Aneis

$(A + \cdot)$ → $(A +)$ grupo abeliano
→ A fechado com respeito a $\cdot$ associativa
→ Distributiva

- $\underline{1 \in A}$ (elemento neutro com respeito a $\cdot$)
dizemos que A é anel com unidade

→ $(2\mathbb{Z}, +, \cdot)$ anel sem unidade

- A é comutativo se $ab = ba$ $\forall a, b \in A$

- A é chamado de <u>dominio de integridade</u>
  - se $\exists 1 \in A$. A comutativo
  - se sempre que

$a \cdot b = 0$ então $a = 0$ ou $b = 0$

↓

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ são dominios (de integridade)

Se $(\mathbb{Z}_{12}, +, \cdot)$ <u>não é domínio</u>

$4, 3 \in \mathbb{Z}_{12}$ com $4 \cdot 3 = 0$

A anel arbitrário com unidade

$I \subseteq A$ ideal

<u>Def</u>: $\frac{A}{I}$ anel quocente, o anel das classes de equivalencia i.e.

$a \sim b$ se $a-b \in I$

a classe sera denotado por $[a]$ ou $\bar{a}$

Exemplo $\mathbb{Z} \supset 12\mathbb{Z} = I = (12)$

$\frac{\mathbb{Z}}{I} = \mathbb{Z}_{12}$ → é um anel quocente

---

$\mathbb{Z} \supseteq I$ $\underbrace{I \text{ ideal}}$ e denotemos por n o mínimo elemento positivo de I

$n \in I \Rightarrow (n) \subseteq I$ (afirmamos que $I = (n)$)

Suponhamos que $(n) \subsetneq I$ Logo existe $m \in I \setminus (n)$, como $-m \in I \setminus (n)$ então podemos supor $m > 0$

dividindo m entre n $m = nq + r$ com $0 < r < n$ (algoritmo da divisão)

$$\underset{\underset{I}{\cap}}{r = m} - \underset{\underset{I}{\cap}}{nq} \in I \Rightarrow$$

Isto é contraditório pois $0 < r < n$ e $r \in I$

o que contradiz a minimalidade de n

· Todo ideal de $\mathbb{Z}$ é da forma (n)

e $\frac{\mathbb{Z}}{(n)} = \mathbb{Z}_n$ e

$\frac{\mathbb{Z}}{(n)}$ é domínio $\Leftrightarrow \nexists\ \bar{a}, \bar{b} \in \mathbb{Z}_n \setminus \{0\}$

tais que $\bar{a}\bar{b} = \bar{0}$

Se n é composto $n = ab$ então

$\mathbb{Z}_n$ não é domínio $\begin{matrix} \bar{a} \neq \bar{0} \\ \bar{b} \neq 0 \end{matrix} \Rightarrow \overline{ab} = 0$

Se $n = p$ $\qquad \mathbb{Z}_p = \frac{\mathbb{Z}}{(p)}$

Se $\bar{a}\bar{b} = 0 \Rightarrow p \mid ab$ $\begin{cases} p \mid a \\ \text{ou} \\ p \mid b \end{cases}$

$\Rightarrow \bar{a} = 0$ ou $\bar{b} = 0$

$$\boxed{\mathbb{Z}_n \text{ dominio} \iff n \text{ é primo}}$$

Exemplo:

$\mathbb{Z}[x] \to$ polinomios com coeficientes inteiros

é dominio $\qquad 1 \in \mathbb{Z}[x]$, $\mathbb{Z}[x]$ comutativo

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \qquad a_n \neq 0$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0 \qquad b_n \neq 0$$

$$f(x)g(x) = \underset{= 0}{a_n b_m} x^{m+n} + \underset{= 0}{(a_n b_{m-1} + a_{n-1} b_m)} x^{m+n-1} + \cdots + \underset{= 0}{a_0 b_0}$$

$= 0$ polinomio zero

em particular $\Rightarrow a_n b_m = 0$ contraditorio

pois $a_n, b_m \neq 0$

$I \subseteq \mathbb{Z}[x]$ $\qquad I_1 = 2\mathbb{Z}[x] \to$ $\left\{\text{polinomios com coeficientes pares}\right.$

exemplos

$I_2 = x\mathbb{Z}[x] \to$ $\left\{\text{polinomios sem termo constante}\right.$

Seja $f(x)$ um polinomio de grau mínimo dentro de I $\quad f(x) \in I$

Logo $(f(x)) \subseteq I$

Se $(f(x)) = I$ ✓

Caso contrario $I \setminus (f(x)) \neq \phi$

seja $g(x)$ polinomio de grau mínimo em $I \setminus (f(x))$

dividindo $g(x)$ entre $f(x)$ (em $\mathbb{Q}[x]$)

$$\begin{array}{r|l} x^2 & 2x+1 \\ \cline{2-2} -x^2-\frac{1}{2}x & \\ \frac{1}{4} & \frac{1}{2}x-\frac{1}{4} \end{array} \qquad x^2 = (2x+1)\left(\frac{1}{2}x-\frac{1}{4}\right)+\frac{1}{4}$$

