PRELIMINARI DI ALGEBRA

GRUPPI

Def Dati due insiemi A, B si indica con $A \times B$ l'insieme delle <u>coppie ordinate</u> (a,b) con $a \in A$ e $b \in B$

cioè $$A \times B = \{(a,b) \mid a \in A, b \in B\}$$

$A \times B$ si chiama <u>prodotto cartesiano</u> di A e B

Esempio: . $A = \{1,2,3\}$ $B = \{a,b\}$

$$A \times B = \{(1,a), (1,b), (2,a), (2,b), (3,a), (3,b)\}$$

. $\mathbb{R}$ insieme dei numeri reali

$$\mathbb{R} \times \mathbb{R} = \{(x,y) \mid x \in \mathbb{R}, y \in \mathbb{R}\} = \mathbb{R}^2$$

notiamo che: $(1,2) \neq (2,1)$

Def Sia S insieme non vuoto. Una operazione su S (o legge di composizione interna ad S) è una funzione

$$* : S \times S \longrightarrow S$$

che associa ad (a,b) un elemento $c \in S$ indicato con $a * b$

Esempi:

i) $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ somma è un'operazione in $\mathbb{Z}$

$(a,b) \to a+b$

$(1,2) \to 3$

ii) $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ prodotto è un'operazione in $\mathbb{Q}$

$(x,y) \to x \cdot y$

$(1,2) \to 2$

[operazioni "numeriche"]

iii) X insieme, $F = \{f : X \to X\}$ insieme delle applicazioni da X in X

$\circ : F \times F \to F$ la composizione di funzioni è un'operazione in F

$(f,g) \to f \circ g$

Def Sia G un insieme e $*$ un'operazione in G. La coppia $(G,*)$ si dice un gruppo se valgono le seguenti proprietà:

i) per ogni $a,b,c \in G$ $(a*b)*c = a*(b*c)$ [PROPRIETÀ ASSOCIATIVA]

ii) esiste $e \in G$ tale che per ogni $a \in G$ $a*e = e*a = a$; e viene detto elemento neutro di G [ESISTENZA ELEMENTO NEUTRO]

4) per ogni $a \in G$ esiste $b \in G$

tale che $a * b = b * a = e$

b viene detto elemento inverso di G

e viene indicato con a^{-1}

[ESISTENZA ELEMENTI INVERSI]

Il gruppo $(G, *)$ viene detto abeliano

se per ogni $a, b \in G$ $\quad a * b = b * a$

[PROPRIETÀ COMMUTATIVA]

Esempi 1) $(\mathbb{Z}, +)$ è un gruppo commutativo

($\mathbb{Z}$: numeri interi)

oss. $(a+b)+c = a+(b+c)$ $\forall a, b, c$

el. neutro $(0+a) = (a+0) = a$ $\forall a \in \mathbb{Z}$

esistenza inverso $\forall a \in \mathbb{Z}$ $\exists -a \in \mathbb{Z}$ tale che $a+(-a) = (-a)+a = 0$

Commut. $a+b = b+a$ $\forall a, b \in \mathbb{Z}$

2) $(\mathbb{Z}, \cdot)$ non è un gruppo commutativo

- associatività è verificata
- elemento neutro esiste ($è 1 \cdot a$)
- alcuni elementi non hanno l'inverso

$2 \cdot z \neq 1$ per ogni $z \in \mathbb{Z}$

3) $(\mathbb{Q}, +)$ è un gruppo

4) $(\mathbb{Q}\setminus\{0\}, \cdot)$ è un gruppo

oss preliminare se $q, q' \in \mathbb{Q}\setminus\{0\}$

allora $q \cdot q' \in \mathbb{Q}\setminus\{0\}$

- oss. el. neutro sono verifiche
- $\forall q \in \mathbb{Q}\setminus\{0\} \quad \exists\, q^{-1} = \frac{1}{q}$ tc $q \cdot \frac{1}{q} = \frac{1}{q} \cdot q = 1$

Tutti i gruppi "numerici" sono abeliani e quelli non abeliani?

5) X insieme $\mathcal{I}(X) = \{f : X \to X \mid f \text{ biettive}\}$

$(\mathcal{I}(X), \circ)$ è un gruppo (composizione di applicazioni)

Ricordo $g : X \to Y$ $f : Y \to Z$

$f \circ g : X \to Z$ $f \circ g(x) = f(g(x))$

oss preliminare f, g biettive $\Rightarrow f \circ g$ biettive

(dim. per esercizio)

associatività la composizione di funzioni è un'operazione associativa

$(f \circ g) \circ h = f \circ (g \circ h)$ (i.e. $(f \circ g) \circ h(x) = f \circ (g \circ h)(x)$ $\forall x \in X$)

esistenza elemento neutro

Id_X è l'identità del gruppo infatti

$$f \circ Id_X = Id_X \circ f$$

esistenza elementi inversi

f biettiva $\iff$ f invertibile

OSS: (da dim.)

