



# Teoria degli insiemi

24/09

Un insieme è una "collezione" di elementi (definizione non rigorosa)

es

$$\{0, 1\} \quad \{\text{rosso, nero}\} \quad \{0, 1, 2, \dots\} = \mathbb{N}$$

$\emptyset$  = insieme vuoto

↪ privo di elementi e contenuto in tutti gli insiemi

Quando un insieme non può essere descritto con una lista viene preso un insieme un insieme "universo"  $U$ . I sottoinsiemi di  $U$  si caratterizzano con delle proprietà

es  $U = \mathbb{N}$

$$I = \{x \in \mathbb{N} : x \text{ è pari}\} \text{ oppure } \{x \in \mathbb{N} : 2 \mid x\}$$

↓ è divisibile per 2

Inoltre gli insiemi hanno delle relazioni tra di essi

es  $I, J$  sottoinsiemi di  $U$

$$I \subseteq J \leftrightarrow \forall x \in I, x \in J$$

$$I \not\subseteq J \leftrightarrow \exists x \in I, x \notin J$$

$$x \in I \leftrightarrow \{x\} \subset I$$

↳ singleton  $x$

equivalentemente si può scrivere

$$\{(I, J) \text{ con } I \subseteq U, J \subseteq U : J \subsetneq I \wedge I \not\subseteq J\} \neq \emptyset$$

$$\exists I, J | I \not\subseteq J \wedge J \not\subseteq I$$

## DEF COMPARABILITÀ

dati:  $I, J \subseteq U$

$I \in J$  sono comparabili se  $I \subseteq J \vee J \subseteq I$

## DEF UGUAGLIANZA

dati:  $I, J \subseteq U$

$I \in J$  sono uguali se  $I \subseteq J \wedge J \subseteq I \leftrightarrow I = J$

operazioni tra insiemi ( $I, J \subset U$ )

$$I \cap J := \{x \in U : x \in I \wedge x \in J\}$$

$$I \cup J := \{x \in U : x \in I \vee x \in J\}$$

es

$$I = \{1, 2, 3\}, J = \{3, 4, 5\}$$

$$I \cap J = \{3\} \quad I \cup J = \{1, 2, 3, 4, 5\}$$

$$\mathbb{N} \supset I = \{x \in \mathbb{N} : x \text{ pari}\} \quad \mathbb{N} \supset J = \{x \in \mathbb{N} : x \text{ dispari}\}$$

$$I \cap J = \emptyset \quad I \cup J = \mathbb{N}$$

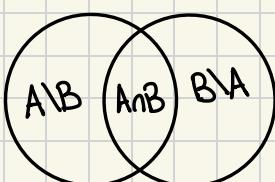
↪ supponiamo per assurdo  $\exists x \in I \cap J$ , il che vuol dire che

$x = 2q = 2q' + 1 \rightarrow 2(q - q') = 1$  che è impossibile dato che 1 non  
è divisibile per 2

algoritmo della divisione euclidea per 2

$$x \in \mathbb{N} \quad \exists !(q, r) \in \mathbb{Z} \times \mathbb{N} \text{ t.c. } x = 2q + r \text{ con } 0 \leq r \leq 1$$

Diagramma di Venn (e la sua fallacia)

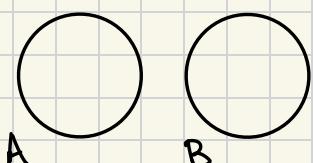


$$A \setminus B = \{x \in A : x \notin B\}$$

$$A \cup B = (A \setminus B) \cup (A \cap B) \cup (B \setminus A)$$

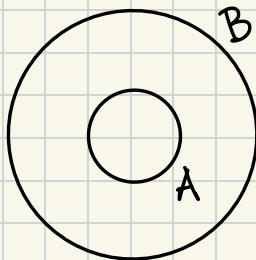
→ unione disgiunta  
 $A \cup B = A \cup B$  nel caso in cui  
A e B sono disgiunti

$$A \cap B = \emptyset$$

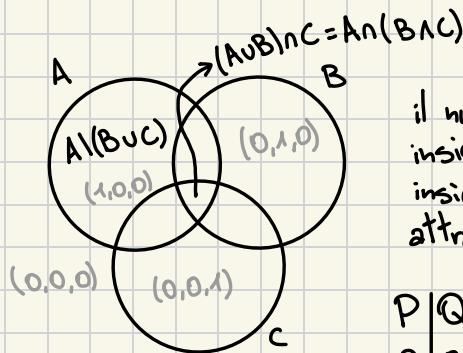


$$A \setminus B = A$$

$$B \setminus A = B$$



$$\begin{aligned} & A \subset B \\ & A \setminus B = \emptyset \\ & A \cap B = A \end{aligned}$$

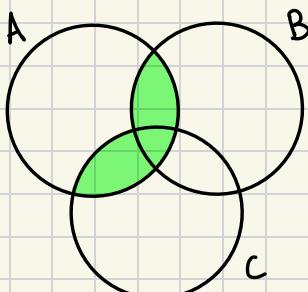


il numero massimo di sezioni date dall'unione di più insiemi è dato da  $2^n$  (dove  $n$  è il numero di insiemi, in questo caso  $2^3=8$ ). Questo è verificabile attraverso una tavola di verità:

P	Q	R
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

Questa verità però crolla quando si provano a rappresentare tutte le sezioni date dall'unione di 4 insiemi dato che in 2 dimensioni posso rappresentare solo 14 sezioni, e non 16

### Esercizio



$$A := \{x \in U : P(x) \text{ vera}\}$$

$$B := \{x \in U : Q(x) \text{ vera}\}$$

$$C := \{x \in U : R(x) \text{ vera}\}$$

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



## Prodotto cartesiano

dati:  $X, Y$  due insiemi non vuoti

si definisce  $X \times Y = \{(x, y) : x \in X, y \in Y\}$

$$\begin{aligned} \mathbb{R}^n &:= \mathbb{R} \times \mathbb{R}^{n-1} \\ \mathbb{R}^1 &:= \mathbb{R} \end{aligned}$$

$$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\} \quad X = Y = \mathbb{R}$$

es

$$(x, y, z) = (x(y, z)) = (x, \{y, \{z\}\}) = \{x, \{x, \{y, \{z\}\}\}\}$$

## Corrispondenza

### DEF CORRISPONDENZA

una corrispondenza su  $X$  e  $Y$  è il dato  $(X, Y, \Gamma)$  questo è detto grafo

dominio codominio gamma, sottoinsieme non vuoto di  $X \times Y$

## Relazione

### DEF RELAZIONE

una relazione è un tipo particolare di corrispondenza in cui il codominio è uguale al dominio

$(X, X, \Gamma) \rightarrow$  generalmente si scrive  $(X, \Gamma)$

$$x R y \leftrightarrow (x, y) \in \Gamma$$

$\hookrightarrow x$  e  $y$  si dice che sono in relazione

## proprietà

### riflessiva

$R$  è riflessiva se  $\forall x \in X \quad x R x \quad (\leftrightarrow \forall x \in X, (x, x) \in \Gamma)$

## simmetrica

$R$  è simmetrica se  $\forall x, y \in X$  se  $x R y$  allora  $y R x$

## transitiva

$R$  è transitiva se presi  $x, y, z \in X$ , ( $x R y$  e  $y R z \rightarrow x R z$ )

una relazione che contemporaneamente soddisfa le 3 proprietà è detta **relazione di equivalenza**

**es** relazione di uguaglianza

si prende  $R = (\mathbb{R}, \Delta)$  dove  $\Delta = \{(x, x) : x \in \mathbb{R}\}$

$$x R y \leftrightarrow x = y$$

= è riflessiva  $\forall x \in \mathbb{R} x = x$

= è simmetrica  $\forall x, y \in \mathbb{R} x = y \rightarrow y = x$

= è transitiva  $\forall x, y, z \in \mathbb{R}, x = y \wedge y = z \rightarrow x = z$

**es**  $X = \{\text{rette di } \mathbb{R}^2\}$

→ rette di  $\mathbb{R}^2$

$r, r' \in X$

$r \parallel r' \leftrightarrow r e r'$  sono parallele

il parallelismo è una relazione di equivalenza

Il è riflessiva: ogni retta è parallela a sé stessa

Il è simmetrica: se  $r \parallel r'$  allora  $r' \parallel r$

Il è transitiva: se  $r \parallel r' \wedge r' \parallel r'' \rightarrow r \parallel r''$

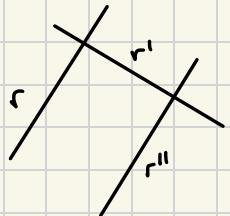
**es**  $X = \{\text{rette di } \mathbb{R}^2\}$

$r, r' \in X r \perp r' \leftrightarrow r e r'$  sono ortogonali

$\perp$  è simmetrica  $\rightarrow$  se  $r \perp r' \rightarrow r' \perp r$

$\perp$  non è riflessiva  $\rightarrow r \not\perp r$

$\perp$  non è transitiva  $\rightarrow$  se  $r \perp r', r' \perp r'' \rightarrow r \not\perp r''$



es  $X = \mathbb{R}$   $x \leq y$

riflessiva  $\forall x, x \leq x$

transitiva  $\forall x, y, z \quad x \leq y \wedge y \leq z \rightarrow x \leq z$

non è simmetrica  $2 \leq 3$  ma  $3 \not\leq 2$

è una relazione antisimmetrica

$\hookrightarrow \forall x, y \in X, x \leq y \wedge y \leq x \rightarrow x = y$

oss notare che c relazione su  $\{Y : Y \subset X\}$  è, come  $\leq$ , riflessiva antisimmetrica e transitiva

è una relazione totale  $\Rightarrow \forall x, y \in \mathbb{R}, x R y \vee y R x$  (non è esclusivo)

