cdot\, b_1, b_2 \Rightarrow \psi(a_1) = b_1$

$\psi(a_2) = b_2$

$\Rightarrow \psi(a_1 + a_2) = \psi(a_1) + \psi(a_2)$

$= b_1 + b_2$

$\psi(a_1 a_2) = b_1 b_2$

$\boxed{\mathbb{Z}_4 = \{1, 2, 3, 0\} \rightsquigarrow \{2, 0\} \text{ anel}}$

$$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \left\{ a + b\,\frac{1+\sqrt{-3}}{2} \;\middle|\; a,b\in\mathbb{Z} \right.$$

$$\frac{2a+b+b\sqrt{-3}}{2} = \left\{ \frac{c+d\sqrt{-3}}{2} \;\middle|\; \begin{array}{l} c,d\in\mathbb{Z} \\ c+d \text{ par} \end{array} \right)$$

$$N\left(\frac{c+d\sqrt{-3}}{2}\right) = 1 = c$$

$$\frac{c+d\sqrt{-3}}{2}\cdot\frac{e+f\sqrt{-3}}{2} = 1$$

$$(ce-3df)+\sqrt{-3}\,(cf+de) = 4$$

$$\begin{cases} ce-3df = 4 \\ de+cf = 0 \end{cases} \qquad \begin{pmatrix} c & -3d \\ d & c \end{pmatrix}\begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} 4 \\ 0 \end{pmatrix}$$

tal qe $e+f$ par. $e,f\in\mathbb{Z}$

$$\begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} c & -3d \\ d & c \end{pmatrix}^{-1}\begin{pmatrix} 4 \\ 0 \end{pmatrix}$$

$$= \frac{1}{c^2+3d^2}\begin{pmatrix} 4c \\ -4d \end{pmatrix} = \begin{pmatrix} \frac{4c}{c^2+3d^2} \\ \frac{-4d}{c^2+d^2} \end{pmatrix}$$

$d = \underline{0} \Rightarrow \frac{4c}{c^2} \in \mathbb{Z} \quad \frac{4}{c} \in \mathbb{Z} \quad c \in \{\underline{\pm 1}\ \pm 2\ \pm 4\}$

$\frac{\pm 2 + 0\sqrt{-3}}{2} = \underline{\pm 1} \qquad \frac{\pm 4 + 0\sqrt{-3}}{2} = \underline{\pm 2}$

$d \neq 0 \qquad \underline{c^2 + 3d^2} \geq c^2 + 3 \overset{?}{\geq} \underline{4c}$

$c^2 - 4c + 3 \geq 0 \Rightarrow (c-3)(c-1) \geq 0$

$c \geq 3$

$c \leq 1$

$c = 1,\ c = 2,\ c = 3$

$c = 1 \rightsquigarrow \frac{4}{1+3d^2} \rightsquigarrow d = \pm 1 \qquad \frac{1 \pm \sqrt{-3}}{2}$

$c = 2 \qquad \frac{4}{4+3d^2}$

$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \subseteq \mathbb{C} \Rightarrow \left(\frac{a+b\sqrt{-3}}{2}\right)^{-1} = \frac{2}{a+b\sqrt{-3}} \in \mathbb{C}$

$\frac{2(a - b\sqrt{-3})}{a^2+3b^2} = \underset{\in \mathbb{Z}}{\frac{2a}{a^2+3b^2}} - \underset{\in \mathbb{Z}}{\frac{2b}{a^2+3b^2}}\sqrt{-3}$

$$\underbrace{\left(c+d\,\frac{1+\sqrt{-3}}{2}\right)}^{-1} = \left(\frac{2c+d+d\sqrt{-3}}{2}\right)^{-1}$$

