Def: M insieme $f: \underbrace{M \times M}_{M^2} \longrightarrow M$ operazione binaria

1. M SEMIGRUPPO se f è ASSOCIATIVA

$\forall a,b,c \in M$ $\quad f((a,b)) =: a*b,\ ab$

per ogni $\quad (a*b)*c = a*(b*c)$

2. M MONOIDE se $\exists\, 1_M : \forall a \in M \quad 1_M * a = a * 1_M = a$

UNITÀ ELEMENTO NEUTRO

3. M GRUPPO 1.+2. e $\forall a \in M \ \exists b \in M \quad a*b = b*a = 1_M$

FATTO: Se esiste b è unico viene detto l'INVERSO di a

$b = a^{-1}$ $\left(\frac{1}{a} \right.$ $\quad A$ matrice $\exists A^{-1}$ se $\det A \neq 0$

$A^{-1} \quad A\underline{x} = \underline{b} \quad \underline{x} = A^{-1}\underline{b}$

$\cancel{\underline{x} = \underline{b}A^{-1}}$ $\quad \cancel{x = \frac{b}{A}}$

$(n \times 1)(n \times n)$ $\qquad$ Ricorsiva

4. Potenza $a \in M$ monoide $\quad a^1 := a \quad a^{k+1} := a^k * a$

$k \in \mathbb{N}_{>0} \quad a^{k+1} := a * a^k$

$a^0 := 1_M \quad a^n a^m = a^{n+m}$

M gruppo $\quad a^{-1} \quad a^k = \begin{cases} a^k & k > 0 \\ 1_M & k = 0 \\ (a^{-1})^{-k} & k < 0 \end{cases}$ $\qquad$ Exercise $\quad (a^{-k})^{-1} = a^k$

M gruppo CICLICO se $\exists a \in M$

$k > 0 \quad \{ \cancel{\ }, a, \underbrace{a^2}_{a*a}, a^3, \ldots, a^k \ldots \}$ SEMIGRUPPO

$k > 0 \quad \{ 1_M, a, \quad a^k \}$ MONOIDE

$\{ \ldots a^{-2}, a^{-1}, 1_M a, \ldots \}$ GRUPPO

=.... generato da a $\langle a \rangle$

M gruppo si dice CICLICO se $\exists a \in M$

$$M = \langle a \rangle = \{ a^k : k \in \mathbb{Z} \}$$

Notate che $1_M = a^0 \in \langle a \rangle$ $a^k * a^l = a^{k+l} \in \langle a \rangle$

<u>Chiusura</u> di $\langle a \rangle$ rispetto a $*$

$(a^k)^{-1} = (a^{-1})^k =: a^{-k}$

5. Si dice che M è ABELIANO se $*$ è COMMUTATIVA

$\forall a, b \in M$ $a * b = b * a$

NOTAZIONE: $M = Mat_n(\mathbb{R})$ anello $+ : M \times M \to M$

$* : M \times M \to M$

$+$ 0_M $0_M + a = a + 0_M = a$

POTENZE "a^k" MULTIPLI ka OPPOSTO "a^{-1}" $-a$

Osservazione: Se $G = \langle a \rangle$ è CICLICO allora è abeliano $a^k * a^l = a^{k+l} = a^{l+k} = a^l * a^k$

$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ $f : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$ $+$ somma vettori

$(\mathbb{R}^2, f)$ è gruppo $v + w = w + v$ $\forall v, w \in \mathbb{R}^2$

è CICLIC

Def A gruppo abeliano rispetto a $+$ si dice ANELLO

1. A è MONOIDE rispetto a $*$ prodotto

2. Valgono LEGGI DISTRIBUTIVE

$$(a+b)*c = a*c + b*c$$

$$c*(a+b) = c*a + c*b$$

3. Se A è un anello (ossia valgono 1. e 2.)
si dice A è COMMUTATIVO se $*$
è " A

4. Se inoltre 1. + 2. + 3. $\forall\, 0_M \neq a \in A\ \exists\, a^{-1}$
A viene detto un CAMPO

Esempi 1. $(\mathbb{N}, +, 0_{\mathbb{N}})$ monoide $a+b \in \mathbb{N}\ \forall a,b \in \mathbb{N}$
$\exists\, 0_{\mathbb{N}}$ + ass. comm abeliano