$$g(x) = q(x)\,f(x) + r(x)$$

$\underline{\underline{q(x)}}$ $\underline{\underline{r(x)}} \in \mathbb{Q}[x]$

$L = \text{mmc}(\text{denominadores})$

$$L\,g(x) = \underset{\mathbb{Z}[x]}{\underset{\cap}{L\cdot q(x)}}\, f(x) + \underset{\mathbb{Z}[x]}{\underset{\cap}{L\cdot r(x)}}$$

$$L \cdot r(x) = \underset{\substack{\Uparrow \\ I}}{L\, g(x)} - L\, q(x) \underset{\substack{\Uparrow \\ I}}{\underline{f(x)}} \in I$$

mas $\quad grau(r) < grau(f) \Rightarrow r \equiv 0$

Conclusão: para cada $g(x) \in I$ existe $L \in \mathbb{Z}^*$ tal que $L\, g(x) \in \langle f(x) \rangle$.

$$I = \langle 2, x \rangle = \{ 2 f(x) + \underbrace{x\, g(x)} \mid f, g \in \mathbb{Z}[x] \}$$

= polinomios com coeficiente independente par

$x \notin \langle 2 \rangle \qquad 2 \notin \langle x \rangle$

Se I é ideal de $\mathbb{Z}[x]$

$\dfrac{\mathbb{Z}[x]}{I}$ é domínio ?

$\Updownarrow$

precisamos que não existam $h(x), \ell(x)$

$h(x), \ell(x) \notin I$ tal que $h(x)\, \ell(x) \in I$

Se $I = (2, x)$

$\overline{h(x)}\,\overline{l(x)} = 0 \iff \underbrace{h(x)\,l(x)}\ \in I \iff$ coeficiente independente é par. $\iff$

o coeficiente independente de $h(x)$ ou de $l(x)$ tem que ser par $\iff$

$h(x)$ ou $l(x)$ pertence a I $\iff \left\{ \begin{array}{l} \overline{h(x)} = 0 \\ \text{ou} \\ \overline{l(x)} = 0 \end{array} \right.$

Teorema: A anel comutativo com unidade e $I \subset A$ ideal então $\frac{A}{I}$ é domínio se sempre que $ab \in I \Rightarrow \left\{ \begin{array}{l} a \in I \\ \text{ou} \\ b \in I \end{array} \right.$

Def: Se $I \subset A$ um ideal é chamado de ideal primo se sempre que $ab \in I \Rightarrow \left\{ \begin{array}{l} a \in I \\ \text{ou} \\ b \in I \end{array} \right.$

Def: $I \subset A$ ideal

$$\frac{A}{I} = \{\bar{a} \mid a \in A\} \qquad a \sim b \iff a - b \in I$$

$$\left(\frac{A}{I}, \oplus, \odot\right) \qquad \bar{a}, \bar{b} \in \frac{A}{I}$$

$$\begin{cases} \bar{a} \oplus \bar{b} := \overline{a+b} \\ \bar{a} \odot \bar{b} := \overline{a \cdot b} \end{cases}$$ (estão bem definidas)

$$a_1 \sim a_2 \qquad b_1 \sim b_2$$

Pergunta: $\overline{a_1 + b_1} = \overline{a_2 + b_2}$?

$$\iff (a_1 + b_1) - (a_2 + b_2) \in I \,?$$

$$= \underbrace{(a_1 - a_2)}_{\in I} + \underbrace{(b_1 - b_2)}_{\in I} \in I \; ✓$$

$\mathbb{Z}_{12}$ $\quad \bar{4} = \{\ldots, -20, -8, 4, 16, 28, \ldots\}$

$\bar{6} = \{\ldots -18, -6, 6, 18, 30, \ldots\}$

$\bar{4} + \bar{6} = \overline{10} = \{\ldots\ldots, -2, 10, 22, 34 \ldots\}$

$\bar{8} + \overline{10} = \bar{4}$

$\dfrac{A}{I}$ } domínio $\Longleftrightarrow$ I é ideal primo.

$\mathbb{Z} \supset p\mathbb{Z} \rightsquigarrow \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ domínio
p primo

<u>Def</u>: $I \subset A$ é um ideal maximal se $\nexists$ J ideal com $I \subsetneq J \subsetneq A$

<u>Teorema</u>: Todo ideal maximal é Ideal primo (maximal $\Rightarrow$ primo) $\not\Leftarrow$

<u>Prova</u>: $I \subset A$ ideal <u>maximal</u> e

seja $a, b \in A$ tais que $a \cdot b \in I$

Suponhamos que $a \notin I$ e $b \notin I$

definimos

$J = \langle a, I \rangle = \{ta + si \mid t, s \in A, i \in I\}$

J é ideal

$$\underbrace{(t_1a+s_1i_1)+(t_2a+s_2i_2)}_{\in J} = \underbrace{(t_1+t_2)}_{\in A}a + \underbrace{(s_1i_1+s_2i_2)}_{\in J}$$

$$\underbrace{c}_{\in A}(ta+s\underbrace{i}_{\in I}) = \underbrace{(ct)}_{\in A}a + cs\underbrace{i}_{\in I} \in J$$