## Studio delle relazioni di equivalenza

sia  $R = (X, \Gamma)$  relazione di equivalenza

$x \in X$ , poniamo  $C(x) = \{y \in X \mid x R y\} \subset X$

$\hookrightarrow$  insieme con tutti gli elementi in relazione tra loro

$C(x)$  è la classe di equivalenza di  $x$  e  $x$  è un rappresentante di tale classe  $C(x) = C(x')$

con  $x \neq x'$

oss notare che  $C(x) \neq \emptyset$ , infatti  $x \in C(x)$  dato che  $R$  è riflessiva

proposizione 1  $R = (X, \Gamma)$  d'equivalenza

1)  $x, y \in X$ , allora  $C(x) = C(y) \leftrightarrow x R y$

2)  $\forall x, y \in X$  allora  $\begin{cases} \circ C(x) = C(y) \\ \circ C(x) \cap C(y) = \emptyset \end{cases} \rightarrow$  disgiunti

in particolare, date una classe di equivalenza  $C$ , allora  $\forall x \in C \quad C = Cl(x)$   
(ogni elemento è rappresentante)

dim 1

supponiamo  $Cl(x) = Cl(y) \rightarrow y \in Cl(x) \rightarrow x R y$

supponiamo  $x R y$  allora  $y \in Cl(x)$

sia  $z \in Cl(y)$  si ha che  $y R z$ , si ha quindi che  $x R y \wedge y R z \rightarrow x R z \rightarrow z \in Cl(x)$

Quindi  $Cl(y) \subset Cl(x)$ . Ma posso scambiare i ruoli di  $x$  e  $y$  e mostrare  
nello stesso modo che  $Cl(x) \subset Cl(y) \rightarrow Cl(x) = Cl(y)$

dim 2

siano  $x, y \in X$ .

se  $Cl(x) \cap Cl(y) = \emptyset$  non c'è nulla da dimostrare

supponiamo che  $Cl(x) \cap Cl(y) \neq \emptyset$

sia  $z \in Cl(x) \cap Cl(y)$  allora si ha  $x R z$  e  $z R y$  per transitività  
 $x R y$  inoltre per ① si ha  $Cl(x) = Cl(y)$

**DEF** INSIEME DELLE PARTI

dato  $X$  insieme non vuoto

consideriamo  $\mathcal{P}$ : cui elementi sono sottoinsiemi di  $X$  ( $P \in \mathcal{P} \rightarrow P \subseteq X$ )

$\mathcal{P} := \{P : P \subseteq X\}$  è detto **insieme delle parti di  $X$**

es)  $X = \{1, 2, 3\}$

$\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

**DEF** PARTIZIONE

sia  $\mathcal{P} \subset \mathcal{P}(X)$  non vuoto

si dice che  $\mathcal{P}$  è una **partizione di  $X$**  se:

1)  $\forall P \in \mathcal{P} \quad P \neq \emptyset$

2)  $\forall P, Q \in \mathcal{P}, P \neq Q \rightarrow P \cap Q = \emptyset$

3)  $\forall x \in X \quad \exists P \in \mathcal{P} \mid x \in P$

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

$$\mathcal{P} = \{\{1\}, \{2\}, \{3\}\} \quad \mathcal{Q} = \{\{1, 3\}, \{2\}\} \quad \mathcal{R} = \{\{1, 2\}, \{3\}\}$$

proposizione 2  $\mathcal{R} = (X, \Gamma)$  relazione di equivalenza

$\mathcal{P} = \{Cl(x) : x \in X\}$  è una partizione di  $X$

dim  
se  $P \in \mathcal{P}$ , allora  $P = Cl(x) \exists x \in X$   
 $\textcircled{1} \quad \mathcal{R}$  riflessiva  $\rightarrow x \in P \rightarrow P \neq \emptyset$

$\textcircled{2}$  se  $Cl(x) \neq Cl(y) \rightarrow Cl(x) \cap Cl(y) = \emptyset$  (dimostrato prima)

$\textcircled{3}$  sia  $x \in X$  allora  $x \in Cl(x)$  ( $\mathcal{R}$  riflessiva)

DEF QUOTIENTE DI  $X$  PER  $\mathcal{R}$

$X/\mathcal{R}$  ( $\circ$   $\frac{X}{\mathcal{R}}$ ) è l'insieme delle classi di equivalenza di  $X$  per  $\mathcal{R}$

$$X/\mathcal{R} = \{Cl(x) : x \in X\}$$

# Sistema completo di rappresentanti $\mathcal{R}(X, \Gamma)$

26/09

Un sistema completo di rappresentanti di  $\mathcal{R}$  (o SCR) è un sottoinsieme  $X' \subset X$  t.c.

1)  $\forall x'_1, x'_2 \in X', x'_1 \neq x'_2 \rightarrow C(x'_1) \cap C(x'_2) = \emptyset$

un insieme che ha  
un elemento per  
classe d'equivalenza

2)  $\forall x \in X \exists! x' \in X' \text{ t.c. } x \in C(x')$

es)  $X = \{r \text{ retta di } \mathbb{R}^2\}$

$\mathcal{R} = \parallel \text{parallelismo} \rightarrow \mathcal{R}$  è una relazione di equivalenza

$X' = \{\text{rette per l'origine}\}$  è un sistema completo di rappresentanti per  $\mathcal{R}$   
 $X' \subset X$

① è verificata in quanto due rette per l'origine distinte non sono parallele

②  $r \in X$  esiste un'unica retta  $r' \in X'$  con  $r' \parallel r$

oss) in generale non c'è unicità per un SCR ad esempio possiamo scegliere  $P \in \mathbb{R}$  e il fascio di rette per  $P: X_P$  è un SCR  
non c'è in generale canonicità nella scelta di un SCR

es)

$X \neq \emptyset \quad x, x' \in X \quad x \mathcal{R} x' \Leftrightarrow x = x'$  (relazione d'equivalenza)

$\mathcal{R}$  è l'uguaglianza  $\frac{X}{\mathcal{R}} = X \rightarrow X$  è l'unico SCR

ogni classe di equivalenza è un singleton

es)

$x, x' \in X$  allora  $x \mathcal{R} x'$  sempre  $\Rightarrow$  es.  $\frac{X}{\mathcal{R}} = X$

c'è una sola classe di equivalenza  $\frac{X}{\mathcal{R}} = \{x\}$

in questo caso ogni SCR è un singleton della forma  $\{x\}$  con  $x \in X$

## Esercizi

Esercizio 1. Determinare il grafico della corrispondenza tra  $X := \{1, 2, 3, 4\}$  ed  $Y := \{1, 3, 5\}$  definita nella seguente maniera:

$x$  "è minore o uguale a"  $y$ .

sto considerando una corrispondenza  $C = (X, Y, \Gamma)$

$$\begin{aligned}\Gamma \subset X \times Y &= \{(x, y) : x \in X, y \in Y, x \leq y\} = \\ &= \{(1, 1)(1, 3)(1, 5)(2, 3)(2, 5)(3, 3)(3, 5)(4, 5)\}\end{aligned}$$

$$X = \mathbb{N}^* := \mathbb{N} \setminus \{0\} = \{1, 2, 3, \dots\}$$

introduciamo la relazione di divisibilità  
se  $x, y \in \mathbb{N}^*$ ,  $x | y$  se  $y$  è un multiplo di  $x$  per un fattore intero  
 $\hookrightarrow$  "divide"

ovvero:

$$x | y \Leftrightarrow \exists k \in \mathbb{N}^* \text{ t.c. } y = kx$$

$$1) \text{ riflessiva} \rightarrow \forall x \in \mathbb{N}^* \quad x | x \quad x = x \cdot 1$$

$$2) \text{ transitiva} \rightarrow x, y, z \in \mathbb{N}^* \text{ con } x | y \wedge y | z \text{ si ha } y = kx, z = ky \\ z = k(kx) = (k'k)x \Rightarrow x | z$$

$$3) \text{ antisimmetrica} \rightarrow x, y \in \mathbb{N}^* \text{ con } x | y \text{ e } y | x \Leftrightarrow y = kx \text{ e } x = k'y \\ \text{quindi } y = k'kx \text{ ma } y \neq 0 \Rightarrow 1 = k \cdot k' \\ \text{ma in } \mathbb{N}^*, kk' = 1 \Rightarrow k = k' = 1 \text{ se ne deduce } y = 1 \cdot x = x \Rightarrow y = x$$

## Esercizio

Esercizio 7. Dire quali delle seguenti relazioni è antisimmetrica: (a)  $x$  è minore o uguale a  $y$  (b)  $x$  è minore di  $y$  (c)  $x + 2y = 10$  (d)  $x$  divide  $y$ .