Ricordo che per definizione $f: X \to X$ è invertibile se e solo se $\exists f^{-1}: X \to X$ tale che

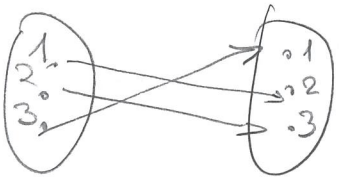
$$f \circ f^{-1} = Id_X \text{ e } f^{-1} \circ f = Id_X$$

CONCLUSIONE: dato $f \in I(X)$ allora f^{-1} è l'inverso di f rispetto all'operazione $\circ$

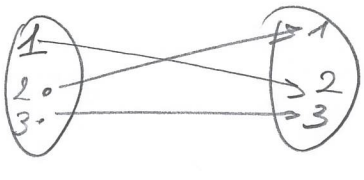
Per la "maggior parte" degli X il gruppo $(I(X), \circ)$ non è abeliano

Esempio $X = \{1,2,3\}$

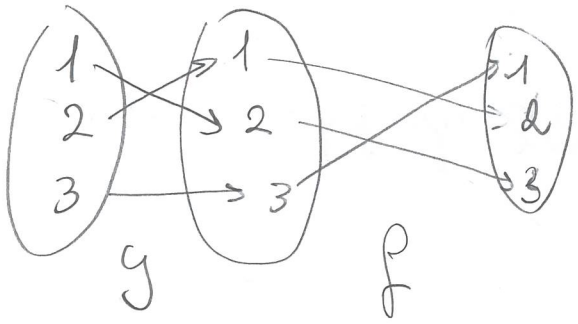
f



g



$f \circ g$

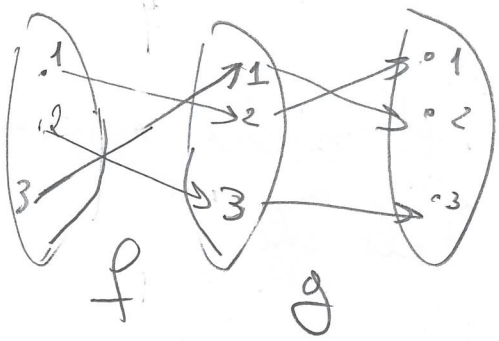


$f \circ g(1) = 3$

$f \circ g(2) = 2$

$f \circ g(3) = 1$

$g \circ f$



$g \circ f(1) = 1$

$g \circ f(2) = 3$

$g \circ f(3) = 2$

<u>Oss</u> se X ha almeno 3 elementi $(I(X), \circ)$ non è abeliano (posso costruire esempio analogo a prima)

<u>Domanda</u>: se X ha n elementi quanti elementi ha $I(X)$?

2 proprietà generali dei gruppi

1) L'elemento neutro in un gruppo è unico

Dim Siano $e, \bar{e}$ due elementi neutri di $(G, \cdot)$

$$e = e \cdot \bar{e} = \bar{e}$$

e è elemento neutro

$\bar{e}$ elemento neutro

□

2) Sia $(G, \cdot)$ un gruppo e $g \in G$
allora esiste un unico inverso di g

Dim $g^{-1}, \bar{g}$ due inversi di g

$$g^{-1} = g^{-1} \cdot e = g^{-1} \cdot (g \cdot \bar{g}) = (g^{-1} \cdot g) \cdot \bar{g} =$$

e el. neutro

$\bar{g}$ inverso di g

oss

$$= e \cdot \bar{g} = \bar{g} \quad \Rightarrow g^{-1} = \bar{g}$$

g^{-1} inverso di g

□

RELAZIONI d'EQUIVALENZA

Prossimo esempio interessante ma ci serve un po di linguaggio che sarà utile anche in altri contesti

Def: Dato X un insieme una relazione su X è un sottoinsieme di $X \times X$

$R \subseteq X \times X$ relazione

Se $(x,y) \in R$ si dice che x è in relazione con y e si scrive xRy (o $x \sim y$ o $x \rho y$)

Se $(x,y) \notin R$ si dice che x non è in relazione con y e si scrive $x \not R y$

Esempio: 1) $X = \{1,2,3\}$

$$R = \{(1,2), (1,3), (3,2), (1,1)\}$$

$1R2$ $1R3$ $3R2$ $1R1$

$2 \not R 1$

di solito ci si dimentica del sottoinsieme e si usa una proprietà per definire la relazione

2) in $\mathbb{Z}$ definisco la seguente relazione

$x \sim y$ (x è in relazione con y) $\Longleftrightarrow$ $x \leq y$

$1 \sim 2$ $\quad 1 \sim 1$ $\quad 2 \not\sim 1$

il corrispettivo sottoinsieme di $\mathbb{Z} \times \mathbb{Z}$ sarebbe $\{(x,y) \mid x \leq y\} = \{(1,1)(1,2)(1,3), \dots\}$

3) in $\mathbb{R}$ definisco la seguente relazione

$x \sim y \Longleftrightarrow$ $x^2 = y$

$1 \sim 1$ $\quad -1 \sim 1$ $\quad 2 \sim 4$ $\quad -2 \sim 4$

$2 \not\sim 1$ ecc...

