Sessione II.

DEFINIZIONI

Def: $(S, \star)$ è un MAGMA se l'insieme S è chiuso rispetto all'operazione $\star$.

Def: un magma $(S, \star)$ è un SEMIGRUPPO se $\star$ è ASSOCIATIVA

Def: un semigruppo $(S, \star)$ è un MONOIDE se S contiene un ELEMENTO NEUTRO per $\star$ [l'elemento neutro, se esiste, è unico]

Def: un monoide $(S, \star)$ è un GRUPPO se S contiene l'elemento INVERSO di ogni elemento di S

Def: una struttura algebrica [magma, semigruppo, monoide, gruppo, ...] si dice ABELIANO, o COMMUTATIVO, se $\star$ soddisfa la proprietà commutativa.

Def: $(S, \star, \heartsuit)$ è un ANELLO se $(S, \star)$ è un GRUPPO ABELIANO, $(S \setminus \{\blacksquare\}, \heartsuit)$ è un MONOIDE, e vale la proprietà

TOLTO IL NEUTRO DI $\star$

DISTRIBUTIVA del ♥ rispetto alla ⋆ [sia a dx che a sx].

Esempi: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ sono ANELLI.

D: $(\mathbb{N}, +, \cdot)$ è un ANELLO? [Per esercizio]

Def: Un anello $(S, \star, \heartsuit)$ è un CAMPO se il monoide $(S \setminus \{\blacksquare\}, \heartsuit)$ è un gruppo abeliano.

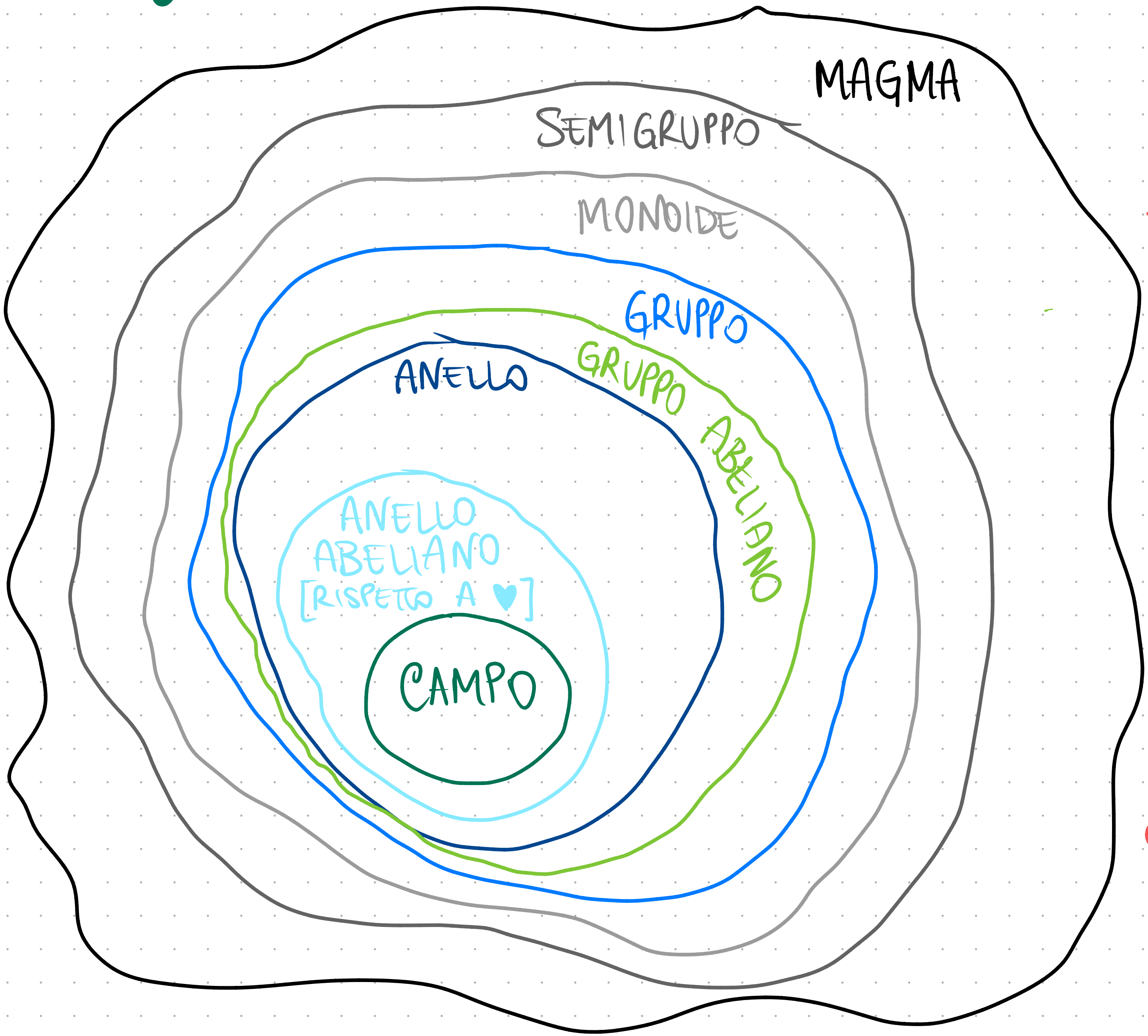
vuol dire che in aggiunta allo anello, "l'insieme con la moltiplic." è anche commutativo e ogni elemento ammette un inverso.