Ⓐ

$$x = \mathbb{R} \quad x R y \Leftrightarrow x + 2y = 10$$

$$x R y \Leftrightarrow x + 2y = 10$$

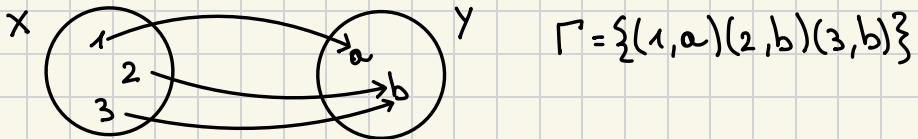
$$y R x \Leftrightarrow y + 2x = 10$$

supponiamo quindi  $x R y, y R x$

$$\begin{cases} x + 2y = 10 \\ y + 2x = 10 \end{cases} \quad \begin{cases} x = 10 - 2y \\ y + 20 - 4y = 10 \end{cases} \quad \begin{cases} x = 10 - 2 \cdot \frac{10}{3} \\ y = \frac{10}{3} \end{cases} \quad \begin{cases} x = \frac{10}{3} \\ y = \frac{10}{3} \end{cases}$$

## Applicazioni (funzioni)

Una funzione è una corrispondenza  $f = (X, Y, \Gamma)$  con le proprietà che  $\forall x \in X \exists! y \in Y$  con  $(x, y) \in \Gamma$   
 si scrive  $y = f(x)$  o anche  $X \xrightarrow{f} Y$

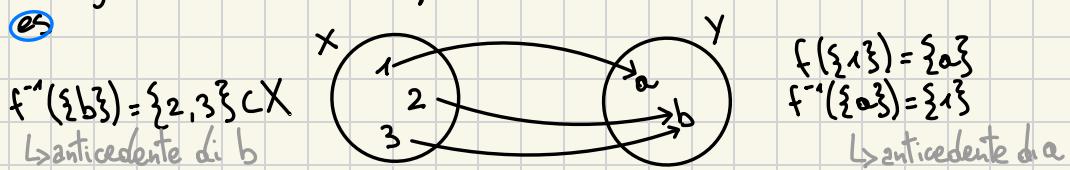


Il **codominio** si dice insieme immagine. Sia  $f: X \rightarrow Y$  funzione  $X' \subset X$   
 $f(X') = \{y \in Y : \exists x \in X' \text{ con } f(x) = y\}$

↳ tutti gli elementi raggiunti  
dal primo insieme

immagine di  $X'$  per  $f$   $f(X') \subset Y$   
 $Y' \subset Y$   $f^{-1}(Y') = \{x \in X : f(x) \in Y'\}$  corrispondente  
 immagine inversa di  $Y'$  ( $f^{-1}(Y')$  sottoinsieme di  $X$ )

es



particolari tipi di funzioni

funzioni iniettive  $X \xrightarrow{f} Y$

una funzione è detta iniettiva se  $x, x' \in X$   $f(x) = f(x')$  allora  $x = x'$   
 alternativamente

$$\forall y \in Y \quad f^{-1}(\{y\}) = \begin{cases} \emptyset \\ \text{singleton} \end{cases}$$

es

$$f: \mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0} \quad f(x) := \frac{1}{x} \quad f(x) = f(x') \Rightarrow x = x' \Rightarrow$$

$$x \mapsto \frac{1}{x} \qquad \Rightarrow \frac{1}{x} = \frac{1}{x'} \Rightarrow x \cdot \frac{1}{x} = x' \cdot \frac{1}{x'} \Rightarrow x = x'$$

funzione suriettiva  $f: X \rightarrow Y$

si dice che  $f$  è suriettiva se  $f(X) = Y$   
 alternativamente  $\forall y \in Y, \exists x \in X$   $f(x) = y$

o anche  $\forall y \in Y, f^{-1}(\{y\}) \neq \emptyset$

(es)  $f: \mathbb{R} \rightarrow \mathbb{R}$

sia  $y \in \mathbb{R}_{\geq 0}$  allora esiste una radice  $x$  dell'equazione polinomiale  $x^2 - y = 0$   $f(x) = y$

dim  $\forall y \in \mathbb{R}_{\geq 0}, \exists x \in X$  t.c.  $f(x) = x^2 = y$  posso porre  $x = \sqrt{y}$  l'unico reale positivo tale che  $x^2 = y$

### funzione biettive

una funzione  $f: X \rightarrow Y$  è biettiva se è al tempo stesso suriettiva e iniettiva  
 $f$  iniettiva  $\Leftrightarrow \forall y \in Y, f^{-1}(\{y\}) = \emptyset$

oppure è un singleton

$f$  suriettiva  $\Leftrightarrow \forall y \in Y, f^{-1}(\{y\}) \neq \emptyset$

dunque  $f$  è biettiva  $\Leftrightarrow \forall y \in Y, f^{-1}(\{y\})$  è un singleton  
ogni elemento del codominio ha un unico antecedente

(es)

$X$  insieme  $\neq \emptyset$   $Id_X := (X, X, \Delta_X)$

$\Delta_X = \{(x, x) : x \in X\} \quad \forall x \quad Id_X(x) = x$

$\hookrightarrow$  sottoinsieme diagonale ( $X \times X$ )

$Id_X^{-1}(\{x\}) = \{x\}$



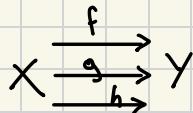
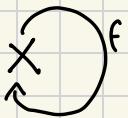
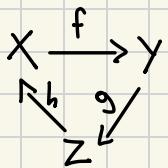
DEF DIAGRAMMA

un diagramma è una collezione di insiemi non vuoti collegati da applicazioni

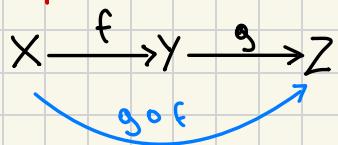
(es)

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \downarrow & \\ & Z & \end{array}$$

è un diagramma



## Operazioni sulle funzioni



in questo caso si ha una funzione  $f$  che unisce  $X$  e  $Y$  e una funzione  $g$  che unisce  $Y$  e  $Z$ , dunque la funzione che collega  $X$  e  $Z$  è detta  $g$  composto  $f$

Si definisce la funzione composta come funzione definita da  $(g \circ f)(x) = g(f(x))$

$$X \xrightarrow{g \circ f} Z$$

(es)

$$X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} T$$

$$(h \circ g \circ f)(x) = h(g(f(x)))$$

DEF FUNZIONE INVERSA

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ f \text{ biettiva} & \leftrightarrow & \exists g: Y & \longrightarrow & X \text{ t.c. } f \circ g = \text{id}_Y \quad g \circ f = \text{id}_X \end{array}$$

$\hookrightarrow$  parte  $Y$  poi applica  $g$  e arriva in  $X$  poi applica  $f$  per tornare in  $Y$   
 $y \in Y, g(y) \in X, f(g(y)) \in Y$

$g$  è chiamata la funzione inversa (se esiste è unica)

dim

$$f \text{ biettiva} \rightarrow \forall y \in Y \ \exists ! x \in X \mid f(x) = y$$

poniamo  $g(y) = x$  ben definita

Osserviamo  $g \circ f$  se  $x \in X$   $g(f(x)) = g(y)$  e  $x$  è l'unico elemento t.c.  $f(x) = y$  quindi  $g(y) = x \rightarrow g \circ f = id_X$   
omettiamo di verificare che  $f \circ g = id_Y$

Mostriamo che  $g$  è suriettiva

Sia  $x \in X$  e poniamo  $y = f(x)$

$g(y) = g(f(x)) = (g \circ f)(x) = x$ , in quanto  $f \circ g = id_Y \rightarrow g^{-1}(\{x\}) \neq \emptyset$   
quindi  $f$  è suriettiva

Mostriamo che  $g$  è iniettiva

Siano  $y, y' \in Y$  |  $g(y) = g(y') = x$

Allora applicando  $f$  a sinistra ottengo  $f(g(y)) = f(g(y')) = f(x)$

$$y = (f \circ g)(y) = (f \circ g)(y') = y$$

**Teorema di struttura per le applicazioni**

$X \xrightarrow{f} Y$  obiettivo costruire una relazione d'equivalenza  $\sim$  su  $X$

Si pone  $x, x' \in X$ ,  $x \sim x' \Leftrightarrow f(x) = f(x')$

$\sim$  è una relazione d'equivalenza

$$x \sim x \rightarrow f(x) = f(x)$$

riflessiva

$$x \sim x' \Leftrightarrow f(x) = f(x') \Leftrightarrow x' \sim x$$

simmetrica

$$x \sim x', x' \sim x'' \Leftrightarrow f(x) = f(x'), f(x') = f(x'') \rightarrow f(x) = f(x'') \rightarrow x \sim x''$$

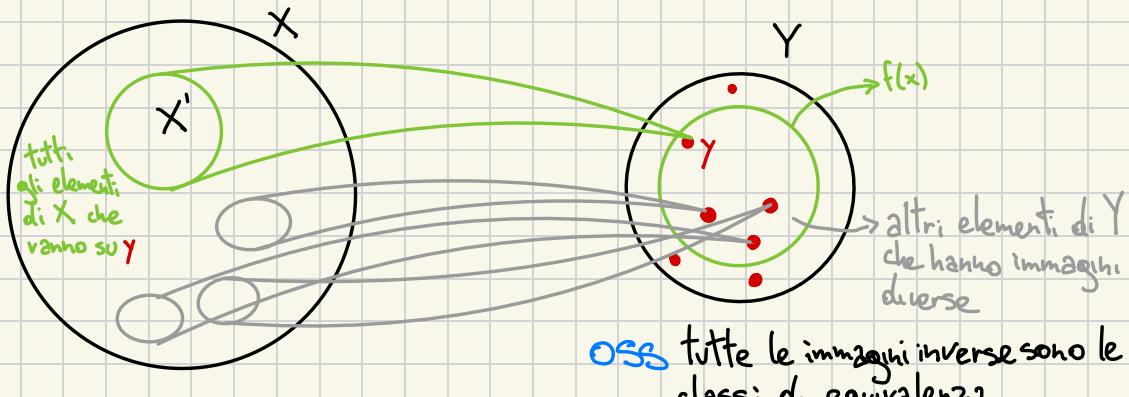
transitiva

consideriamo l'insieme quoziente  $X/\sim$

Allora  $x' \in X/\sim \Leftrightarrow x' \in X$  e  $\exists y \in Y, x' = f^{-1}(\{y\})$

L se sono nella stessa classe di equivalenza hanno la stessa immagine

$$x, x' \in X, x \sim x' \Leftrightarrow f(x) = f(x')$$



OSS tutte le immagini inverse sono le classi di equivalenza  $X' \subset X$  e

1)  $\forall x \in X, \exists x' \in X' \text{ t.c. } x \in X' \rightarrow$  ogni elemento ha la propria classe di equivalenza

2)  $X'_1, X'_2 \in X'$  e  $X'_1 \neq X'_2 \rightarrow X'_1 \cap X'_2 = \emptyset \rightarrow$  due cl. eq. distinte non hanno elementi in comune

