Sia

$$\mathcal{A} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \; a, b \in \mathbb{R}, \; (a,b) \neq (0,0) \right\}$$

con l'operazione di moltiplicazione

$\Downarrow$

$(\mathcal{A}, \cdot)$ struttura algebrica

Ma ... di che tipo?

$\Rightarrow$

1) é associativa?

Dati $A, B, C \in \mathcal{A} \Rightarrow \underbrace{A \cdot (B \cdot C) = (A \cdot B) \cdot C}_{\text{Vale } \forall \text{ matrice}}$

Ora dimostriamo che "$\cdot$" é interna ad $\mathcal{A}$

$\Downarrow$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd \; (1) & ad + bc \; (2) \\ -bc - ad \; (3) & -bd + ac \; (4) \end{pmatrix}$$

$$\left. \begin{array}{l} (1) = (4) \\ (2) = -(3) \end{array} \right\} \text{OK!}$$

$$((1), (2)) \neq (0,0)$$

$\Rightarrow$ "$\cdot$" é interna

2) $\exists$ elemento neutro ?

(Riprendo la moltiplicazione precedente)

$\Downarrow$

$$\begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & ac-bd \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

$$\Rightarrow \begin{cases} ac-bd=a \\ ad+bc=b \\ \text{Le altre due sono superflue} \end{cases} \quad \begin{cases} c = 1 + \dfrac{bd}{a} \\ ad \cancel{+b} + \dfrac{b^2d}{a} = \cancel{b} \end{cases} \quad \begin{cases} \text{---} \\ a^2d + b^2d = 0 \end{cases}$$

$a \neq 0$

$$\begin{cases} \text{---} \\ d(a^2+b^2)=0 \end{cases} \quad \begin{cases} c=1 \\ d=0 \end{cases}$$

Se $a=0$?
$\hookrightarrow$ $c=1$
$d=0$

$$\Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ elemento neutro}$$

3) $\overbrace{\exists}^{\forall A \in \mathcal{Q}}$ $A^{-1} \;/\; A \cdot A^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ e $A^{-1} \cdot A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$?

$$\Rightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{cases} ac-bd=1 \\ ad+bc=0 \end{cases} \quad a \neq 0 \begin{cases} c = \dfrac{1+bd}{a} \\ a^2d + b + b^2d = 0 \end{cases} \quad \begin{cases} c = \dfrac{a}{a^2+b^2} \\ d = \dfrac{-b}{a^2+b^2} \end{cases}$$

$$\Downarrow$$

$$\begin{pmatrix} \frac{a}{a^2+b^2} & -\frac{b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix}$$ é l'opposto di A

$\Downarrow$

a é gruppo!

Abeliano? Si deve vedere se "∘" é commutativo -

Si K un campo e $K[x] = \{$polinomi nella variabile x a coefficienti in K$\}$

(Esponenti $\in \mathbb{N}$)!

(ESEMPIO
In $\mathbb{R}[x]$ ho $3x^4 - \sqrt{2}\,x^3 + 2x - 1$)

In $K[x]$ é data una "somma"

$$(a_n x^n + a_{n-1} x^{n-1} + \dots + a_0) + (b_p x^p + b_{p-1} x^{p-2} + \dots + b_0) =$$

SUPPONENDO $n > p$

$$= a_n x^n + \dots + x^p(a_p + b_p) + \dots + (a_0 + b_0)$$

É data una moltiplicazione in $K[x]$

$\Downarrow$

$$(a_n x^n + \dots + a_0) \circ (b_p x^p + \dots + b_0) =$$

$$= (a_n \circ b_p) x^{n+p} + \dots + (a_n \circ b_0) x^n + (b_p \cdot a_0) x^p + \dots + (a_0 \cdot b_0)$$

Dimostrare che $\underbrace{(K[x], +, \circ)}_{\text{Non é campo}}$ é anello unitario

$\nexists$ reciproco di un polinomio in $K[t]$, a meno che t ~~[illegible]~~ sia di grado zero (allora sarei in K)

