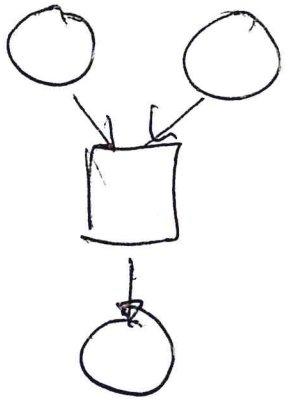
ALGEBRA

Studio delle operazioni

X insieme operazione = funzione $X \times X \to X$

prodotto cartesiano = coppie ordinate di elem. di X



$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$

$(2,7) \mapsto 9$

$\cup$ unione $X = \{ \text{insiemi} \}$

$A \cup B \mapsto A \cup B$

$A \cup B = B \cup A$ ok

$(A \cup B) \cup C = A \cup (B \cup C)$ ok

$A \cup \emptyset = A$ ok

$\forall A \; \exists B$ t.c. $A \cup B = \emptyset$? NO

un'altra operazione è l'intersezione (ha proprietà simili)

Aritmetica modulo n

ore $16,5 + 10 = 2,5$

0 —— 24 25
‖ ↑
0 1

$\{0, \dots, 23\}$ somma modulo 24

$n+m$ → $n+m$ se $n+m < 24$

$n+m$ → $n+m-24$ se $n+m \geq 24$

1) associativa
2) commutativa
3) $\exists$ elem. neutro 0
4) $\forall n \in \{0, \dots, 23\} \; \exists$ l'opposto $24-n$

GRUPPO COMMUTATIVO

Ex Somma modulo 10 $\{0, \dots, 9\}$

$$\begin{array}{r} 17 \\ +\ 49 \\ \hline 66 \end{array}$$

Ex somma modulo 2 $\{0,1\}$ $1+1=0$ somma digitale

In generale $\forall n$ somma modulo n

$\mathbb{Z}_n = \{0, \dots, n-1\}$ è gruppo commutativo.

Ex Prodotto modulo 24 $7 \cdot 8 = 56 \to 32 \to 8$

prodotto modulo 10 $7 \cdot 8 = 56 \dashrightarrow 6$

$$\begin{array}{r} 327 \cdot \\ \quad 8 \\ \hline 6 \end{array}$$

Ex prodotto modulo 10

esiste l'inverso di 7? $\exists n$ t.c. $7n = 1$?

$7 \cdot 3 = 21 \to 1$

esiste l'inverso di 5? non c'è.

$5 \cdot 4 = 0$

In generale

prodotto modulo n ogni numero diverso da 0 ha un inverso quando n è primo

$n = 5$

$\frac{1}{1} = 1 \quad \frac{1}{2} = 3 \quad \frac{1}{3} = 2 \quad \frac{1}{4} = 4$

$\mathbb{Z}_n$ $+$ $\cdot$

CAMPO NUMERICO se $\cdot$ è distributivo risp. a $+$
e ogni elem. $\neq 0$ ha inverso

$\mathbb{Q}$ $\mathbb{R}$ $\mathbb{C}$ $\mathbb{Z}_n$ n è primo $\mathbb{Z}_2$ $\mathbb{Z}_3$ $\mathbb{Z}_5$

Ex $\begin{cases} x+y=1 \\ x-y=0 \end{cases}$ fra i reali $x=y=1/2$ $(1/2, 1/2)$

in $\mathbb{Z}_2$? $-y=(-1)y$ chi è -1? $-1=1$ (in $\mathbb{Z}_2$)

$-y=y$

$\begin{cases} x+y=1 \\ x+y=0 \end{cases}$ insolubile in $\mathbb{Z}_2$

in $\mathbb{Z}_3$? $-1=2$ $\begin{cases} x+y=1 \\ x+2y=0 \end{cases}$

$\left(\begin{array}{cc|c} 1 & 1 & 1 \\ 1 & 2 & 0 \end{array}\right)$ $R_2 \to R_2 - R_1$