Anche nella vita comune si costruiscono relazioni (sposato con, più alto, ecc.)

In matematica alcuni tipi di relazioni importanti: funzioni, relazioni di equivalenza e relazioni d'ordine

Noi considereremo le rel. di equivalenza.

Def Sia X un insieme e $\sim$ una relazione su X; diciamo che $\sim$ è una **relazione di equivalenza** se valgono le seguenti

i) per ogni $x \in X$ $\quad x \sim x$ (Proprietà riflessiva)

ii) se $x \sim y$ allora $y \sim x$ (Proprietà simmetrica)

iii) se $x \sim y$ e $y \sim z$ allora $x \sim z$ (proprietà transitiva)

Esempi 0) (esempio "0")

l'uguaglianza è una rel. di eq.

i) $x = x \quad \forall x$

ii) se $x = y$ allora $y = x$

iii) se $x = y$ e $y = z$ allora $x = z$

1) "essere congruenti" è una relazione di equivalenza fra i triangoli nel piano

i) T è congruente con se stesso

ii) se T è congruente con S allora S è congruente con T

iii) se T è congruente con S e S è congruente con U allora T è congruente con U

2) "minore o uguale" $\leq$ non è una relazione di equivalenza in $\mathbb{Z}$ (né in $\mathbb{R}$ ecc.)

Perché:

$1 \leq 2$ ma non è vero che $2 \leq 1$

non vale la proprietà simmetrica

3) [caso che ci interessa ora] Fisso $n \in \mathbb{Z}$

definiamo in $\mathbb{Z}$ la seguente relazione

x è congruo a y modulo n $(x \equiv_n y)$ $\iff$ $\exists\, h \in \mathbb{Z}$ tale che $x - y = hn$

$\iff$ $x - y$ è multiplo di n

Oss

$\equiv_n$ è una relazione di equivalenza

Dim i) $\forall n \in \mathbb{Z}$ $x - x = 0 = 0 \cdot n$ (riflessività)

ii) $x \equiv_n y \Rightarrow \exists\, h \in \mathbb{Z}$ tc $x - y = hn$

$\Rightarrow \exists\, -h \in \mathbb{Z}$ tc $y - x = (-h)n$

$\Rightarrow y \equiv_n x$ (simmetria)

111) $x \equiv_n y$ e $y \equiv_n z \Rightarrow \exists h, k \in \mathbb{Z}$

tale che $x - y = hn$ e $y - z = kn$

$\Rightarrow \exists h, k \in \mathbb{Z}$ t.c. $(x-y)+(y-z) = hn + kn$

$\Rightarrow \exists h, k \in \mathbb{Z} \quad (x-z) = (h+k)n$

$\Rightarrow \exists a \in \mathbb{Z}$ t.c $(x-z) = an$

$\Rightarrow x \equiv_n z$ (transitività)

$x \equiv_n y$ si dice anche che hanno lo stesso classe resto modulo n, perché?

Prop: divido x per n e ottengo r come resto $(0 \leq r < n)$

divido y per n e ottengo r' come resto $(0 \leq r' < n)$

$x \equiv_n y \iff r = r'$

Dim $x = nq + r \qquad y = nq' + r'$

$x - y = (q - q')n + r - r'$

- se $r = r'$ $x - y = (q-q')n + \underbrace{r-r'}_{0}$

$\Rightarrow x \equiv_n y$

- se $x \equiv_n y$ $x = nq + r$ e $x - y = hn$

$\Rightarrow x = nq + r \quad y = x - hn$

$\Rightarrow y = x - hn = nq + r - hn = (q-h)n + r \Rightarrow$ r resto di y diviso per n

□

Oss con questa definizione equivalente
la dim. che la relazione è di equivalenza
è molto più facile

Generalità sulle relazioni di equivalenza

Def $\sim$ relazione di equivalenza su X, $x \in X$
$[x]_\sim = \{y \in X \mid y \sim x\}$ è la classe di equivalenza
di x rispetto alla relazione $\sim$

Esempi: 1) $=$ (uguaglianza) rel. di eq. su X

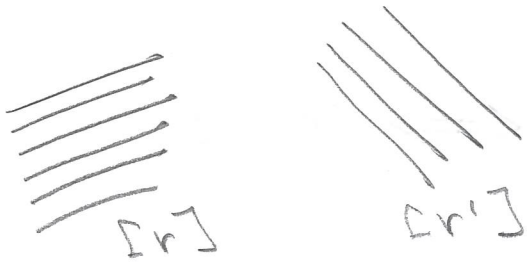
$$[x] = \{x\}$$

2) $\Gamma = \{\text{rette nel piano}\}$

$r \sim r' \iff$ r è parallela a r'
(se $r = r'$ & conv. diciamo parallele)