DEFINIZIONE

Sia $A \subset G$, G gruppo con operazione "$*$"

se $\forall\, a, b \in A \Rightarrow a * b \in A$ e l'elemento neutro $e \in A \Rightarrow A$ é detto <u>SOTTOGRUPPO</u> di G. Il concetto é estendibile ad anelli e campi:

DEFINIZIONE

Sia $A \subset K$, con $(K, +, \cdot)$ campo, se gli elementi neutri di "+" e "·" stanno in A e A è chiuso rispetto a "+" e "·" $\Rightarrow$ A é <u>SOTTOCAMPO</u> di K.

DEFINIZIONE

Dati due gruppi $(G, \square)$ e $(G', *)$, l'applicazione $f: G \longrightarrow G'$ é detta <u>MORFISMO di gruppi</u> o <u>OMOMORFISMO di gruppi</u>, se l'immagine $f(g_1 \square g_2) = f(g_1) * f(g_2)$ $\forall g_1, g_2 \in G$

DEFINIZIONE

Se considero due anelli $(A, +, \cdot)$ e $(B, \hat{+}, \hat{\cdot})$

$\Downarrow$

$f: A \longrightarrow B$ é <u>MORFISMO di anelli</u>

$$\left.\begin{array}{l} \text{Se } f(a_1 + a_2) = f(a_1) \hat{+} f(a_2) \\ \text{Se } f(a_1 \cdot a_2) = f(a_1) \hat{\cdot} f(a_2) \end{array}\right] \forall a_1, a_2 \in A$$

Sia $(\mathbb{Q}, +, \cdot)$ campo dei razionali,

e $(\mathbb{Z}, +, \cdot)$ anello dei relativi.

La somma su $\mathbb{Q}$ é $\neq$ da quella su $\mathbb{Z}$ (come pure il prodotto).

Diamo $f: \mathbb{Z} \longrightarrow \mathbb{Q}$

$m \longmapsto \frac{m}{1}$

è morfismo di anelli

$\Downarrow$

Lo dimostro

$$+ \begin{cases} f(m_1 + m_2) = \dfrac{m_1 + m_2}{1} \\ \qquad\qquad \| \\ f(m_1) + f(m_2) = \dfrac{m_1}{1} + \dfrac{m_2}{1} = \dfrac{m_1 + m_2}{1} \end{cases}$$

$\forall\ m_1, m_2 \in \mathbb{Z}$

$$\cdot \begin{cases} f(m_1 \cdot m_2) = \dfrac{m_1 \cdot m_2}{1} \\ \qquad\qquad \| \\ f(m_1) \cdot f(m_2) = \dfrac{m_1}{1} \cdot \dfrac{m_2}{1} = \dfrac{m_1 \cdot m_2}{1} \end{cases}$$

$\Downarrow$

f é morfismo d'anelli

Ma ...

f é iniettiva? Sí.

$f(m_1) = f(m_2) \longrightarrow \underbrace{\frac{m_1}{1} = \frac{m_2}{1}}$

Vera quando
$m_1 = m_2$

Se considero $f': \mathbb{Z} \longrightarrow \mathrm{Im} f = f(\mathbb{Z})$

$f' \equiv f$

$\Downarrow$

f' é BIETTIVA (poiché é anche SURIETTIVA)

f' é EPIMORFISMO

$\underbrace{f' \text{ é ISOMORFISMO}}$

Si puó lavorare in entrambe le strutture algebriche

(a livello di struttura algebrica ho $\mathbb{Z} = \mathrm{Im}\,\mathbb{Z}$)

$\Downarrow$

Considero $\underbrace{\mathrm{Im}\,\mathbb{Z}}$ $\subset \mathbb{Q}$

Noi lo identifichiamo con $\mathbb{Z}$ grazie all'ISOMORFISMO

QUINDI $\mathbb{Z} \simeq \left\{ \frac{m}{1} \in \mathbb{Q} \mid m \in \mathbb{Z} \right\}$

ISOMORFO