Esempi: $(\mathbb{Q}, +, \cdot)$ OLTRE CHE UN ANELLO è anche un CAMPO.

$(\mathbb{Z}, +, \cdot)$ È SOLTANTO UN ANELLO ma non è UN CAMPO.

$(\mathbb{N}, +, \cdot)$ NON È NEMMENO UN ANELLO, figuriamoci UN CAMPO

Diagramma di Venn delle strutture algebriche [che abbiamo visto...]



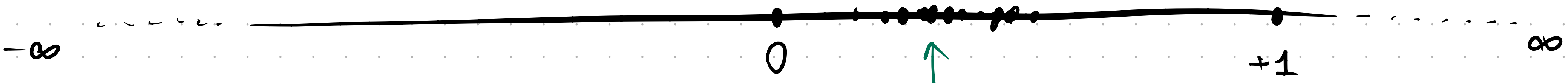
LOGICA:
I CAMPI sono POCHISSIMI, è molto RESTRITTIVO ESSERE UN CAMPO, è molto speciale, è poco GENERALE.

VICEVERSA

CI SONO MOLTE PIÙ STRUTTURE ALGEBRICHE con meno proprietà.

Q. Sembra che $(\mathbb{Q},+,\cdot)$, essendo un CAMPO, abbia già tutte le proprietà che si possano desiderare. Ma è davvero così?

A: Rappresentiamo $\mathbb{Q}$ geometricamente:



I PUNTI DI $\mathbb{Q}$ SONO "INFINITAMENTE FITTI" NEL SENSO CHE TRA DUE NUMERI RAZIONALI C'È SEMPRE UNO (INFINITI) NUMERO RAZIONALE E SONO ARBITRARIAMENTE VICINI

[SI DICE CHE $\mathbb{Q}$ È DENSO IN $\mathbb{R}$]

EPPURE CI SONO DEI "BUCHI"! PER ESEMPIO $\sqrt{2}$ E π <u>NON SONO RAZIONALI</u>.

MA SI POSSONO APPROSSIMARE CON PRECISIONE ARBITRARIA TRAMITE NUMERI RAZIONALI

Esempio:

$\pi = 3,1415926535\ 897932\ldots$ [Non periodico]

$3 = 3$ [Esatto FINO A ZERO CIFRE DECIMALI]

$\frac{22}{7} = 3,14\,2857142857$ [Esatto " " 2 " "]

$\frac{333}{106} = 3,1415\,0943396226$ [Esatto " " 4 " "]

$\frac{355}{113} = 3,141592\,920354\ldots$ [Esatto " " 6 " "]

$\frac{103993}{33102} = 3,141592653\,0119025$ [Esatto " " 9 " "]

$\vdots$

CI SI PUÒ AVVICINARE FINCHÉ SI VUOLE A π USANDO NUMERI RAZIONALI [E NON RAGGIUNGERLO MAI]

Allora estendiamo ancora il nostro insieme, per riempire questi "buchi": $\rightsquigarrow (\mathbb{R}, +, \cdot)$. Buona notizia: è ANCORA UN CAMPO!