2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ gruppi abeliani rispetto a $+$ 0

3. $(\mathbb{Z}, +, 0)$ gruppo abeliano $\exists\, a \in \mathbb{Z}$:

$$\mathbb{Z} = \langle a \rangle = \{ka : k \in \mathbb{Z}\}$$

$\langle 2 \rangle = 2\mathbb{Z} \subsetneq \mathbb{Z}$ $\qquad \langle 1 \rangle = \mathbb{Z} = \langle -1 \rangle$

$1 \in \mathbb{Z} = \langle a \rangle$ $\exists\, k \in \mathbb{Z}$ $1 = ka$ $a = \pm 1$ generatori

4. $(\mathbb{R}^n, +, \underline{0})$ gruppo abeliano
vettore nullo
$v = (a_1 \ldots a_n)$ $w = (b_1 \ldots b_n)$
$$v + w = (\ldots, a_i + b_i, \ldots)$$

5. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ campi $(\mathbb{Q}, +, 0)$ gruppo abeliano
$\downarrow$ campo $\qquad (\mathbb{Q}, *, 1)$ monoide commutativo

$$0 \neq q = \frac{a}{b} \quad q^{-1} = \frac{b}{a}$$

distributive

Paradossi: Brouwer

6. $Mat_n(\mathbb{R})$ $+, *$ anello non commutativo $n>1$

7. B_n booleano anello commutativo

8. $\mu_n = \{ \exp\left(\frac{2\pi i k}{n}\right) ; k \in \mathbb{Z} \}$ gruppo ciclico

$e^{\frac{2\pi i k}{n}}$

9. $\mathbb{R}[x]$ polinomi in x su $\mathbb{R}$ anello commutativo

$$\sum_i a_i x^i + \sum_j b_j x^j = \sum_k{}' (a_k + b_k) x^k$$

$$(2 + x + 3x^3) + (1 - x + 7x^4) = 3 + 0 \cdot x + 3x^3 + 7x^4$$

$$\left(\sum_i a_i x^i\right) * \left(\sum_j b_j x^j\right) = \sum c_k x^k$$

$$c_k = \cancel{\left(\sum_i a_i\right)\left(\sum_j b_j\right)}$$

$$c_k = \sum_{i+j=k}{}' a_i b_j \qquad x^i x^j = x^{i+j}$$

10. $\mathbb{R}[[x]]$ $\sum_{k=0}^{\infty}{}' a_k x^k$ prodotto di CONVOLUZIONE di CAUCHY

Esercizi Provare che $\neg(p \vee q) = (\neg p) \wedge (\neg q) = \neg p \wedge \neg q$

Provare che però $\neg(p \vee q) \neq \neg p \vee q$

$$1 + x + y + xy \overset{?}{=} (1+x) + y + (1+x)y = 1 + x + \cancel{y} + \cancel{y} + xy$$

Notate che $\forall b \in B_2$ $2b = 0_{B_2}$ $b + b = 0_{B_2}$ $b = -b$

$$1 + x + y + xy \overset{?}{=} 1 + x + xy$$

Sono SINTATTICAMENTE DIVERSE

Sommo opposto di $(1+x+xy)$ a entrambi i termini

$-(1+x+xy) = 1+x+xy$

$$1+x+y+xy-(1+x+xy) = (1+x+xy)-(1+x+xy)$$

$$0$$

$$\cancel{1}-\cancel{1}+\cancel{x}-\cancel{x}+y+\cancel{xy}-\cancel{xy} = 0$$

Semantica $y=1$ rende diverse le due formule

$$1+x+1+x \neq 1+x+x$$

$$0=1 \quad \text{Assurdo}$$

Ex 2. Mostrare che $\forall\, b \in B_n \quad b^2=b$

$$B_n = \mathbb{F}_2[x_1 \;\; x_n] \big/ \langle x_1^2-x_1, \dots, x_n^2-x_n \rangle \qquad \mathbb{F}_2 = B_0 = \{0,1\}$$