$\sim$ è una relazione di equivalenza su Γ
(si verificano le tre proprietà)

$$[r] = \{\text{tutte le rette parallele a } r\}$$



Interpretazioni

$$\{[r] \mid r \in \Gamma\} = \{\text{direzioni delle rette nel piano}\}$$

111) $\equiv_4$

$[0] = \{z \in \mathbb{Z} \mid z-0 \text{ multiplo di } 4\} = \{\dots,-8,-4,0,4,8,\dots\}$

$[1] = \{z \in \mathbb{Z} \mid z-1 \text{ multiplo di } 4\}$

$= \{z \in \mathbb{Z} \mid z = 1+4h \text{ con } h \in \mathbb{Z}\}$

$= \{\dots,-7,-3,1,5,9,13,\dots\}$

$[2] = \{z \in \mathbb{Z} \mid z = 2+4h\}$

$= \{\dots,-6,-2,2,6,10,\dots\}$

$[3] = \{z \in \mathbb{Z} \mid z = 3+4h\}$

$= \{\dots,-5,-1,3,7,11,\dots\}$

$[4] = [0]$

$[5] = [1]$ ecc...

<u>Oss</u> $[x]_\sim = [y]_\sim \iff x \sim y$

$\equiv_4$ ha 4 classi di equivalenza
(esattamente i 4 resti possibili quando divido per 4)

in generale $\equiv_n$ ha n classi di equiv

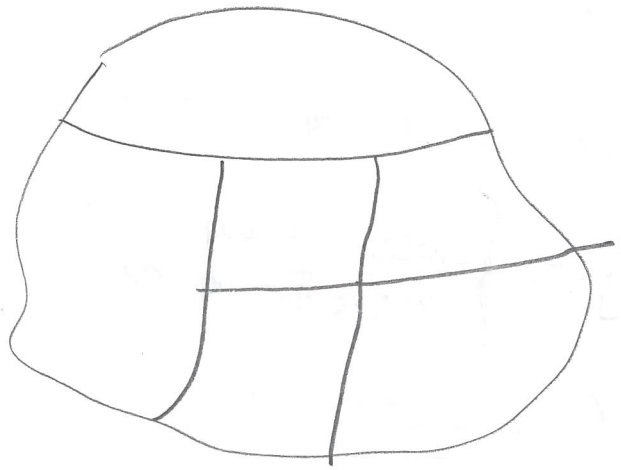
$[0]\ [1] \dots [n-1]$

(esattamente gli n resti possibili nella divisione per n)

- Partizione X insieme $\mathcal{P} \subseteq \mathcal{P}(X)$ (insieme delle parti di X)

$\mathcal{P}$ si dice una partizione di X se

1) $\emptyset \notin \mathcal{P}$
2) $\bigcup_{Y \in \mathcal{P}} Y = X$
3) se $Y_1, Y_2 \in \mathcal{P}$ e $Y_1 \cap Y_2 \neq \emptyset$ allora $Y_1 = Y_2$



Proposizione X insieme, $\sim$ relazione di equivalenza

$\{[x]_\sim\}$ (insieme delle classi di eq è una partizione)

Dim $x \in [x]_\sim \begin{cases} \Rightarrow [x]_\sim \neq \emptyset & \text{i) ok} \\ \Rightarrow \bigcup [x]_\sim = X & \text{ii) ok} \end{cases}$

$[x]_\sim \cap [y]_\sim \neq \emptyset \Rightarrow \exists z$ t.c. $z \sim x$ e $z \sim y$

$w \in [x]_\sim \iff w \sim x \iff w \sim z \iff w \sim y$

$\iff w \in [y]_\sim$

$\Downarrow$

$[x]_\sim = [y]_\sim$ ▨

Def X insieme, $\sim$ relazione di equivalenza

$$X/_\sim = \{[x]_\sim \mid x \in X\} = \left\{\begin{array}{l}\text{classi di equivalenza} \\ \text{rispetto a } \sim\end{array}\right\}$$

è il quoziente di X rispetto a $\sim$

I GRUPPI $\mathbb{Z}_n$

$n \geq 2$

$\mathbb{Z}_n = \{$ classi di equivalenza di $\equiv_n \}$

$= \{ [0], [1], \dots [n-1] \}$ n-elementi

$= \{ \bar{0}, \bar{1}, \dots, \overline{n-1} \}$ (nuova notazione più comoda)

Definiamo in $\mathbb{Z}_n$ $\bar{x} + \bar{y} = \overline{x+y}$

Esempio: in $\mathbb{Z}_4$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}=\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}=\bar{0}$	$\bar{5}=\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{5}=\bar{1}$	$\bar{6}=\bar{2}$

Punto sottile: c'è qualcosa di "delicato" nella definizione, cosè?

diversi numeri possono essere usati per definire la stessa classe di equivalenza può creare problemi? Vediamo

in $\mathbb{Z}_4$ $\bar{0} = \bar{4}$

$\bar{0} + \bar{2} = \overline{0+2} = \bar{2}$ sembra diverso ma $\bar{2} = \bar{6}$