3) se  $X' \in X'$  allora  $f|_{X'}$  è costante, ovvero la sua immagine è un singleton  
 (restringimento del dominio della funzione su  $X'$ )

si costruisca a partire da  $X \xrightarrow{f} Y$  una funzione  $\phi: X' \rightarrow f(X) \subset Y$

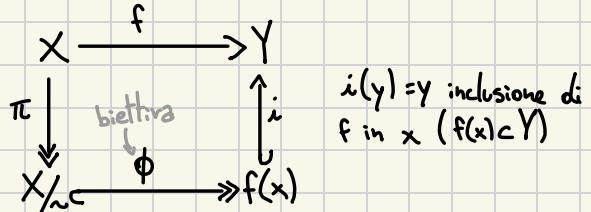
si  $X' \in X'$ , allora  $X' = [x] \exists x \in X$

si pone  $y = f(x) \in Y$ , allora definiamo  $\phi(X') = y$

L'applicazione  $\phi$  è ben definita (l'immagine di una classe non dipende dalla scelta di un rappresentante se  $c = [x] = [x'] \Rightarrow f(x) = f(x')$ ), è biettiva, e permette di calcolare  $f$  fattorizzandola come diagramma seguente

$$f = i \circ \phi \circ \pi$$

fattorizzazione di  $f$



Per vedere che  $\phi$  è biettiva, basta porre per  $y \in f(x)$ ,  $\psi(y) = \{x \in X : f(x) = y\}$   
tele insieme è  $\neq \emptyset$   
 $f$  è suriettiva su  $Y$  (la sua immagine) dunque  
 $\psi(y) = [x]$  con  $f(x) = y$  in modo che  $\psi = \phi^{-1}$

↳ funzione inversa  
 $f(x) \xrightarrow{\psi} X$

## Esercizi

02/10

Esercizio 20. Definizione costruttiva di  $\mathbb{Q}$  a partire da  $\mathbb{Z}$   
Definiamo in  $\mathbb{Z} \times \mathbb{N}^*$  (dove  $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ ) la relazione

$$(m, n) \sim (m', n') \Leftrightarrow mn' = nm'.$$

(a) Verificare che  $\sim$  è una relazione d'equivalenza.

poniamo  $X = \mathbb{Z} \times \mathbb{N}^* = \{(n, d) : \frac{n}{d} \in \mathbb{Z}\}$

$\sim$  è definita come  $(n, d) \sim (n', d') \Leftrightarrow nd' = n'd$

riflessiva  $\rightarrow (n, d) \sim (n, d)$  infatti  $nd = nd$

simmetrica  $\rightarrow (n, d) \sim (n', d') \Leftrightarrow (n', d') \sim (n, d)$  infatti  $nd' = n'd \Leftrightarrow n'd = nd'$

In questo modo ovvio, questa relazione è riflessiva e simmetrica

transitività  $(n, d) \sim (n', d') \Leftrightarrow nd' = n'd$

$$(n', d') \sim (n'', d'') \Leftrightarrow \frac{n'}{d'} = \frac{n''}{d''} \Leftrightarrow n'd'' = n''d'$$

possiamo supporre  $n' \neq 0$  ( $\Leftrightarrow n, n'' \neq 0$ )

moltiplicando termine a termine le due uguaglianze troviamo

$$nd' \cdot n''d'' = n'd \cdot n''d' \Rightarrow nd'' = nd'' \Leftrightarrow (n, d) \sim (n'', d'')$$

notazione poniamo  $\frac{n}{d}$  la classe di equivalenza della coppia  $(n, d)$

$$\frac{n}{d} := [(n, d)]$$

la classe  $r = \frac{x}{y}$  (rappresentante di  $(x, y)$ ) è  $\{(x', y') \in \mathbb{Z} \times \mathbb{N}^* : xy' = x'y\}$

tal insieme è il grafo di  $\sim$

poniamo  $\mathbb{Q} = \frac{\mathbb{Z} \times \mathbb{N}^*}{\sim}$  l'insieme dei numeri razionali

È conseguenza del teorema fondamentale dell'aritmetica ovvero, che ogni intero positivo si scrive in modo unico come prodotto di minimi termini

Il fatto che ogni classe contenga un unico elemento della forma  $(x, y)$  con  $x$  e  $y$  primi tra loro

OSS  $\frac{10}{5} = \frac{2 \cdot 5}{5} = \frac{2}{1} = 2$  abbiamo più scritture della stessa frazione in quanto quelli che leggiamo sono solo dei rappresentanti della classe di equivalenza

L'insieme  $\left\{ \frac{n}{d} \in \mathbb{Q} : n, d \text{ primi tra loro} \right\}$  è un SCR per  $\mathbb{Q}$

mostriamo che esiste un'operazione di addizione + su  $\mathbb{Q}$

consideriamo  $r = \frac{n}{d}, r' = \frac{n'}{d'} \in \mathbb{Q}$

poniamo  $r + r' := \frac{nd' + n'd}{dd'} \in \mathbb{Q}$

ma mi chiedo, è ben definita? non deve dipendere dalla scelta dei rappresentanti.

Mostriamo che l'addizione di  $\mathbb{Q} = \frac{\mathbb{Z} \times \mathbb{N}^*}{\sim}$  è ben definita

Se  $r = \frac{x}{y}$  allora  $r = [(x, y)]$

Allora

$$r = [(x, y)] = [(z, t)] \xleftrightarrow{\text{1}} xt = yz$$

$$r' = [(x', y')] = [(z', t')] \xleftrightarrow{\text{2}} x't' = y'z'$$

$$\Rightarrow \frac{x}{y} + \frac{x'}{y'} = \frac{xy' + x'y}{yy'} \text{ sotto forma di } [ ]$$

$$r + r' = [(x, y)] + [(x', y')] := \underset{\sim}{[(xy' + x'y, yy')]} := \underset{\sim}{[(x, y) + (x', y')]} := \underset{\sim}{[(x + x', y + y')]} := \underset{\sim}{[(x + x', y + y', 1)]}$$

$$r + r' = [(z, t)] + [(z', t')] := \underset{\sim}{[(zt' + z't, tt')]} := \underset{\sim}{[(z, t) + (z', t')]} := \underset{\sim}{[(z + z', t + t', 1)]}$$

per mostrare che le due operazioni sono uguali le devo mettere in relazione

utilizzo la definizione di  $\sim$

si ha che  $[(x'y' + x'y, yy')] = [(zt' + z't, tt')] \leftrightarrow (xy' + x'y)tt' = (zt' + z't)yy'$

calcoliamo

$\hookrightarrow$  se sono uguali (stanno nella stessa classe d'equivalenza) vuol dire che sono in relazione

$$(xy' + x'y)tt' \stackrel{?}{=} (zt' + z't)yy'$$

$$xy' \underset{||}{tt'} + x'y \underset{||}{tt'} = zt' \underset{||}{yy'} + z't \underset{||}{yy'}$$

$$\boxed{x} \underset{||}{t} y \underset{||}{t} + \boxed{x} \underset{||}{t} y \underset{||}{t}$$

$$\boxed{y} \underset{||}{z} y \underset{||}{t} + \boxed{y} \underset{||}{z} y \underset{||}{t} = zt' \underset{||}{yy'} + z't \underset{||}{yy'}$$

$$yzy't' + y'zy't = yzy't' + y'zy't \text{ VERO}$$

quindi  $[(xy' + x'y, yy')] = [(zt' + z't, tt')]$

Se  $r = \frac{n}{d}$  e  $r' = \frac{n'}{d'} \in \mathbb{Q}$

$r \cdot r' := \frac{nn'}{dd'}$  è ben definito?

$$r = [(x, y)] = [(z, t)] \xleftrightarrow{\textcircled{1}} xt = yz$$

$$r' = [(x', y')] = [(z', t')] \xleftrightarrow{\textcircled{2}} x't' = y'z'$$

$$r \cdot r' = [(x, y)] \cdot [(x', y')] := \overset{\textcircled{1}}{[(xx', yy')]} \quad \text{~}\sim$$

$$r \cdot r' = [(z, t)] \cdot [(z', t')] := \overset{\textcircled{2}}{[(zz', tt')]} \quad \text{~}\sim$$

applico quindi la definizione di  $\sim$

$$[(xx', yy')] = [(zz', tt')] \leftrightarrow xx'tt' = yy'zz'$$

$$x \cdot x' + t' = yy'zz'$$

||

$$\boxed{x} \cdot \boxed{x'} + t'$$

① ②

$$yz \cdot y'z'$$

||

$$yy'zz' = yy'zz' \text{ VERO}$$

Tornando indietro

es

$$X = \mathbb{Z}, b \in \mathbb{N}^* \quad Y = \{0, \dots, b-1\}$$

algoritmo della divisione euclidea per b

$$\forall x \in \mathbb{Z} \quad \exists! (q, r) \in \underbrace{\mathbb{Z}}_x \times \underbrace{\{0, \dots, b-1\}}_{Y=r} \text{ tale che}$$

$$x = qb + r$$

↳ resto  
↳ quoziente

**oss**  $y \in \mathbb{Z}$  e che  $f|_Y = id_Y$

definiamo  $f: X \longrightarrow Y$  ponendo  $f(x) := r$

questa funzione è chiamata **riduzione di modulo b** (funzione che mi restituisce il resto di una divisione tra numeri interi) ed è un'applicazione suriettiva  $f(x) = Y$

↳ qualsiasi divisione del tipo  $\frac{x}{b}$  ha un resto  $0 \leq r \leq b-1$

Allora la relazione d'equivalenza associata, notiamola  $\equiv$ , si chiama **congruenza modulo b**