$$\frac{a+b}{a^2+ab+b^2} - \frac{b}{a^2+ab+b^2}\,\frac{1+\sqrt{-3}}{2}$$

$c=a+b$ $\qquad a=b-c \qquad (b-c)^2+b(b-c)+b^2$

$$\frac{c}{} \qquad b^2-2bc+c^2+b^2-bc+b^2$$

$\Uparrow$

K corpo $\qquad [K:\mathbb{Q}]=\underline{n}<\infty$

$|$

$\mathbb{Q}$ $\qquad \tau : K \to \mathbb{C}$ $\qquad \tau$ <u>homomorfismo</u>

qe <u>fixam $\mathbb{Q}$</u>

Existem $\underbrace{\tau_1\ \tau_2\ \dots\ \tau_n}$

$$N : K \to \mathbb{Q}$$

$$a \longmapsto \underbrace{\tau_1(a)\,\tau_1(a)\cdots\tau_n(a)}$$

$K = \mathbb{Q}(\sqrt[3]{2})$ $\Big]\, 3$ $\longrightarrow$ $1, \sqrt[3]{2}, \sqrt[3]{4}$ base de $\mathbb{Q}(\sqrt[3]{2})$ sobre $\mathbb{Q}$

$\mathbb{Q}$

$$\tau : \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{C}$$

$$\sqrt[3]{2} \longmapsto \ ? \begin{cases} \sqrt[3]{2} \\ \sqrt[3]{2}\,\xi_3 \notin \mathbb{Q}(\sqrt[3]{2}) \\ \sqrt[3]{2}\,\xi_3^2 \end{cases}$$

$$\boxed{X^3 - 2 = 0}$$

$\tau(\sqrt[3]{2}) = u$??

$\tau(\sqrt[3]{2})^3 = u^3 = \tau(2) = 2$

$$K = \langle \sqrt[j]{2} \rangle_{j \in \mathbb{N}} \subseteq \mathbb{C}$$

$$K_n := \langle \sqrt[2]{2}, \sqrt[3]{2}, \dots, \sqrt[n]{2} \rangle \Leftarrow$$

$\mathbb{Q}$

$$K_n \subseteq K_{n+1} \subseteq K_{n+2} \dots$$

$$K = \bigcup_{n=1}^{\infty} K_n \text{ é um corpo}$$

$\mathbb{Q}$

$$[K ; \mathbb{Q}] = \infty$$

- $\alpha, \beta \in K = \bigcup_{n=1}^{\infty} K_n \Rightarrow \exists \underline{N}$ tal que

$\alpha, \beta \in K_N \Rightarrow$
- $\alpha+\beta \in K_N \subset K$
- $\alpha \cdot \beta \in K_N \subset K$
- $\alpha^{-1} \in K_N \subset K$

$$\begin{array}{c} K \\ | \\ L \end{array}$$

falamos que a extensão é finita se K visto como L-espaço vetorial tem dimensão finita

Logo $[K:L] := \dim_L K = n$

Logo existem $\alpha_1, \alpha_2 \ldots \alpha_n \in K$ tal que $K = \alpha_1 L \oplus \alpha_2 L \oplus \cdots \oplus \alpha_n L$

$$\begin{array}{c} | \\ \mathbb{C}\{x\} \\ | \\ \mathbb{C} \end{array}$$

$\mathbb{C}\{x\}$ = Corpo de frações de polinomios

$$= \left\{ \frac{P(x)}{Q(x)} \;\middle|\; \begin{array}{c} P(x)\ Q(x) \in \mathbb{C}[x] \\ Q(x) \neq 0 \end{array} \right\}$$

Teorema:
Se K é corpo então existe $\overline{K}$ que contém K e é algebricamente fechado

Prova: Lema de Zorn

$\mathbb{Z} \rightarrow$ Dominio Euclideano $\Rightarrow$ D.I.P. $\Rightarrow$ DFU

$\mathbb{Z}[x] \supseteq (2, x)$ não é principal

$\downarrow$

Não é DIP $\Rightarrow$ Não é D.E.

Em geral se D é DIP mas não é corpo então $D[x]$ Não é PIP (se D é corpo $\Rightarrow$ $D[x]$ e D.E.)