D: Quindi con $(\mathbb{R}, +, \cdot)$ possiamo fare TUTTO ?!

A: Possiamo fare molto.

Per esempio c'è la necessità di risolvere EQUAZIONI POLINOMIALI:

Esempi:

$5x + 3 = 0$ ⟶ la soluzione $x \in \mathbb{R}$ ok

$\pi \cdot x + \frac{\sqrt{2}}{17} = 0$ ⟶ la soluzione $x \in \mathbb{R}$ ok

$1 \cdot x^2 - 1 = 0$ ⟶ le soluzioni $x = \pm 1 \in \mathbb{R}$ ok

$1 \cdot x^2 + 1 = 0$ ⟶ NON CI SONO SOLUZIONI in $\mathbb{R}$!

D: E allora cosa possiamo fare? R: Aggiungiamo altri numeri!

$\mathbb{C} := \{ a + i \cdot b \mid a, b \in \mathbb{R} \}$ e $i^2 = -1$ UNITÀ IMMAGINARIA.

OTTENIAMO I NUMERI COMPLESSI. Due ottime notizie:

1. $(\mathbb{C}, +, \cdot)$ È UN CAMPO
2. [TEOREMA FONDAMENTALE dell'ALGEBRA] In $\mathbb{C}$ TUTTI I POLINOMI HANNO SOLUZIONI!

Sessione III

D: Quindi tutte le strutture dell'algebra sono abeliane (i.e. commut.) anche sulla seconda operazione ♥ ?

R: No → ESEMPIO CHIAVE DI TUTTA L'ALGEBRA LINEARE

$$M_{2\times 2}(\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{R} \right\}$$

STA PER "MATRICI", CIOÈ "TABELLE DI NUMERI"

LARGHEZZA DELLA MATRICE E ALTEZZA

CI SERVE UN CAMPO PER I NUMERI DELLA MATRICE

Es: $M_2(\mathbb{Q})$, $M_2(\mathbb{C})$, ...

DEFINIAMO DUE OPERAZIONI:

$\boxed{\star = + \text{ DELLE MATRICI}}$

lo chiamiamo comunque +, ma è una nuova operazione

$$\begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 5 \\ 0 & 7 \end{pmatrix} = \begin{pmatrix} 3+1 & 1+5 \\ 0+0 & 1+7 \end{pmatrix} = \begin{pmatrix} 4 & 6 \\ 0 & 8 \end{pmatrix}$$

Ha l'elemento neutro $\blacksquare := \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ per $\star = +$

$(M_{2\times 2}(\mathbb{R}), +)$ ha l'associatività e l'opposto, commut.

$\Rightarrow (M_{2\times 2}(\mathbb{R}), +)$ È UN GRUPPO ABELIANO

$\boxed{\heartsuit = \cdot \text{ DELLE MATRICI}}$

NUOVO PRODOTTO

USUALE PRODOTTO IN $\mathbb{R}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} := \begin{pmatrix} a\cdot e + b\cdot g & a\cdot f + b\cdot h \\ c\cdot e + d\cdot g & c\cdot f + d\cdot h \end{pmatrix}$$

SI CHIAMA PRODOTTO RIGA per COLONNA e l'INTERO CORSO SI APPOGGIA SU QUESTA DEFINIZIONE.

Ha l'elemento neutro $\odot := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ per $\heartsuit = \cdot$

$(M_{2\times 2}(\mathbb{R})^{\times}, \cdot)$ ha l'associatività.

D: Ma Commuta ? R: Proviamo con $A := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ e $B := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$

LA MATRICE NULLA

$$A \cdot B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \mathbf{0} \Rightarrow \underset{\neq 0}{A} \cdot \underset{\neq 0}{B} = 0$$

MOLTO STRANO!

$$B \cdot A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = B \Rightarrow B \cdot A = B$$

MA A NON È L'IDENTITÀ

ALTRETTANTO BIZZARRO!