↳ due numeri sono in relazione se, quando divisi per b hanno lo stesso resto

se due interi  $x, x'$  sono in relazione si scrive  $x \equiv x' \pmod{b}$  e si legge "x congruenza x' modulo b"

$$X' \in \frac{X}{\equiv} \leftrightarrow \exists r \in Y, \forall x \in X', x = qb + r$$

L'insieme  $Y \subset \mathbb{Z}$  è in questo caso un SCR infatti:

①  $f$  è suriettiva e quindi  $\forall r \in Y \ \exists x \in X$  t.c.  $x \equiv r \pmod{b}$  ②

$$\hookrightarrow X = \mathbb{Z} \quad b = 5 \quad Y = \{0, 1, 2, 3, 4\}$$

$$0 \equiv 0 \rightarrow 0 = 5 \cdot 0 + 0$$

$$2 \equiv 2 \rightarrow 2 = 5 \cdot 0 + 2$$

$$4 \equiv 4 \rightarrow 4 = 5 \cdot 0 + 4$$

$$1 \equiv 1 \rightarrow 1 = 5 \cdot 0 + 1$$

$$3 \equiv 3 \rightarrow 3 = 5 \cdot 0 + 3$$

$$9 \equiv 4 \rightarrow 9 = 5 \cdot 1 + 4$$

②  $r \neq r'$  con  $r, r' \in Y$ ,  $r \not\equiv r' \pmod{b}$ . Infatti, supponiamo per assurdo che  $r \equiv r' \pmod{b}$ ,

$$\begin{cases} r = qb + \tilde{r} \\ r' = q'b + \tilde{r}' \end{cases} \text{ quindi } r - r' = (q - q')b \Rightarrow r - r' = bK \quad (K \in \mathbb{Z} - \{0\})$$

con  $K > 0$   $r = r' + bK \geq r' + b$  ma  $r \geq r' + b \geq b$  contraddizione  $r$  deve essere strettamente  $<$  di  $b$

$\phi$  è la biezione tra  $\frac{X}{\equiv}$  e  $Y$  che manda ogni classe  $X'$  nell'unico  $r \in Y$  t.c.  $\forall x \in X', f(x) = r$  ①

In pratica,  $r$  è il resto della divisione euclidea di  $x$  per  $b$ , e non cambia al variare di  $x$  in  $X'$

$\forall X' \in \frac{X}{\equiv}$  si scrive  $X' = [x] = [x'] = [r] \quad (\forall x, x' \in X')$   
 e se  $\phi(X') = r \in Y = f(X) (= f(Y))$

## Esercizio

Esercizio 14. Data la funzione  $f : \mathbb{N} \rightarrow \mathbb{Z}$  definita da:

$$f(n) = \begin{cases} 3n & \text{se } n \text{ è pari} \\ n - 1 & \text{se } n \text{ è dispari} \end{cases}$$

determinare  $f^{-1}(0)$ ,  $f^{-1}(1)$  e  $f(\mathbb{N})$ .

$$f^{-1}(0) = f^{-1}(\{0\}) = \{n \in \mathbb{N} \text{ t.c. } f(n) = 0\}$$

Si ha  $0$  pari e  $3 \cdot 0 = 0$  quindi  $f(0) = 0$  e  $0 \in f^{-1}(\{0\})$

Inoltre 1 è dispari e  $f(1) = n - 1 = 0$   
quindi  $\{0, 1\} \subset f^{-1}(\{0\})$   $\hookrightarrow$  con  $n=1$

controllo quindi se ci sono altri elementi

sia adesso  $n \in f^{-1}(\{0\})$ , quindi  $f(n) = 0$

1) se  $n$  è pari,  $f(n) = 3n = 0 \Rightarrow n = 0$

2) se  $n$  è dispari,  $f(n) = n - 1 = 0 \Rightarrow n = 1$

ne deduciamo  $f^{-1}(\{0\}) = \{0, 1\}$

sia  $n \in f^{-1}(1)$

1) se  $n$  è dispari  $f(n) = n - 1 = 1 \Rightarrow n = 2 \rightarrow$  impossibile (è pari)

2) se  $n$  è pari  $f(n) = 3n = 1 \Rightarrow$  impossibile (definito su  $\mathbb{N}$ )

quindi  $f^{-1}(1) = \emptyset$

$f(\mathbb{N}) = \{y \in \mathbb{Z} \text{ t.c. } \exists x \in \mathbb{N} \text{ con } f(x) = y\}$

$f(\mathbb{N}) = f(\underbrace{\{ \text{numeri pari} \}}_{2\mathbb{N}}) \cup f(\underbrace{\{ \text{numeri dispari} \}}_{2\mathbb{N}+1}) =$

$$= 3(2\mathbb{N}) \cup (2\mathbb{N}+1) - 1 = 6\mathbb{N} \cup 2\mathbb{N}$$

ma  $6\mathbb{N} \subset 2\mathbb{N}$  quindi  $f(\mathbb{N}) = 2\mathbb{N}$

variante funzione di Lothar Collatz

definiamo  $f: \mathbb{N}^* \rightarrow \mathbb{N}^*$   $f(n) = \begin{cases} 3n+1 & \text{se } n \text{ è dispari} \\ \frac{n}{2} & \text{se } n \text{ è pari} \end{cases}$

calcolare  $f^{-1}(1), f^{-1}(2), f^{-1}(4)$

$f(n) = 1$  se  $n$  dispari  $f(n) = 3n+1 > 1$  quindi  $n$  non può essere dispari  
 se  $n$  pari  $f(n) = \frac{n}{2} = 1 \Leftrightarrow n = 2$   
 quindi  $f^{-1}(1) = \{2\}$

$f(n) = 2$  se  $n$  dispari  $f(n) = 3n+1 > 2$  quindi  $n$  non può essere dispari  
 se  $n$  pari  $f(n) = \frac{n}{2} = 2 \Leftrightarrow n = 4$   
 quindi  $f^{-1}(2) = \{4\}$

$f(n) = 4$  se  $n$  dispari  $f(n) = 3n+1 = 4 \Leftrightarrow n = 1$   
 se  $n$  pari  $f(n) = \frac{n}{2} = 4 \Leftrightarrow n = 8$   
 quindi  $f^{-1}(4) = \{1, 8\}$

Calcoliamo  $f^{-1}(\{1, 8\}) = f^{-1}(1) \cup f^{-1}(8) = \{2\} \cup f^{-1}(8)$

$n$  dispari  $f(n) = 3n+1 = 8 \rightarrow 3n = 7$  impossibile

$n$  pari  $f(n) = \frac{n}{2} = 8 \rightarrow n = 16$

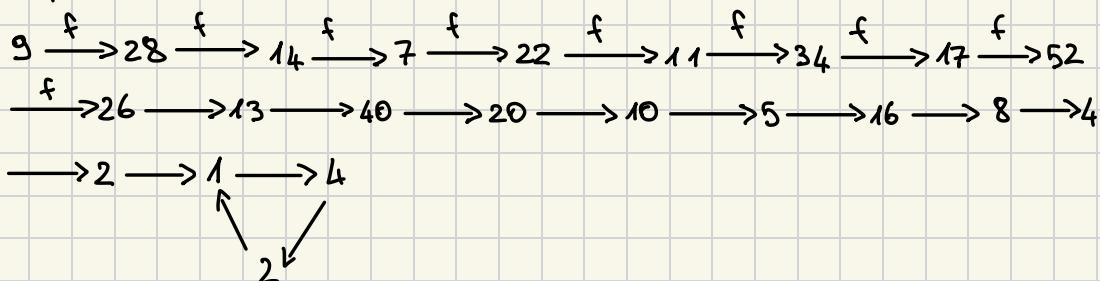
quindi  $f^{-1}(\{1, 8\}) = \{2, 16\}$  continuiamo

$f^{-1}(\{2, 16\}) = \{4\} \cup f^{-1}(16) = \{4, 5, 22\}$

$f^{-1}(\{4, 5, 22\}) = \{1, 8, 10, 64\}$

congettura (Collatz)  $\forall n \in \mathbb{N}^*$  esiste  $m$  t.c.  $n \in \underbrace{f^{-1}(f^{-1}(\dots f^{-1}(1) \dots))}_{m \text{ volte}}$

essendo una congettura non è stata ancora riuscita a dimostrarne, ad ora è la congettura della dinamica (cose iterabili) più complessa



questo vuol dire che  $9 \in \underbrace{f^{-1}(\dots f^{-1}(1) \dots)}_{19 \text{ volte}}$

## Esercizio

03/10

- Esercizio 3. Studiare l'applicazione  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  che ad  $x \in \mathbb{Z}$  associa  $f(x) = ax + 1$ , al variare del parametro  $a \in \mathbb{Z}$ . Dire quando essa è suriettiva, iniettiva.