$\bar{4} + \bar{2} = \overline{4+2} = \bar{6}$

in $\mathbb{Z}_7$ $\quad \overline{3} = -\overline{4}$

$\overline{3} + \overline{2} = \overline{5}$ $\qquad$ ma $\quad -\overline{5} = -\overline{2}$

$-\overline{4} + \overline{2} = \overline{-4+2} = -2$

È un caso? NO

Prop in $\mathbb{Z}_n$ se $\overline{x} = \overline{a}$ e $\overline{y} = \overline{b}$

allora $\overline{x+y} = \overline{a+b}$

Dim $\overline{x} = \overline{a} \Rightarrow \exists h \in \mathbb{Z}$ tc $x - a = hn$

$\overline{y} = \overline{b} \Rightarrow \exists k \in \mathbb{Z}$ tc $y - b = kn$ $\Rightarrow$

$\Rightarrow \exists h, k \in \mathbb{Z}$ tc $(x-a) + (y-b) = hn + kn$

$\Rightarrow \exists h, k \in \mathbb{Z}$ tc $(x+y) - (a+b) = (h+k)n$

$\Rightarrow \overline{x+y} = \overline{a+b}$ $\qquad$ ▨

Prop $(\mathbb{Z}_n, +)$ è un gruppo abeliano

Dim (il punto difficile è il precedente le proprietà di gruppo dipendono dalle proprietà in $\mathbb{Z}$)

associatività

$\forall \overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_n \quad (\overline{x} + \overline{y}) + \overline{z} = (\overline{x+y}) + \overline{z} =$

$= \overline{(x+y)+z} = \overline{x+(y+z)} = \overline{x} + \overline{(y+z)}$

$= \overline{x} + (\overline{y} + \overline{z})$

esistenza elemento neutro

$\forall \bar{x} \in \mathbb{Z}_m \quad \bar{0} + \bar{x} = \overline{0+x} = \bar{x}$

$\overline{x+0} = \overline{x+0} = \bar{x}$

esistenza opposto

$\forall \bar{x} \in \mathbb{Z}_n \quad \exists\ \overline{-x} \in \mathbb{Z}_n$ tale che

$$\bar{x} + \overline{(-x)} = \overline{x + (-x)} = \bar{0}$$

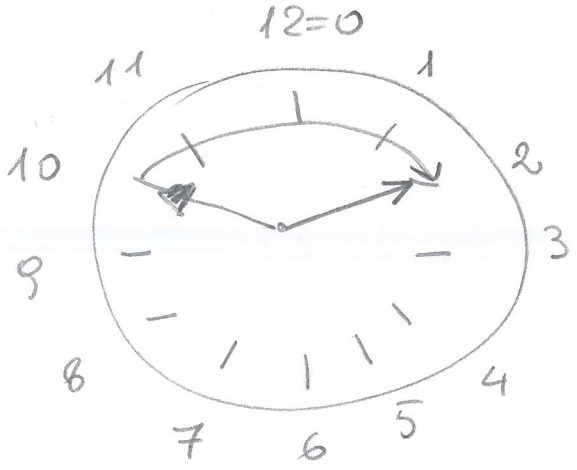
$$\overline{(-x)} + \bar{x} = \overline{(-x)+x} = \bar{0}$$

gruppo abeliano

$\forall \bar{x}, \bar{y} \in \mathbb{Z}_n \quad \bar{x} + \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} + \bar{x}$

Viene chiamata anche aritmetica dell'orologio

Sono le 10, torno fra 4 ore!
Torno alle 2



è come lavorare in $\mathbb{Z}_{12}$!

CAMPI

Def Sia K un insieme con due operazioni $+$ (chiamata somma) e $\cdot$ (chiamata prodotto)

La terna $(K, +, \cdot)$ si dice un <u>campo</u> se valgono le seguenti proprietà

1) $\forall a,b,c \in K \quad (a+b)+c = a+(b+c)$
(PROP. ASS. PER SOMMA)

2) $\exists 0 \in K$ tale che $(a+0)=(0+a)=a$
(ES. EL. NEUTRO PER LA SOMMA detto ZERO)

3) $\forall a \in K \quad \exists -a \in K$ tale che

$$a+(-a)=(-a)+a=0$$

(ES. EL. INVERSI PER LA SOMMA detti OPPOSTI)

---

4) $\forall a,b \in K \quad a+b = b+a$

(PROP. COMMUTATIVA PEL LA SOMMA)

[$1+2+3+4 \Longrightarrow (K,+)$ è un gruppo abeliano]

---

5) $\forall a,b,c \in K \quad (a \cdot b)\cdot c = a\cdot(b\cdot c)$
(PROP. ASS PER IL PRODOTTO)

6) $\exists\, 1 \in K \setminus \{0\}$ tale che $(1 \cdot a) = (a \cdot 1) = a$

(ES. EL. NEUTRO PER IL PRODOTTO detto UNITÀ)

---

attenzione $K \setminus \{0\}$

7) $\forall a \in K \setminus \{0\}\ \exists\, a^{-1} \in K$: tale che

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

(ESISTENTA ELEMENTI INVERSI PER IL PRODOTTO)

---

8) $\forall a, b \in K \quad a \cdot b = b \cdot a$.