Logo J é ideal e por construção $\begin{matrix} I \subseteq J \\ a \in J \end{matrix} \Rightarrow I \subsetneq J$

Como I é maximal segue que

$J = A \ni 1 \Rightarrow$ em particular $1 \in J$

$$\begin{cases} 1 = ta + i & \text{para alguns } t \in A \setminus I,\ i \in I \\ ab \in I. \end{cases}$$

$$b = \underbrace{tab}_{\in I} + \underbrace{ib}_{\in J} \Rightarrow b \in I$$

contraditório

Logo I é ideal primo

$\mathbb{Z}$ todo ideal primo também é maximal

$$\mathbb{Z}[x] \supseteq (2) = I_1$$
$$\supseteq (x) = I_2$$

I_1, I_2 são ideais primos

Se $f(x) \cdot g(x) \in I_2$ $\quad$ $f(x) \cdot g(x)$ não tem termo independente

$$f(x) = a_n x^n + \dots + a_1 x + a_0$$
$$g(x) = b_m x^m + \dots b_1 x + b_0$$

$\Rightarrow f(x) g(x) = \dots + \underset{0}{\underset{\|}{a_0 b_0}}$

$\Rightarrow a_0 b_0 = 0 \nearrow a_0 = 0 \Rightarrow f(x) \in I_2$
ou
$\searrow b_0 = 0 \Rightarrow g(x) \in I_2$

$\Rightarrow I_2$ é primo (igual com I_1)

I_1 e I_2 não são maximais

$$(2), (x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$$

$(2, x)$ é maximal pois se

$(2, x) \subsetneq J \quad \Rightarrow \exists f(x) \in J \setminus (2, x)$

$\Rightarrow \quad f(x) = a_n x^n + \dots + a_1 x + a_0$ com

a_0 é ímpar

$$\underset{\underset{J}{\cap}}{f(x)} = \underbrace{a_n x^n + \dots + a_1 x + (a_0 - 1)}_{\underset{\underset{J}{\cap}}{(2, x)}} + 1$$

$\Rightarrow 1 \in J \Rightarrow \mathbb{Z}[x] = J \Leftarrow$

- J ideal primo $\Rightarrow \dfrac{A}{J}$ domínio

- I ideal maximal $\Rightarrow \dfrac{A}{I} = \dots$

Teorema: Seja A um anel comutativo com unidade

I é maximal $\Longleftrightarrow \dfrac{A}{I}$ é um corpo

$\boxed{\text{\underline{Def}: } (L, +, \cdot) \text{ domínio é chamado de Corpo se } (L^*, \cdot) \text{ é um grupo}}$

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ corpos

<u>Prova:</u> ($\Rightarrow$) suponhamos I maximal

$\bar{a} \in \left(\frac{A}{I}\right)^*$, isto é, $\underline{a \notin I}$

$\langle a, I \rangle = J \Rightarrow I \subsetneq J = A$

$\Rightarrow \quad 1 \in A = J \quad \Rightarrow$

$1 = ta + i \quad \Rightarrow \quad 1 - ta \in I$

$\Rightarrow \quad 1 \sim ta \quad \Rightarrow \bar{t}\,\bar{a} = \bar{1}$

$\bar{a}$ tem inverso. $\Rightarrow$ $\frac{A}{I}$ é corpo

($\Leftarrow$) $\frac{A}{I}$ é corpo. e suponhamos que I <u>não</u> é maximal $\Rightarrow$ $\exists J$ com $I \subsetneq J \subsetneq A$ $\Rightarrow \begin{cases} 1 \notin J \\ \exists a \in J \setminus I \end{cases}$

$\bar{a} \neq \bar{0} \Rightarrow \exists \bar{b}$ tal $\bar{a}\bar{b} = \bar{1}$

$$\overline{ab} = \overline{1} \Rightarrow \underset{\in J}{ab} - 1 = c \in I$$

$$\Rightarrow$$

$$1 = \underset{\in J}{ab} - \underset{\in I \subset J}{c} \in J \quad \text{contradição}$$

Teorema: Todo anel possui ideais maximais

<u>Prova:</u> $\mathcal{I} = \{ I \subseteq A \mid I \text{ ideal} \}$

$$I \leq J \Leftrightarrow I \subseteq J$$

$(\mathcal{I}, \leq)$ é um conjunto parcialmente ordenado

$$\{I_i\}_{i \in G} \subseteq \mathcal{I} \qquad I_i \leq I_j \quad i<j$$

definimos $J = \bigcup_{i \in G} I_i$ é ideal

Pelo <u>Lema de Zorn</u> $\mathcal{I}$ tem elementos maximais.