Se  $a=0$   $\forall x \in \mathbb{Z}, f(x)=1 \rightarrow$  non è né iniettiva né suriettiva

Se  $a=1$   $f(x)=x+1$  quindi  $f$  ha inversa  $g(y)=y-1$  ed è quindi biiettiva  
infatti:  $(f \circ g)(y) = f(y-1) = (y-1)+1 = y \Rightarrow f \circ g = \text{Id}_{\mathbb{Z}}$

$(g \circ f)(x) = (x+1)-1 = x \Rightarrow x=x \Rightarrow g \circ f = \text{Id}_{\mathbb{Z}} \Rightarrow f$  biiettiva

Lo stesso si può dire per  $a=-1$  (con lo stesso metodo  $f$  è biiettiva)

Se  $a \neq 0$  allora  $f$  è iniettiva:

$$\begin{aligned} f(n_1) = f(n_2) &\Leftrightarrow an_1 + 1 = an_2 + 1 \Leftrightarrow an_1 - an_2 = 0 \Leftrightarrow a(n_1 - n_2) = 0 \\ &\Leftrightarrow n_1 - n_2 = 0 \Leftrightarrow n_1 = n_2 \end{aligned}$$

Quindi se  $a \neq 0$  si ha che  $f$  è iniettiva

Se  $a \notin \{1, 0, -1\}$   $f$  non è suriettiva

Infatti:  $f^{-1}(\{a\}) = \emptyset$ . Se  $f$  fosse suriettiva avremmo  $\exists x \in \mathbb{Z}$  t.c.  $f(x) = a$   
ma allora

$$f(x) = ax + 1 = a \rightarrow a(x-1) = -1 \rightarrow a(1-x) = 1$$

ma in  $\mathbb{Z}^2$  ci sono soltanto due coppie di interi  $(x, y)$  con  $xy = 1$ :  $(1, 1)$  e  $(-1, -1)$

Oss si riformula scrivendo " $\mathbb{Z}^X = \{1, -1\}$ "

In particolare questo implica  $a \in \{1, -1\}$ , ipotesi che abbiano escluso

preparazione all'esercizio 21



sia  $\mathcal{P} = \{X_1, X_2\}$  una partizione di  $X (\neq \emptyset)$

sia  $\mathcal{Q} = \{Y_1, Y_2, Y_3\}$  una partizione di  $Y$  ( $\neq \emptyset$ )

quindi  $X$  ha almeno 2 elementi e  $Y$  ha almeno 3 elementi.

Mostrare che  $\mathcal{R} = \{X_i \times Y_j : i=1,2, j=1,2,3\}$  è una partizione di  $X \times Y$

partizione di  $X$  insieme di sottoinsiemi  $\neq \emptyset$

$$\{X_i : i \in I\} \subset \mathcal{P} \text{ t.c. } ① X = \bigcup_{i \in I} X_i$$

insieme degli indici, nel nostro caso  $I = \{1, 2\}$

$$② \forall i \neq j \quad X_i \cap X_j = \emptyset$$

rappresentazione grafica di  $\mathcal{R}$

$\hookrightarrow$  ① e ② si sintetizzano

$$\text{con } X = \bigcup_{i \in I} X_i$$

nel nostro caso

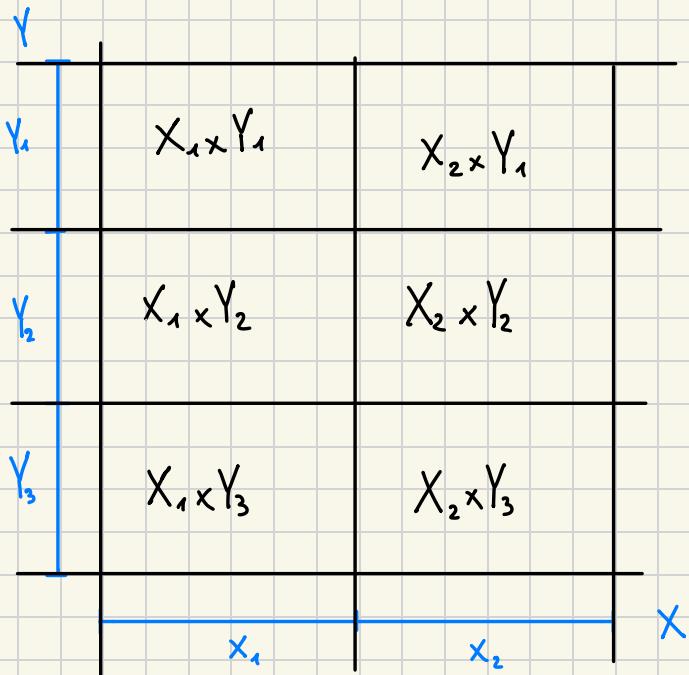
$$X = \bigcup_{i \in \{1, 2\}} X_i$$

$$Y = \bigcup_{i \in \{1, 2, 3\}} Y_i$$

$$\text{con } \{X_1, X_2, Y_1, Y_2, Y_3\} \cap \emptyset = \emptyset$$

$$\text{poniamo } I = \{1, 2\}$$

$$J = \{1, 2, 3\}$$



Allora  $\mathcal{R}' = \{X' \times Y' : X' \in \mathcal{R}, Y' \in \mathcal{Q}\} =$

$$= \{X_1 \times Y_1, X_2 \times Y_1, X_1 \times Y_2, X_2 \times Y_2, X_1 \times Y_3, X_2 \times Y_3\}$$

Dimostra che  $\mathcal{Q}$  è una partizione di  $X \times Y$

①  $\forall (i, j) \in I \times J \quad X_i \times Y_j \neq \emptyset$

②  $\forall (x, y) \in X \times Y \quad \exists (i, j) \text{ t.c. } (x, y) \in X_i \times Y_j$

③ se  $(i, j) \neq (i', j')$  allora  $X_i \times Y_j \cap X_{i'} \times Y_{j'} = \emptyset$

① siccome  $X_i \neq \emptyset$  ( $\mathcal{Q}$  è una partizione)  $\exists x \in X_i$   
in modo analogo  $Y_j \neq \emptyset$  ed  $\exists y \in Y_j$

Quindi  $(x, y) \in X_i \times Y_j \Rightarrow X_i \times Y_j \neq \emptyset$

② dati  $(x, y) \in X \times Y$ ,  $\mathcal{Q}$  partizione  $\Rightarrow \exists i \in I$  t.c.  $x \in X_i$   
 $\mathcal{Q}$  partizione  $\Rightarrow \exists j \in J$  t.c.  $y \in Y_j$

$(x, y) \in X_i \times Y_j$

③ ma  $(i, j) \neq (i', j') \Leftrightarrow i \neq i' \vee j \neq j'$

se  $i = i'$  allora  $X_i \cap X_{i'} = \emptyset$  ( $\mathcal{Q}$  partizione)

calcoliamo allora  $(X_i \times Y_j) \cap (X_{i'} \times Y_{j'}) = \{(x, y) : \begin{array}{l} x \in X_i \cap X_{i'} \\ y \in Y_j \cap Y_{j'} \end{array}\} = \emptyset$

se invece si ha  $j \neq j'$  allora  $Y_j \cap Y_{j'} = \emptyset$  questo implica, per lo stesso ragionamento  $(X_i \times Y_j) \cap (X_{i'} \times Y_{j'}) = \emptyset$

Esercizio 21. Mostrare che se  $\{X_i : i \in I\}$  è una partizione di un insieme  $X$  e  $\{Y_j : j \in J\}$  è una partizione di un insieme  $Y$ , allora  $\{X_i \times Y_j : (i, j) \in I \times J\}$  è una partizione di  $X \times Y$ .

Siano date due partizioni  $\{X_i : i \in I\}$  e  $\{Y_j : j \in J\}$

**oss** l'insieme quoziente di una relazione d'equivalenza su un insieme è una partizione

$\forall (i, j) \in I \times J$  si ha  $X_i \times Y_j \in X \times Y$  e chiaramente  $X_i \times Y_j \neq \emptyset$  dato che  $X_i \neq \emptyset$  e  $Y_j \neq \emptyset$

Inoltre sia  $m = (x, y) \in X \times Y$

$\exists i \in I$  t.c.  $x \in X_i$  ( $\{X_i : i \in I\}$  è una partizione).

In modo simile,  $\exists j \in J$  t.c.  $y \in Y_j$

Quindi  $(x, y) \in X_i \times Y_j$

Da qui ne segue che  $X \times Y \subset \bigcup_{(i,j) \in I \times J} X_i \times Y_j$

siccome  $\forall (i, j)$   $X_i \times Y_j \subset X \times Y$ , si ottiene  $X \times Y = \bigcup_{(i,j)} X_i \times Y_j$

Inoltre siano  $(i, j), (i', j') \in I \times J$  distinti

Allora si ha  $i \neq i'$  oppure  $j \neq j'$ .

Calcoliamo  $(X_i \times Y_j) \cap (X_{i'} \times Y_{j'})$  nel caso  $i \neq i'$

$(X_i \times Y_j) \cap (X_{i'}, Y_{j'}) = \{(x, y) \in X \times Y \text{ t.c. } x \in X_i \cap X_{i'} \text{ e } y \in Y_j \cap Y_{j'}\}$   
ma  $i \neq i' \rightarrow X_i \cap X_{i'} = \emptyset$

Da cui  $(X_i \times Y_j) \cap (X_{i'} \times Y_{j'}) = \emptyset$

si tratta il caso  $j \neq j'$  in modo analogo

### Esercizio (pigeon hole principle)

Esercizio 12. Sia  $f : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$  un'applicazione. Si provi che se  $n > m$  allora  $f$  non è iniettiva, se  $n < m$  allora  $f$  non è suriettiva.