$\left(\begin{array}{cc|c} 1 & 1 & 1 \\ \boxed{0} & 1 & -1 \end{array}\right)$

$y=-1=2$ $x+2=1$ $x=1-2=-1=2$

risolubile in $\mathbb{Z}_3$

Aritmetica nella modulo n

a, b sono uguali mod. n se e solamente se $\iff$ a−b è divisibile per n

Ex $88 = 73 \mod 5$ perché $88 - 73 = 15$ è div. per 5

Relazioni di equivalenza

X $\quad R \subseteq X \times X$

1) riflessiva $(a,a) \in R \quad \forall a$
2) simmetrica $(a,b) \in R \Rightarrow (b,a) \in R$
3) transitiva $(a,b) \in R \quad (b,c) \in R \Rightarrow (a,c) \in R$

classe di equivalenza di $y \in X$ $\quad \{x : (x,y) R\}$

Ex X = città del mondo

$(a,b) \in R \iff$ a, b stanno nella stessa nazione

(Francoforte, Berlino) $\in R$ $\quad$ (Roma, Milano) $\in R$ $\quad$ (Roma, Parigi) $\notin R$

R è una relaz. di equiv.

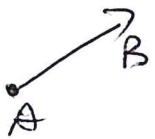
classe di equiv. di Milano = {tutte le città d'Italia}

Ex **equipollenza**

X = coppie ordinate di punti

- $((A,B),(C,D)) \in R \iff ACDB$ è parallelogr.

R è relaz. di equiv.

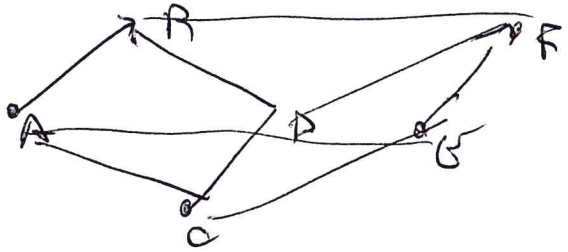


$ABBA$ è parall. $\Rightarrow$ riflessiva

$ACDB$ parall. simm.

$\Rightarrow CBAD$ //

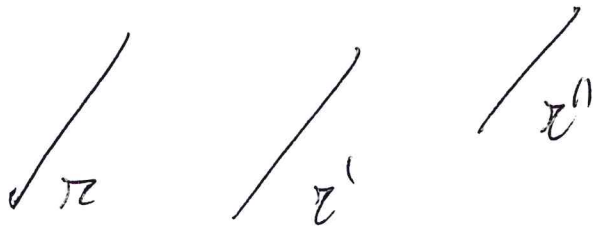
$ACDB$ parall. $CEFD$ parall $\Rightarrow AEFB$ parall.



vettore geom = classe di equiv. di coppie di punti

Ex parallelismo

X = {rette dello spazio} $(r, r') \in R$ se r è parallela a r', $r \parallel r'$



R è relazione di equivalenza

—

Def Dato X e una relaz. di equiv. su X presa una classe di equivalenza, ogni elemento si chiama RAPPRESENTANTE della classe di equivalenza.

—

Ex Dato in vettori geom. $\forall$ punto O $\exists$ un unico rappresentante di v che ha punto di applic. O

ex $\mathbb{Z}$ fissato n

$(a,b) \in R \iff a = b$ modulo n

1) riflessiva (a,a) $a - a = 0$ divisibile per n

2) simm. $(a,b) \in R \overset{?}{\Rightarrow} (b-a) \in R$

$\Downarrow$ $\Uparrow$

$a-b$ è div. per n $\Rightarrow$ $b-a$ è div. per n

3) trans. $(a,b) \in R$ $(b,c) \in R \overset{?}{\Rightarrow} (a,c) \in R$

$\Downarrow$ $\Downarrow$

$a-b$ div. per n $b - c = hn$ $a - c = a - b + b - c$

$a - b = kn$ $= kn + hn = (k+h)n$

è mult. di n.

quindi R è di equival.

Ex $n = 5$

classe di eq. di $7 = \{ \dots, -8, -3, 2, 7, 12, 17, 22, 27, \dots \}$

$11 = \{ \dots, -4, 1, 6, 11, 16, 21, 26, \dots \}$

$\exists$ un unico rappresentante $0 \le \quad \le n-1$