(PROP. COMMUTATIVA PER IL PRODOTTO)

---

9) $\forall a, b, c \in K$

$$(a+b) \cdot c = a \cdot c + b \cdot c$$

(PROP. DISTRIBUTIVA DEL PRODOTTO RISPETTO ALLA SOMMA)

Esempi: $(\mathbb{Q}, +, \cdot)$ campo dei numeri razionali.

$(\mathbb{R}, +, \cdot)$ campo dei numeri reali.

$(\mathbb{Z}, +, \cdot)$ non è un campo perché mancano gli inversi rispetto al prodotto

$(\mathbb{C}, +, \cdot)$ campo dei numeri complessi. (per chi non li ha visti vi introdotti in analisi)

CAMPI IMPORTANTI IN QUESTO CORSO

Perchè questa generalità?
80 % delle teorie che svilupperemo vale per un generico campo ($\mathbb{R}$ o $\mathbb{C}$ o ....)

4 proprietà generali dei campi

$(K, +, \cdot)$ campo

1) **per ogni $a \in K$ $\quad 0 \cdot a = 0$**

$$0 \cdot a = (0+0) \cdot a = (0 \cdot a) + (0 \cdot a)$$

↑ 0 el. neutro per +

↑ proprietà distributiva

Chiamo $b = 0 \cdot a$ e ottengo

$$b = b + b$$

$$0 = b + (-b) = (b+b) + (-b) = b + \underbrace{(b + (-b))}_{\text{II} \leftarrow \text{prop opposto}} = b$$

0

↑ prop opposto

↑ oss.

da cui $0 \cdot a = b = 0$

∎

notazioni compatte:

$$a - b = a + (-b)$$
$$ab = a \cdot b$$
$$\frac{a}{b} = a \cdot b^{-1}$$

2) **se $a \cdot b = 0$ allora $a = 0$ oppure $b = 0$**

Dim

Siano $a, b \in K$ tali che $a \cdot b = 0$

Se $a = 0$ la tesi è verificata

Supponiamo $a \neq 0 \Rightarrow$ esiste a^{-1}

$$b = (\underbrace{a^{-1} \cdot a}_{= 1}) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$$

(assoc.; per proprietà precedente)

concludiamo $b = 0$ ▨

Oss: se $a \neq 0$ e $b \neq 0$ allora $a \cdot b \neq 0$

$(K \setminus \{0\}, \cdot)$ è un gruppo abeliano

3) **Sia -1 l'opposto di 1**

$(-1) \cdot a = -a$

Dim

$$(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = \overbrace{(-1 + 1)}^{= 0} \cdot a = 0$$

(prop distr)

Unicità elemento opposto

$(-1)\cdot a = -a$

4) Risoluzioni equazioni:

- siano $a, b \in K$, esiste un unico x tale che $x+a=b$ $(x = b-a)$
- siano $a, b \in K$ $a \neq 0$, esiste un unico x tale che $ax=b$ $(x = ba^{-1} = \frac{b}{a})$

Dim (lascio a voi)

CAMPI FINITI

Ricordo che abbiamo definito $(\mathbb{Z}_n, +)$

Possiamo fare le stessa cosa per il prodotto?

definiamo $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$

l'operazione è ben definita?

Supponiamo $\overline{x} = \overline{x}'$ e $\overline{y} = \overline{y}'$

Esistono h, k tali che

$x - x' = nh \quad x = nh + x'$

$y - y' = nk \quad y = nk + y'$

$$xy = x'y' + nhy' + nkx' + n^2hk$$

$$xy = x'y' + n(hy' + kx' + nhk)$$

$xy - x'y'$ multiplo di n

$$\overline{x \cdot y} = \overline{x' \cdot y'}$$

Conclusione: l'operazione è ben definita

▶ $(\mathbb{Z}_n, +, \cdot)$ è un campo?

- vivono che valgono l'associatività del prodotto e la distributività
- $\overline{1}$ è l'elemento neutro rispetto al prodotto

$$\overline{x} \cdot \overline{1} = \overline{x1} = \overline{x}$$

▶ esistono elementi inversi rispetto al prodotto?