Como não é corpo $\Rightarrow$ $a \notin U(D)$

$\langle a, x \rangle$ é ideal de $D[x]$

mas não é principal pois caso contrario $\langle a, x \rangle = \langle f(x) \rangle$

tal que $\quad f(x)$ divide $a \Rightarrow f(x) = c$
$\quad f(x)$ divide x

$\Rightarrow c$ divide $x \quad \Rightarrow x = c \cdot (\underset{\underset{D[x]}{\cap}}{c^{-1}x})$

$\Rightarrow c^{-1} \in D \Rightarrow c$ é uma unidade

$\Rightarrow \langle f(x) \rangle = \langle c \rangle = D$

mas $\quad 1 \notin \langle a, x \rangle \quad$ pois

$$1 = \underbrace{a\, g(x)}_{\downarrow} + \underbrace{x h(x)}_{\uparrow}$$

$1 = ab_0 + \dots + x(\dots) \quad \Rightarrow 1 = ab_0 \Rightarrow a \in U(D)$
contraditório

<u>Teorema</u>: Se D é D.F.U. então $D[x]$ é D.F.U.

<u>Def</u>: Dizemos que $I \subset D$ é gerado por $\{\alpha_j\}_{j \in J}$ se todo elemento $\beta \in I$ pode-se escrever como uma combinação linear <u>finita</u> dos $\{\alpha_j\}_{j \in J}$

i.e., existem $j_1, j_2 \dots j_s \in J$ e

$a_1, a_2, \dots a_s \in D$ tal que $\beta = a_1\alpha_{j_1} + a_2\alpha_{j_2} + \dots + a_s\alpha_{j_s}$

<u>Def</u>: Um ideal I é finitamente gerado se existem $\alpha_1, \alpha_2 \dots \alpha_\ell$ $\ell \in \mathbb{N}$ tal que

$$\langle \alpha_1, \alpha_2, \dots, \alpha_\ell \rangle_D = I$$

<u>Def</u>: Um ideal I é principal se existe $\alpha \in I$ tal que $I = \langle \alpha \rangle$

Em $\mathbb{Z} \Rightarrow \langle 12, 15 \rangle = \langle 3 \rangle$

$$\langle n_1, \dots, n_k \rangle = \langle mdc(n_1, \dots n_k) \rangle$$

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \to$ DIP que não é DE

$\mathbb{Z}[x] \to$ DFU mas não é DIP

$mdc(2, x) = 1$ $\qquad 1 = 2f(x) + xg(x)$

Não é possível

I está contido em alguns ideais primos $P_1\ P_2 \dots P_k$

Dizemos que D tem fatoração única de ideais se $I = P_1^{e_1} \cdots P_k^{e_k}$ ideais primo de forma única

$$\boxed{\begin{gathered} AB = \langle ab \mid a \in A\ \ b \in B \rangle \subset A \subseteq D \\ AB \subseteq A \cap B \end{gathered}}$$

$\mathbb{Z}$

$$X^2 + Y^2 = Z^2$$

$mdc(x,y) = 1$

resolver nos números inteiros

$$(X+iy)(x-iy) = \underset{p_1^{2e_1} p_2^{2e_2} \cdots p_t^{2e_t}}{z^2}$$

primo

$\mathbb{Z}[i]$

DE

$\Downarrow$

DFU

$mdc(x+iy,\ x-iy) = mdc(2x,\ x-iy) = mdc(2,\ x-iy)$

$mdc(x,\ x-iy) = mdc(x,-iy) = mdc(x,y) = 1$

$2 = (1+i)(1-i) \longrightarrow mdc(2,\ x-iy) = 1,\ 1+i,\ 1-i$

$x = \pm 1 \quad y = \pm 1$ não é solução da eq.

$$x + iy = (m + in)^2 \Rightarrow z = (m+in)(m-in)$$

$\mathbb{Z}[i]$

$$= m^2 + 2mni - n^2$$

$$\left\{\begin{array}{l} x = m^2 - n^2 \\ y = 2mn \\ z = m^2 + n^2 \end{array}\right\}$$ Todas as soluções com $mdc(x,y) = 1$

$\rightarrow \underline{(m,n) = 1}$ $\underline{m+n \text{ ímpar}}$

$\rightarrow$ Triplas pitagóricas primitivos

$$\left\{\begin{array}{l} x = (m^2 - n^2)\ell \\ y = 2mn\ell \\ z = (m^2 + n^2)\ell \end{array}\right\}$$ Todas as triplas pitagóricas

$m = 5$ $\quad n = 2$

$$\left.\begin{array}{l} x = 21 \\ y = 20 \\ z = 29 \end{array}\right\}$$