$\quad$ $\shortparallel$ GF(2) campo

$(\mathbb{F}_2, +, 0)$ gruppo abeliano

$(\mathbb{F}_2, *, 1)$ monoide $\qquad a \neq 0 \quad \exists\, a^{-1}=a \quad a=1=1^{-1}$

$\mathbb{F}_2$ campo

$R[x] \quad R[x,y] \quad R[x_1 \;\; x_n] \quad \mathbb{F}_2[x_1 \;\; x_n]$

$n=0 \quad b \in B_0 \quad b^2=b$ banale $\quad B_0 = \mathbb{F}_2 = \{0,1\}$

$n=1 \quad b \in B_1 \quad \{0,1,x,x+1\} \quad b$

$\qquad 0, 1, x, \qquad b^2$

$b=(1+x) \quad b^2=(1+x)^2 = \underset{R_1}{1} + \underset{\shortparallel}{2x} + x^2 \qquad (a+b)^n = \sum \binom{n}{k} a^k b^{n-k}$

Pascal triangolo $\qquad 1+x^2 \underset{R_2}{=} 1+x$

$n=2 \qquad (a+bx+cy+dxy)^2 = \,?$

$$\left(\sum_i t_i\right)^2 = \left(\sum_i t_i\right)\left(\sum_j t_j\right) =$$

$$\cancel{\left(\sum_i t_i\right)\left(\sum_i t_i\right)} = \sum_i t_i^2$$

$$= \sum_{i,j=1}^{n} t_i t_j = \sum_{i=j} t_i^2 + \sum_{i\neq j} t_i t_j$$

$$= \sum_i t_i^2 + 2\sum_{1\le i<j\le n} t_i t_j$$

$$(a+b)^2 = (a+b)(a+b) = a(a+b)+b(a+b) =$$

$$= a^2 + ab + \underset{\overset{\shortparallel}{ab}}{ba} + b^2 = a^2+2ab+b^2$$

Ex: $(a+b+c)^2$

$$\left(\sum_{i=1}^{n} t_i\right)^2 = \sum_{i=1}^{n} t_i^2 + 2\sum_{1\le i<j\le n} t_i t_j$$

In $B_m \ni t_i \qquad \left(\sum_{i=1}^{n} t_i\right)^2 \underset{R_1}{\equiv} \sum_{i=1}^{m} t_i^2$

(Student's dream $\quad (a+b)^2 = a^2+b^2$

$\sqrt{a^2+b^2} = a+b$)

$t_i = axy \qquad t_i^2 = a^2x^2y^2 \underset{R_{1,2}}{\equiv} axy = t_i$

$\forall t_i$ monomio vale $\quad t_i^2 \equiv t_i$

$b = \sum_i t_i \qquad b^2 = \left(\sum t_i\right)^2 \equiv \sum t_i^2 \equiv \sum t_i = b$

Ex: Trasformare in termini algebrici la seguente fm.. la luglio 2023

$$\overbrace{(\underbrace{y \vee \neg x}_{b_1}) \wedge x}^{b_2} \longrightarrow (y \vee \neg w)$$

$$b_1 = \cancel{y} + (1+x) + y(\cancel{1}+x) = 1 + x + xy$$

$$b_2 = (1+x+xy)x = x + x^2 + x^2 y = \cancel{x} + \cancel{x} + xy$$

$$b_3 = 1 + w + wy$$

$$b_4 = b_2 \to b_3 = 1 + b_2 + b_2 b_3 = 1 + xy + xy(1+w+wy)$$

$$= 1 + \cancel{xy} + \cancel{xy} + \cancel{xyw} + \cancel{x\underset{\overset{\|}{y}}{y^2}w} = 1$$

tautologia