Domínios (de integridade)

$D \rightarrow$ Anel comutativo com unidade tal que não tem divisores de zero ($ab=0 \Rightarrow a=0$ ou $b=0$)

$I \rightarrow$ I é ideal primo sempre que se tem que $ab \in I \Rightarrow a \in I$ ou $b \in I$

$\rightarrow$ I é ideal maximal se $\nexists J$ ideal $I \subsetneq J \subsetneq D$

$$\boxed{\text{Teorema: Maximal} \Rightarrow \text{Primo}}$$

$(\Leftarrow)$ Não necessariamente é verdade

$\mathbb{Z}[x] \rightarrow I_1 = (2)$ $I_2 = (x)$ são ideais primos que não são maximais

---

$\mathbb{R}[x_1, x_2, x_3]$ $I_1 = (x_1)$ $I_2 = (x_1, x_2)$

$I_3 = (x_1, x_2, x_3)$

$I_1 = \{ x_1 f(x_1, x_2, x_3) \mid f(x_1, x_2, x_3) \in \mathbb{R}[x_1, x_2, x_3] \}$ é ideal primo

Pois $g(x_1,x_2,x_3)\,h(x_1,x_2,x_3) \in I_1 \Rightarrow x_1$ divide $g \cdot h$

$\Rightarrow x_1$ divide g ou h $\Rightarrow$ $g \in I_1$ ou $h \in I_1$

I_2 tambem é ideal primo e I_3 também

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \mathbb{R}[x_1,x_2,x_3]$$

Pois I_3 não contém os polinomios que tem coeficiente constante $\neq 0$

$nm \in 3\mathbb{Z} \subseteq \mathbb{Z}$ $\quad 3 \mid mn \Rightarrow \begin{cases} 3 \mid m \\ \text{ou} \\ 3 \mid n \end{cases}$

$6\mathbb{Z} \subseteq \mathbb{Z}$ $\rightarrow$ não é ideal primo

por $2 \cdot 3 = 6 \in 6\mathbb{Z}$ mas $2 \notin 6\mathbb{Z}$, $3 \notin 6\mathbb{Z}$

---

em $\mathbb{Z}$ Ideais primo $\Leftrightarrow$ Ideais maximais

---

$\dfrac{D}{P}$ $\rightsquigarrow$ dominio

$P \leftarrow$ primo

$\dfrac{P}{M}$ $\longrightarrow$ Corpo

$M \leftarrow$ maximo

$(L, +, \cdot)$ é um corpo se
- $(L, +, \cdot)$ é um <u>domínio</u>
- $(L^*, \cdot)$ é grupo

$$\left.\begin{array}{l} (\mathbb{Q}, +, \cdot) \\ \cap\!| \\ (\mathbb{R}, +, \cdot) \\ (\mathbb{C}, +, \cdot) \end{array}\right\} \text{Corpos}$$

- $(\mathbb{Q}^* \cdot)$ é um grupo
- $(\mathbb{Q}, +, \cdot)$ domínio

$$\mathbb{Q}[\sqrt{2}] \overset{\subseteq \mathbb{R}}{=} \{ \underline{\underline{a + \sqrt{2}\, b}} \mid a, b \in \mathbb{Q} \}$$

é um corpo.

Porque $(a + \sqrt{2}\, b)(c + \sqrt{2}\, d)$ $\quad a, b, c, d \in \mathbb{Q}$

$$ac + \sqrt{2}\, ad + \sqrt{2}\, bc + 2bd$$

$$= (\underbrace{ac + 2bd}_{\in \mathbb{Q}}) + \sqrt{2}(\underbrace{ad + bc}_{\in \mathbb{Q}}) \in \mathbb{Q}[\sqrt{2}]$$

$$(a + \sqrt{2}\, b)^{-1} = \frac{1}{a + \sqrt{2}\, b} = \frac{a - \sqrt{2}\, b}{a^2 - 2b^2}$$

$$= \underbrace{\frac{a}{a^2 - 2b^2}}_{\in \mathbb{Q}} - \sqrt{2}\, \underbrace{\frac{b}{a^2 - 2b^2}}_{\in \mathbb{Q}} \in \mathbb{Q}[\sqrt{2}]$$

$$\mathbb{Q}[\sqrt[3]{2}] = \{ a + \sqrt[3]{2}\, b + \sqrt[3]{4}\, c \mid a,b,c \in \mathbb{Q} \}$$

é um corpo!!