Esempio 1 $(\mathbb{Z}_4, \cdot)$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4} = \overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$(\mathbb{Z}_4, +, \cdot)$ non è un campo

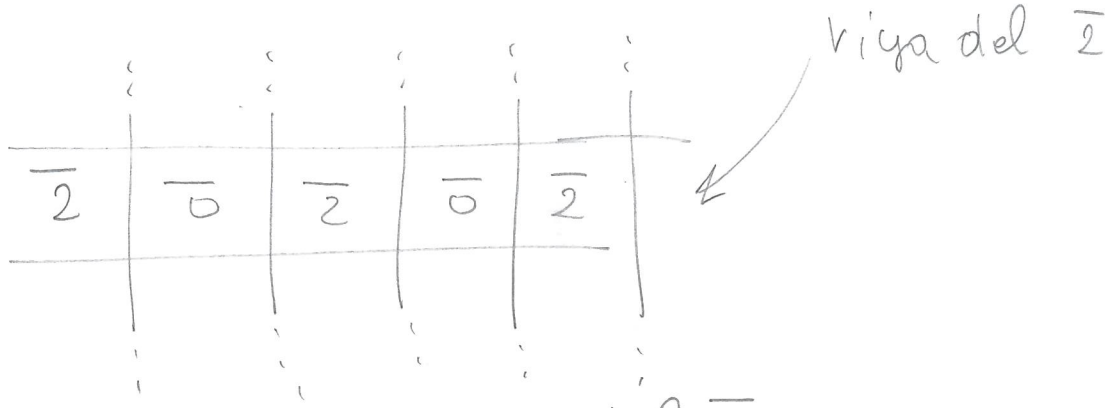
Due modi per vederlo:

1) $\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$

$\neq_0 \quad \neq_0$

Nei campi non può succedere!

2)



non c'è $\bar{1}$ nella riga del $\bar{2}$.

$\bar{2}$ non ha l'inverso!

Esempio 2 $(\mathbb{Z}_5, \cdot)$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}=\bar{1}$	$\bar{8}=\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{9}=\bar{4}$	$\bar{12}=\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Otteniamo

$\bar{1}\cdot\bar{1}=\bar{1}$ $\bar{2}\cdot\bar{3}=\bar{1}$ $\bar{3}\cdot\bar{2}=\bar{1}$ $\bar{4}\cdot\bar{4}=1$

tutti gli elementi tranne lo zero hanno inverso

$(\mathbb{Z}_5, +, \cdot)$ è un campo

CASO GENERALE

Prop $(\mathbb{Z}_n, +, \cdot)$ è un campo se e solo se n è primo

Dim

1° parte $(\mathbb{Z}_n, +, \cdot)$ è un campo $\Rightarrow n$ primo

dimostriamo l'implicazione equivalente

n non è primo $\Rightarrow (\mathbb{Z}_n, +, \cdot)$ non è un campo

Se n non è primo esistono d, d' tali che $n = d\,d'$

e $1 < d, d' < n$

In $\mathbb{Z}_n$ $\bar{d} \neq \bar{0}$ $\bar{d}' \neq \bar{0}$ e $\bar{d}\cdot\bar{d}' = \overline{dd'} = \bar{n} = \bar{0}$

otteniamo che $(\mathbb{Z}_n, +, \cdot)$ non è un campo

2ª parte

Ci servono alcune proprietà che si usano spesso

Prop1 $p, a, b \in \mathbb{Z}$, p numero primo

Se $p \mid a \cdot b$ allora $p \mid a$ o $p \mid b$

($x \mid y$ significa x divide y)

Prop2 $f : X \to X$ X insieme finito

i) se f è iniettiva allora f è biettiva

ii) se f è suriettiva allora f è biettiva

(Principio delle piccionaia)

Supponiamo n sia primo e fissiamo

$\bar{a} \in \mathbb{Z}_n$ con $\bar{a} \neq \bar{0}$

Definiamo $\varphi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$

$\bar{x} \longrightarrow \bar{a}\,\bar{x}$

1° passo φ è iniettiva

$$\varphi(\bar{x}) = \varphi(\bar{y})$$

$$\Rightarrow \bar{a}\,\bar{x} = \bar{a}\,\bar{y}$$

$$\Rightarrow \overline{ax} = \overline{ay}$$

$$\Rightarrow \overline{ax - ay} = \bar{0}$$

$\Rightarrow p$ divide $ax - ay = a(x-y)$

Per proposizione 2
ottengo che $n \mid a$ oppure $n \mid (x-y)$
Se $n \mid a$ allora $\overline{a} = \overline{0}$ contraddizione
Quindi ho che $n \mid (x-y)$
ole cui $\overline{x} = \overline{y}$

2° passo φ è suriettivo

per il principio delle piccionaie

3° passo $\overline{a}$ ha elemento inverso

φ suriettivo $\Longrightarrow$ $\forall\, \overline{y} \in \mathbb{Z}_m \; \exists\, \overline{x} \in \mathbb{Z}_n$ tale che $\varphi(\overline{x}) = \overline{y}$

Considero $\overline{1} \in \mathbb{Z}_m$ allora esiste $\overline{x} \in \mathbb{Z}_m$ tale che

$$\varphi(\overline{x}) = \overline{a}\,\overline{x} = \overline{1}$$

(per def)