① mostriamo che se  $n > m \geq 1$  allora  $f : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$  non è iniettiva  
 $\forall f$  applicazione

Per semplificare scriviamo  $E_n := \{1, \dots, n\}$

Arremo bisogno delle seguenti proprietà

1)  $E_n = E_{n-1} \sqcup \{n\}$

2)  $\forall m_0 \in E_{m_0}, \exists E_m \setminus \{m_0\} \xrightarrow[\cong]{f} E_{m-1}$

3) Sia  $X \xrightarrow{h} Y$  iniettiva. Allora il grafo  $\Gamma$  di  $h$  ha la proprietà che  
 $\forall y \in Y$ , se  $\exists x \in X$  con  $(x, y) \in \Gamma$ , allora  $x$  è unico

1) chiaro

2) l'applicazione  $E_{m_0} \setminus \{m_0\} \xrightarrow{f} E_{m-1} \rightarrow \{1, 2, 4, 5\} \rightarrow \{1, 2, 3, 4\}$

$$\text{definita da } f(x) = \begin{cases} x & \text{se } x < m_0 \\ x-1 & \text{se } x \geq m_0 \end{cases}$$

$$f(1) = 1 \quad f(2) = 2$$

$$f(4) = 3 \quad f(5) = 4$$

è invertibile di inversa

$$f^{-1}(x) = \begin{cases} y & \text{se } y < m_0 \\ y+1 & \text{se } y \geq m_0 \end{cases}$$

$$\begin{aligned} f \circ f^{-1}(y) &= \begin{cases} y & \text{se } y < m_0 \\ y+1 & \text{se } y \geq m_0 \end{cases} \\ &= y = f(f^{-1}(y)) \Rightarrow y = y \end{aligned}$$

$$\begin{aligned} f^{-1} \circ f(x) &= \begin{cases} x & \text{se } x < m_0 \\ x-1 & \text{se } x \geq m_0 \end{cases} \\ &= \begin{cases} f^{-1}(f(x)) & \text{se } x < m_0 \\ f^{-1}(f(x))-1 & \text{se } x \geq m_0 \end{cases} \\ &= \begin{cases} x & \text{se } x < m_0 \\ (x-1)+1 & \text{se } x \geq m_0 \end{cases} \\ &= x = x \end{aligned}$$

3) chiaro:  $h$  iniettiva  $\Leftrightarrow \forall y \in Y \ h^{-1}(y) = \emptyset$  oppure singleton

Si ha  $\exists x \in X$  t.c.  $h(x) = y \Leftrightarrow h^{-1}(y) \neq \emptyset$

In tal caso  $(x, y) \in \Gamma \Leftrightarrow f(x) = y \Leftrightarrow \{x\} = f^{-1}(y)$

Se  $m=1$  non c'è nulla da dimostrare

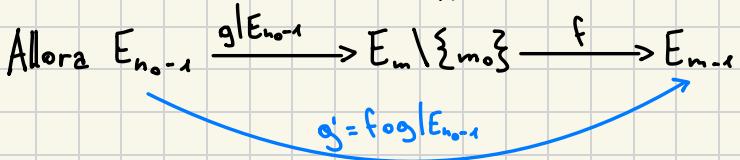
Supponiamo per assurdo che l'affermazione sia falsa

Allora  $\exists n_0, m$  con  $n_0 > m > 1$  e  $g: E_{n_0} \rightarrow E_m$  iniettiva

Poniamo  $m_0 := g(n_0)$

2)  $\Rightarrow \exists E_m \setminus \{m_0\} \xrightarrow[\cong]{f} E_{m-1}$

ma  $n_0 - 1 > m - 1$  possiamo supporre  $m - 1 \geq 1$



$g$  non è iniettiva (per minimalità di  $n_0$ )

↳ se non è valido per il valore minimo di  $n_0$ , ovvero  $n_0 = m + 1$  allora non è più valido quindi sostituendo si ha  $g: m \rightarrow m - 1$

3)  $\Rightarrow$  sia  $\Gamma'$ : il grafo di  $g$

$$\exists y \in Y = E_{m - 1} \text{ e } x_1, x_2 \in X = E_{n_0 - 1} \quad x_1 \neq x_2 \quad \text{t.c. } (x_1, y), (x_2, y) \in \Gamma'$$

questo implica che  $g|_{E_{n_0 - 1}}$  non è iniettiva ( $f$  è necessariamente biettiva come dimostrato)

Infatti  $(x_1, f^{-1}(y)), (x_2, f^{-1}(y))$  appartengono al suo grafo  $\tilde{\Gamma}$

Ma il grafo  $\Gamma$  di  $g$  è dato da  $\tilde{\Gamma} \sqcup \{(n_0, m_0)\}$  che contiene sempre i due elementi per cui  $g$  non è iniettiva. Contraddizione

2) si può procedere in modo analogo. Altrimenti, si può fare un'induzione su  $n$  (equivolentemente)

$$f: \{1, \dots, n\} \longrightarrow \{1, \dots, m\} \text{ con } m_0 = f(n) \text{ si ha}$$

$$\{1, \dots, n-1\} \xrightarrow{f|_{\{1, \dots, n-1\}}} \{1, \dots, m\} \setminus \{m_0\} \xrightarrow{g} \{1, \dots, m-1\}$$

per ipotesi induttiva  $g \circ f|_{\{1, \dots, n-1\}}$  non è suriettiva

Quindi  $f|_{\{1, \dots, n\}}$  non è suriettiva, e quindi neanche  $f$  lo è

L'insieme  $\mathbb{Z}$  è munito di operazione "opposto"

08/10

opposto

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ a & \longmapsto & -a \end{array}$$

e di due operazioni binarie

somma

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow{+} & \mathbb{Z} \\ (a,b) & \longmapsto & a+b \end{array}$$

prodotto

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow{\cdot} & \mathbb{Z} \\ (a,b) & \longmapsto & a \cdot b = \begin{cases} \text{se } b=0 \Rightarrow 0 \text{ } b \text{ volte} \\ \text{se } b>0 \Rightarrow \underbrace{a+a+\dots+a}_{b \text{ volte}} \\ \text{se } b<0 \Rightarrow (-a)+(-a)\dots+(-a) \end{cases} \end{array}$$

L'operazione di "opposto" associa ad ogni  $a \in \mathbb{Z}$  l'unico elemento  
e.t.c.  $a + (-a) = 0$

Ci sono diverse condizioni di compatibilità, tra queste:

$$a(b+c) = ab+ac$$

$$a+b = b+a$$

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

$$(ab)c = a(bc)$$

formalizziamo

**DEF ANELLO** (commutativo unitario)

Un anello è il dato di una sestupla  $(A, +, -, \cdot, 0_A, 1_A)$

dove

$$A = \text{insieme} \neq \emptyset$$

↑. Il tutto forma A

$+: A \times A \longrightarrow A$  (addizione, mult. plazione)

$-: A \longrightarrow A$  (oppuesto)

$0_A$  elemento neutro per addizione  $0_A \in A$

$1_A$  elemento neutro per moltiplicazione  $1_A \in A$

Questi dati devono soddisfare le condizioni seguenti.

- ①  $\forall a, b \in A, a+b = b+a$  + è commutativa
- ②  $\forall a, b, c \in A (a+b)+c = a+(b+c)$  + è associativa
- ③  $\forall a \in A a+0_A = 0_A + a = a$
- ④  $\forall a \in A a+(-a) = 0_A$

queste proprietà stanno ad indicare che  $(A, +, -, 0_A)$  è un gruppo abeliano in notazione additiva (sarà descritto ulteriormente)

- ⑤  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  • è associativa
- ⑥  $a \cdot (b+c) = a \cdot b + a \cdot c$  • è distributiva
- ⑦  $a \cdot 1_A = 1_A \cdot a = a$   
↳ l'elemento neutro per la moltiplicazione  
rende l'anello "unitario"
- ⑧  $a \cdot b = b \cdot a$  • è commutativa

es)

$\mathbb{Z} = (\mathbb{Z}, +, -, \cdot, 0, 1)$  è un anello commutativo unitario

$\mathbb{N}$  non è un anello dato che non c'è l'oppuesto

L'anello  $A = \mathbb{Z}$  ha proprietà più specifiche: buon ordinamento e ordine totale

esiste un sottoinsieme  $\mathbb{N}^* \subset \mathbb{Z}$  che permette di definire una relazione su  $\mathbb{Z}$

si scrive  $a > b \iff a - b \in \mathbb{N}^*$

↳ relazione ordine totale?

proprietà di tricotomia ordine totale?

$\forall a \in \mathbb{Z}$  si ha che:  
o  $a = 0$   
o  $-a \in \mathbb{N}^*$   $\rightarrow a$  è positivo,  $a > 0$

o  $-a \notin \mathbb{N}^*$   $\rightarrow a$  è negativo,  $a < 0$

Ogni sottoinsieme  $E \subset \mathbb{N}^*$  non vuoto possiede un più piccolo elemento per  $\exists c \in E$  t.c.  $\forall e \in E \setminus \{c\}$  si ha che  $e > c$  buon ordinamento

Un anello commutativo e unitario che soddisfa le proprietà di tricotomia e la proprietà del buon ordinamento è "essenzialmente"  $\mathbb{Z}$

Se  $a < b$   $c < d$  allora  $a+c < b+d$  e  $-a > -b$

$\hookrightarrow$  l'operazione + e < sono compatibili

In modo simile  $ac < bd$

$\hookrightarrow$  l'operazione  $\cdot$  e < sono compatibili

### Legge di cancellazione in $\mathbb{Z}$

hp  $ab = ac$  con  $a \neq 0$

th  $b = c$

dim

si può supporne  $a > 0$ . Induzione su  $a \geq 1$

$a=1$  chiaro

$(a-1)b = (a-1)c$  supponiamo che  $b \neq c$   $b > c \Rightarrow (a-1)b + b > (a-1)c + c \Rightarrow$   
 $\Rightarrow b(a-1+1) > c(a-1+1) \Rightarrow$   
 $\Rightarrow ab > ac$   
contraddizione

### Elementi invertibili A anello $1_A \neq 0_A$

DEF

$a \in A$  t.c.  $\exists b \in A$   $ab = ba = 1_A$  è detto elemento invertibile  
(si dice che  $b$  è inverso di  $a$  e si scrive  $b = a^{-1}$ )

**es**

$1_A$  è invertibile d. inverso  $1_A^{-1} = 1_A$

si pone  $A^X = \{a \in A \text{ t.c. } a \text{ è invertibile}\}$

**teorema**

se  $a$  è invertibile  $a^{-1}$  è unicamente determinato

dim

$$a \cdot b = a \cdot b' = 1 \text{ con } b, b' \in A \quad (a \cdot b)b' = a \cdot (b \cdot b') = a(b' \cdot b) = (ab')b$$

$$\text{allora } (ab)b' = 1_A b' = b'$$

$$(ab')b = 1_A b = b$$

quindi  $b = b'$  è l'inverso  $a^{-1}$  di  $a$  è ben definito

**teorema**

①  $A^X$  è non vuoto

② se  $a \in A^X$  allora  $a^{-1} \in A^X$

③ se  $a, b \in A^X$  allora  $ab \in A^X \Rightarrow (ab)^{-1} = a^{-1} \cdot b^{-1}$