$$(a + \sqrt[3]{2}\, b + \sqrt[3]{4}\, c)(d + \sqrt[3]{2}\, f + \sqrt[3]{4}\, g) \overset{?}{=} 1$$

$$= (\underbrace{ad + 2bg + 2cf}_{=1}) + (a\underbrace{f + bd + 2cg}_{=0})\sqrt[3]{2}$$

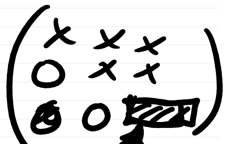
$$+ (\underbrace{cd + bf + ag}_{=0})\sqrt[3]{4} \qquad \text{fechado}$$

$$\begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix} \begin{pmatrix} d \\ f \\ g \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$\det \begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix} = a(a^2 - 2cb) - 2c(ab - 2c^2)$$
$$+ 2b(b^2 - ac)$$

$$a^3 - 2abc - 2abc + 4c^3 + 2b^3 - 2abc$$

Escalonando



$$\boxed{a^3 + 2b^3 + 4c^3 - 6abc = 0 \;??}$$

tem solução racional não trivial.

$$(a + \sqrt[3]{2}\, b + \sqrt[3]{4}\, c)(a + \sqrt[3]{2}\, \xi b + \sqrt[3]{4}\, \xi^2 c)(a + \sqrt[3]{2}\, \xi^2 b + \sqrt[3]{4}\, \xi c)$$

onde $\xi^3 = 1$ com $\xi \neq 1$

$$\xi^3 - 1 = (\xi - 1)\underbrace{(\xi^2 + \xi + 1)}_{=0} \qquad \xi = \frac{-1+\sqrt{-3}}{2}$$

$$\Rightarrow a + \sqrt[3]{2}\, b + \sqrt[3]{4}\, c = 0 \Rightarrow a = b = c = 0 \quad \text{i.e.}$$

$\Rightarrow 1, \sqrt[3]{2}, \sqrt[2]{4}$ são L.I. sobre $\mathbb{Q}$!! (Pensar)

$$\boxed{(\sqrt{2} - \sqrt{3}) + (\sqrt{3} - \sqrt{5}) + (\sqrt{5} - \sqrt{2}) = 0}$$

Irracional Irracional

Exemplo:

$\mathbb{Z}_p$ corpo finito com p elementos $\qquad \mathbb{Z}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ ← maximal

---

$\mathbb{Q}[x] \ni f(x) \qquad f(x)$ irredutível !!

$f(x) = x^2 + 1 \qquad f(x) = x^2 - 3$

$I = (f(x))$ ideal gerado por $f(x)$

Afirmação: I é maximal!

Suponhamos que $\exists\ J$ ideal

$$I \subsetneq J \subsetneq \mathbb{Q}[x]$$

$\exists\ g(x) \in J \setminus I \Rightarrow g(x)$ não é divisível por $f(x)$

$\downarrow$

$$\mathrm{mdc}(f(x), g(x)) = 1$$

existem $a(x)$ e $b(x) \in \mathbb{Q}[x]$ tais que

$$\underbrace{a(x)f(x)}_{\in I \subseteq J} + \underbrace{b(x)g(x)}_{\in J} = 1 \in J$$

$1 \in J \Rightarrow \mathbb{Q}[x] \subseteq J$ contraditório

---

$\dfrac{\mathbb{Q}[x]}{(f(x))} \leftarrow$ é um corpo.

$(f(x))$ ← maximal

$f(x)$ irredutível em $\mathbb{Q}[x]$

$\downarrow$

$\exists\ \alpha \in \mathbb{C}$ tq $f(\alpha) = 0$

$\dfrac{\mathbb{Q}[x]}{(f(x))}$ corpo ✓

Afirmação $\dfrac{\mathbb{Q}[x]}{(f(x))} \simeq \mathbb{Q}[\alpha]$

↑ menor anel que contém $\mathbb{Q}$ e α

$$\psi: \mathbb{Q}[x] \longrightarrow \mathbb{Q}[\alpha]$$ ψ homomorfismo

$$x \longmapsto \alpha$$

$$\mathbb{Q} \ni a \longmapsto a.$$

$$\psi(x^2) = \psi(x)^2 = \alpha^2$$

$$\psi(3x+2x^2) = \psi(3x) + \psi(2x^2)$$

$$= \psi(3)\psi(x) + \psi(2)\psi(x)\psi(x)$$

$$= 3\alpha + 2\alpha^2$$

Em geral $\mathbb{Q}[x] \ni h(x) \longmapsto h(\alpha)$

ψ é homomorfismo de aneis. que é sobre

$$\mathrm{Ker}(\psi) = \{ h(x) \in \mathbb{Q}[x] \mid \psi(h(x)) = h(\alpha) = 0 \}$$