NON POSSO SEMPLIFICARE:

[i.e. $BA = B \not\Rightarrow A = 1$

neutro per il prodotto]

D: E l'inverso? Possiamo invertire una matrice 2×2 rispetto al prodotto riga per colonna tra matrici?

R: Proviamo a mano a vedere come dovrebbe essere

Parto da $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e cerco $A^{-1} = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ tale che

tale che $A \cdot A^{-1} = \mathbb{1}$ ma anche $A^{-1}A = \mathbb{1}$

Quindi dobbiamo imporre che:

ENTRAMBI DEVONO ESSERE VERI!

$$\underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}}_{\substack{\| \\ \text{PRODOTTO RIGA PER COLONNA}}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \& \quad \underbrace{\begin{pmatrix} e & f \\ g & h \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{\substack{\| \\ \text{PRODOTTO RIGA PER COLONNA}}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

deve essere $= 0$

$$\begin{pmatrix} \underbrace{ae + bg}_{1=} & \underbrace{af + bh}_{=0} \\ \underbrace{ce + dg}_{0=} & \underbrace{cf + dh}_{=1} \end{pmatrix} \qquad \begin{pmatrix} \underbrace{ea + fc}_{1=} & \underbrace{eb + fd}_{=0} \\ \underbrace{ga + hc}_{=0} & \underbrace{gb + hd}_{=1} \end{pmatrix}$$

deve essere $= 1$

Quindi abbiamo le equazioni:

$$ae + bg = 1 \Rightarrow ae = 1 - bg \Rightarrow a = \frac{1-bg}{e}$$ [assumendo $e \neq 0$]

$$af + bh = 0$$

$$ce + dg = 0$$

$$cf + dh = 1$$

$$ea + fc = 1 \Rightarrow ae = 1 - fc \Rightarrow a = \frac{1-fc}{e}$$

$$eb + fd = 0$$

$$ga + hc = 0$$

$$gb + hd = 1$$

MA QUESTO PRODOTTO È IL PRODOTTO IN $\mathbb{R}$! QUINDI È COMMUTATIVO, QUINDI $ea = ae$!

$$bg = fc \Rightarrow g = f \cdot \underbrace{\left(\frac{c}{b}\right)}_{\text{NOTI}}$$

ABBIAMO TROVATO UNA RELAZIONE TRA g ed f!

Continuando si trova la formula: [PER ESERCIZIO]

$$\boxed{A^{-1} = \frac{1}{\underbrace{ad-bc}_{\det(A)}} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}}$$

[stiamo usando che $5 \cdot \begin{pmatrix} 1 & 0 \\ 2 & -3 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 10 & -15 \end{pmatrix}$]

ASSUMENDO CHE $\underbrace{ad - bc}$ $\neq 0$!

QUESTO SI CHIAMA IL DETERMINANTE DI $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

ED È DEFINITO SOLO PER LE MATRICI QUADRATE.

Quindi solo alcune matrici 2x2 sono invertibili! E sono proprio quelle che hanno DETERMINANTE DIVERSO DA ZERO.

$$GL_2(\mathbb{R}) := \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; ad - bc \neq 0 \right\}$$

$$= \left\{ A \in M_{2\times 2}(\mathbb{R}) \;\middle|\; \det(A) \neq 0 \right\} \subset M_{2\times 2}(\mathbb{R})$$

E si ha che $(GL_2(\mathbb{R}), \cdot)$ è un GRUPPO NON COMMUTATIVO.

D: Funziona tutto anche con $\mathbb{Q}$ e $\mathbb{C}$ al posto di $\mathbb{R}$?

R: Sì, funziona almeno con tutti i campi, anche se con alcuni campi bisogna stare attenti

somma e prodotto tra matrici

D: Quindi $(GL_2(\mathbb{R}), +, \cdot)$ è UN ANELLO?

R: No, $GL_2(\mathbb{R})$ non è nemmeno un MAGMA per $+$!

E per esempio $\mathbb{O} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ ha $\det(\mathbb{O}) = 0$ quindi non appartiene a $GL_2(\mathbb{R})$

D: Quindi $(M_{2\times 2}(\mathbb{R}), +, \cdot)$ è UN ANELLO? R: Sì, ma non commutativo