$\overline{x}$ è l'inverso di $\overline{a}$

Ogni elemento diverso da 0 ha elemento inverso

$\Longrightarrow$

se m è primo $(\mathbb{Z}_m, +, \cdot)$ è un campo

compi $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \mathbb{Z}_{11}, \ldots$

non compi $\mathbb{Z}_4, \mathbb{Z}_6, \mathbb{Z}_8, \mathbb{Z}_9, \ldots$

Esempi (riepilogo)

$(\mathbb{Q}, +, \cdot)$ $(\mathbb{R}, +, \cdot)$ $(\mathbb{C}, +, \cdot)$

$(\mathbb{Z}_p, +, \cdot)$ ← compi finiti

ESERCIZI

1) In $\mathbb{R}^2$ si definiscano le seguenti operazioni

$$(x,y) + (z,w) = (x+z, y+w)$$

$$(x,y) \cdot (z,w) = (xz - yw, xw + yz)$$

Verificare che $(\mathbb{R}^+, +, \cdot)$ è un campo

Dim $\boxed{+ \text{ è associativa}}$ per ogni $(x,y),(z,w),(u,v) \in \mathbb{R}^2$

$$((x,y)+(z,w))+(u,v) =$$

$$= (x+z, y+w)+(u,v) =$$

$$= ((x+z)+u, (y+w)+v) =$$

$$= (x+(z+u), y+(w+v)) =$$

$$= (x,y) + (z+u, w+v) =$$

$= (x,y) + ((z,w) + (u,v))$

esistenza zero

per ogni $(x,y) \in \mathbb{R}^2$ $(0,0) + (x,y) =$

$= (y,x) + (0,0) = (x,y)$

$(0,0)$ è lo zero di $(\mathbb{R}^2, +, \cdot)$

esistenza elementi opposti

Fissato $(x,y) \in \mathbb{R}^2$ ottengo

$(x,y) + (-x,-y) = (-x,-y) + (x,y) = (0,0)$

$(-x,-y)$ è l'opposto di (x,y)

+ è commutativa

Per ogni $(x,y), (z,w) \in \mathbb{R}^2$

$(x,y) + (z,w) = (x+z, y+w)$

$= (z+x, w+y) = (z,w) + (x,y)$.

• è associativa

per ogni (x,y), (z,w) $(u,v) \in \mathbb{R}^2$

$$((x,y)\cdot(z,w))\cdot(u,v) =$$

$$= (xz-yw, xw+yz)(u,v)$$

$$= ((xz-yw)u-(xw+yz)v, (xz-yw)v+(xw+yz)u)$$

$$= (xzu-ywu-xwv-yzv, xzv-ywv+xwu+yzu)$$

$$(x,y)\cdot((z,w)\cdot(u,v)) =$$

$$= (x,y)\ (zu-wv, zv+wu)$$

$$= (x(zu-wv)-y(zv+wu), x(zv+wu)+y(zu-wv))$$

$$= (xzu-xwv-yzv-ywu, xzv+xwu+yzu-ywv)$$

confrontando otteniamo:

$$((x,y)\cdot(z,w))\cdot(u,v) = (x,y)\cdot((z,w)\cdot(u,v))$$

esistenza unità

per ogni $(x,y) \in \mathbb{R}^2$

$$(x,y)\cdot(1,0) = (x\cdot 1 - y\cdot 0,\ x\cdot 0 + y\cdot 1)$$
$$= (x,y)$$

$$(1,0)\cdot(x,y) = (1\cdot x - 0\cdot y,\ 1\cdot y + 0\cdot x)$$
$$= (x,y)$$

$\Rightarrow$ $(1,0)$ è l'unità di $(\mathbb{R}^2, +, \cdot)$

esistenza inversi $(x,y) \neq (0,0)$

$$(x,y)^{-1} = \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right)$$

infatti

$$(x,y)\cdot\left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right) =$$

$$= \left(\frac{x^2}{x^2+y^2} - \frac{y\cdot(-y)}{x^2+y^2},\ \frac{-xy}{x^2+y^2} + \frac{yx}{x^2+y^2}\right)$$

$$= \left(\frac{x^2+y^2}{x^2+y^2},\ 0\right) = (1,0)$$

analogamente

$$\left(\frac{x}{x^2+y^2}, -\frac{y}{x^2+y^2}\right)\cdot(x,y) = (1,0)$$

- è commutativa

- vale la prop. distributiva di $\cdot$ rispetto a $+$

Lasciate per esercizio

$(\mathbb{R}^2, +, \cdot)$ è un campo

Oss per chi conosce $\mathbb{C}$

$$(x,y) \longrightarrow x+iy$$

$(x,y)+(z,w) = (x+z, y+w)$

$(x+iy)+(z+iw)$
$= (x+z)+i(y+w)$

$(x,y)\cdot(z,w) = (xw-yz, xw+yz)$

$(x+iy)\cdot(z+iw)$
$= (xz-yw)+i(xw+yz)$

$(0,1)\cdot(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0)$
$= (-1,0) = -(1,0)$

$i^2 = -1$