Afirmação $\mathrm{Ker}(\psi) = (\underline{f(x)})$

$(\supseteq)$ $g(x)f(x) \in (f(x)) \Rightarrow \psi(g(x)f(x)) = g(\alpha)f(\alpha) = 0$

$\Rightarrow g(x)f(x) \in \mathrm{Ker}(\psi)$

$(f(x)) \subseteq \mathrm{Ker}(\psi)$ é um ideal maximal

Logo $\quad Ker(\psi) = (f(x))$

ou

$Ker(\psi) = \mathbb{Q}[x]$

$1 \in \mathbb{Q}[x] \quad \psi(1) = 1 \neq 0 \Rightarrow 1 \notin Ker(\psi)$

Logo $\quad Ker(\psi) \neq \mathbb{Q}[x]$

Concluímos $\quad Ker(\psi) = (f)$

Pelo teorema de homomorfismo de anéis

$$\mathbb{Q}\text{ F } \frac{\mathbb{Q}[x]}{(f(x))} = \frac{\mathbb{Q}[x]}{Ker(\psi)} \approx \mathbb{Q}[\alpha]$$

isomorfos

Em particular $\mathbb{Q}[\alpha]$ é um corpo.

$$\alpha = \sqrt[3]{2} \longrightarrow x^2 - 2 = 0 \Rightarrow \frac{\mathbb{Q}[x]}{(x^2-2)} \simeq \mathbb{Q}[\sqrt[3]{2}]$$

corpo $\qquad$ corpo

Se $\alpha \in \mathbb{C}$ tal que é raiz de um polinomio com coeficientes racionais então $\mathbb{Q}[\alpha]$ é um corpo!!

$\mathbb{Q} \subsetneq \mathbb{Q}[\sqrt{2}] \subsetneq \mathbb{Q}[\sqrt{2}, \sqrt[3]{3}] \subsetneq \mathbb{Q}[\sqrt{2}, \sqrt[3]{3}, \sqrt{11}]$

$A := \{ \alpha \in \mathbb{C} \mid \alpha$ é raiz de um polinomio com coef $\mathbb{Q} \}$

A corpo dos números algebricos

Teorema: A é enumeravel

Logo $A \subsetneq \mathbb{C}$ não enumeravel

$\mathbb{C}[x] \ni f(x)$ é iredutivel $\Updownarrow$ Teo. Fund. Algebra

$ax+b$ $\quad$ $f(x)$ tem grau 1.

$$\frac{\mathbb{C}[x]}{(f(x))} \simeq \mathbb{C}$$

Teorema: Seja L corpo então existe um corp $\overline{L}$ tal que

- $L \subseteq \overline{L}$
- $\overline{L}$ é algebricamente fechado

Teorema:
Em $\mathbb{R}[x]$ os únicos polinomios iredutíveis são de grau ≤ 2

$f(x) \in \mathbb{R}[x]$ e seja $\alpha \in \mathbb{C} \setminus \mathbb{R}$ raiz de f ie $f(\alpha) = 0$

Consideremos $h(x) = (x - \alpha)(x - \bar{\alpha})$

$$h(x) = x^2 - \underset{\substack{\Uparrow \\ \mathbb{R}}}{(\alpha + \bar{\alpha})} x + \underset{\substack{\Uparrow \\ \mathbb{R}}}{\alpha\bar{\alpha}} \in \mathbb{R}[x]$$

$$f(\alpha) = 0 \Rightarrow \overline{f(\alpha)} = \bar{0} = 0$$

$$\overline{f(\alpha)} = f(\bar{\alpha}) \Rightarrow \bar{\alpha} \text{ é raiz de } f$$

$\Rightarrow$ Logo $\underset{\substack{\Uparrow \\ \mathbb{R}[x]}}{h(x)}$ divide $f(x)$ ← iredutível em $\mathbb{R}[x]$

grau 2

$\Rightarrow f(x) = h(x)$

Se pego $f(x)$ iredutível de grau 2

$$\mathbb{R} \subsetneq \frac{\mathbb{R}[x]}{(f(x))} \simeq \mathbb{R}[\alpha] \subseteq \mathbb{C} = \mathbb{R}[i]$$

$$\mathbb{R}[i] = \frac{\mathbb{R}[x]}{(x^2+1)}$$

$$\Downarrow$$

$$\mathbb{R}[\alpha] = \mathbb{C}$$