④  $\mathbb{Z}^X = \{1, -1\}$

①  $1_A \in A \quad 1_A \cdot 1_A = 1_A \Rightarrow 1_A \in A^X$

②  $a^{-1} \cdot b = b \cdot a^{-1} = 1_A$

possiamo vedere che  $b$  è proprio  $a$  infatti:  $a^{-1} \cdot a = a \cdot a^{-1} = 1_A$

③  $a \cdot a^{-1} = a^{-1} \cdot a = 1_A \quad b \cdot b^{-1} = b^{-1} \cdot b = 1_A$

$$ab \cdot (a^{-1} \cdot b^{-1}) = aa^{-1} \cdot bb^{-1} = a \cdot 1_A = 1_A \cdot b = 1_A$$

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

$$\text{dunque } (a^{-1} \cdot b^{-1}) = (ab)^{-1}$$

④ sia  $a \in \mathbb{Z}^X$  mostriamo che  $a \in \{1, -1\}$

sia quindi  $a \in \mathbb{Z}^X$  con  $a > 0$

$\exists b \in \mathbb{Z}$  t.c.  $ab=1$ . Ne deduco che  $b>0$  (altrimenti  $b \leq 0$ )  
ma  $ab = \underbrace{b + \dots + b}_{a \text{ volte}} = 1$

siccome  $b$  è positivo  $1 \geq b > 0 \Rightarrow b=1$   
quindi  $a=a \cdot 1=1$

### Esercizio

$(\mathbb{Q}, +, -, \cdot, 0, 1)$  è un anello calcolare  $\mathbb{Q}^{\times}$

dati:  $q, r \in \mathbb{Q}$   $q \neq r$  per essere invertibili  $qr=1$

$$q = \frac{a}{b} \quad e \quad r = \frac{c}{d} \quad a, c \in \mathbb{Z} \quad b, d \in \mathbb{Z} \setminus \{0\}$$

$$\frac{a}{b} \cdot \frac{c}{d} = 1 \Rightarrow \text{ma poiché } qr=1 \text{ allora } a, c \neq 0$$

$$\text{dunque } q = \frac{a}{b} \quad e \quad q^{-1} = \frac{b}{a} \quad q q^{-1} = \frac{a}{b} \cdot \frac{b}{a} = 1 \text{ per cancellazione di } \mathbb{Z}$$

$$\mathbb{Q}^{\times} = \{r \in \mathbb{Q}, r \neq 0\}$$

"piccoli esempi"

①  $\forall a \in A, a \cdot 0_A = 0_A$

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

② supponiamo  $0_A = 1_A$  mostriamo che  $\forall a \in A$  si ha  $a = 0_A$  ( $A = \{0_A\}$ )

$$a \in A : 1_A = 0_A \Rightarrow \underbrace{a \cdot 1_A}_{=a} = a \cdot 0_A = 0_A$$

③ se  $1_A \neq 0_A$  allora  $0_A \notin A^{\times}$

supponiamo per assurdo che  $\exists x \in A^{\times}$  t.c.  $1_A = x \cdot 0_A \stackrel{?}{=} 0_A$

contraddizione  
 $1_A \neq 0_A$

**Esercizio**

C'è un unico elemento neutro (in ogni anello)

Siano  $u, u'$  due elementi neutri

$$\forall a \in A \quad au = ua = a$$

$$au' = u'a = a$$

↓

$$a = u \quad uu' = u'u = u$$

$$a = u' \quad u'u = uu' = u'$$

$$\left. \begin{array}{l} a = u \\ a = u' \end{array} \right] \longrightarrow u'u = u = u'u = u' \Rightarrow u = u'$$

**Esercizio**

Dedurre che anche l'elemento neutro dell'addizione è unicamente determinato

Siano  $u, u'$  due elementi neutri

$$\forall a \in A \quad u + a = a + u = a$$

$$u' + a = a + u' = a$$

↓

$$a = u \quad u' + u = u + u' = u$$

$$a = u' \quad u + u' = u' + u = u'$$

$$\left. \begin{array}{l} a = u \\ a = u' \end{array} \right] \longrightarrow u' + u = u = u' + u = u' \Rightarrow u = u'$$

**Relazione di divisibilità DEF**

sia  $A$  un anello e introduciamo la relazione  $a, b \in A$

$$a|b \iff \exists c \in A \text{ t.c. } b = ac$$

**es**

$$2|6 \rightarrow 6 = 2 \cdot 3$$

è una relazione riflessiva  $\forall a \in A, a = a \cdot 1_A$  e transitiva  $a, b, c \in A$

supponiamo che

$$a|b \iff b = aa' \quad \exists a' \in A$$

$$b|c \iff c = bb' \quad \exists b' \in A$$

$$\Rightarrow c = bb' = (aa')b' = a(a'b') = aa'' \iff a|c$$

ma non è una relazione né simmetrica né antisimmetrica su  $\mathbb{Z}$   
 supponiamo per assurdo  $a|b$  e  $b|a$  con  $a \neq b$  (SIMMETRIA)  
 vuol dire che

$$\begin{aligned} b &= ac \quad c \in A \quad \Rightarrow a = bc' \rightarrow a = acc' \rightarrow a = ac'' \stackrel{c''=1}{\rightarrow} c'' = 1 \quad \text{prendendo} \\ a &= bc' \quad c' \in A \quad \stackrel{c=c'=1}{\text{si ha contraddizione}} \end{aligned}$$

non è antisimmetrica infatti

$$a, b \in \mathbb{Z} \quad a|b \text{ e } b|a \Rightarrow \exists c \in \mathbb{Z}^{\times} \text{ t.c. } a = bc \text{ ovvero } a \in \{b, -b\}$$

o anche  $\{a, -a\} = \{b, -b\}$

possiamo supporre che  $a, b \neq 0$

$$a|b \text{ e } b|a \Rightarrow b = aa', a = bb' \quad \exists a', b' \in \mathbb{Z}$$

$$b = bb'a' \rightarrow 1 = a'b' \rightarrow a', b' \in \{1, -1\} \Rightarrow \{a, -a\} = \{b, -b\}$$

altre proprietà

se  $a|b$  e  $a|c$  allora  $a|b+c$  (compatibilità)

$$\begin{aligned} a|b &\Leftrightarrow \exists a' \in A \text{ t.c. } b = aa' \quad \Rightarrow b + c = aa' + ac'' = a(a' + a'') \Leftrightarrow a|b+c \\ a|c &\Leftrightarrow \exists a'' \in A \text{ t.c. } c = aa'' \end{aligned}$$

più generalmente se  $\alpha, \beta \in A$ ,  $a|b$ ,  $a|c$   $\rightarrow a|ab + \beta c$

Elementi irriducibili e primi

DEF

$a \in A \setminus A^{\times}$   $a \neq 0$  è detto **irriducibile** se  $\forall b, c \in A$ ,  $a = bc$  allora  $0 < b \in A^{\times}$  o  $c \in A^{\times}$

es  $A = \mathbb{Z}$

$12 = 4 \cdot 3$  ma  $4, 3 \notin \mathbb{Z}^{\times} \Rightarrow 12$  non è irriducibile

$7 = 1 \cdot 7 = 7 \cdot 1 \quad 1 \in \mathbb{Z}^{\times} \Rightarrow 7$  è irriducibile

$9 = 3 \cdot 3 \Rightarrow$  non è irriducibile

$1 \in \mathbb{Z} \Rightarrow$  non è irriducibile per ipotesi

### DEF

$a \in A \setminus A^{\times}$   $a \neq 0$  è **primo** se  $\forall b, c \in A$ , se  $a \mid bc$  allora  $a \mid b$  oppure  $a \mid c$

**LEMMA**  $p \in \mathbb{Z}$  primo  $\Leftrightarrow p$  è irriducibile

dim

$p$  primo, siano  $a, b \in \mathbb{Z}$  t.c.  $p \mid ab \Rightarrow p \mid ab \Rightarrow p \mid a$  o  $p \mid b$

Supponiamo che  $p \mid a \Rightarrow a = pa'$   $\exists a' \in \mathbb{Z} \Rightarrow p = p(a'b) \Rightarrow 1 = a'b \Rightarrow a, b \in \{-1, 1\}$

se  $a = 1$  allora  $a = p \Rightarrow p = pb \Rightarrow b = 1$

se  $b = 1$  allora  $a = -p \Rightarrow p(-b) \Rightarrow -b = 1 \Rightarrow b = 1 \quad \boxed{\Rightarrow p \text{ è irriducibile}}$

**Valore assoluto**  $\mathbb{Z} \xrightarrow{| \cdot |} \mathbb{Z}$

$a \in \mathbb{Z}$  se  $a = 0$   $|a| = 0$

se  $a \neq 0$  allora  $|a|$  è l'unico elemento di  $\mathbb{N}$  contenuto nell'insieme da due elementi  $\{a, -a\}$

### Algoritmo della divisione euclidea DEF

hp  $a, n \in \mathbb{Z}$   $n \neq 0$

th esistono unicamente determinati,  $q \in \mathbb{Z}$   $r \in \{0, \dots, n-1\}$  t.c.  $a = nq + r$

quoziente  
resto

legame con la congruenza

$a \equiv b \pmod{n} \Leftrightarrow n \mid a - b \Leftrightarrow \exists q \in \mathbb{Z}$  t.c.  $a - b = qn$

ovvero, il resto della divisione di  $a - b$  per  $n$  è zero

La congruenza modulo  $n$  è una relazione di equivalenza

ricordiammo perché è transitiva  $a \equiv b \pmod{n}$   $b \equiv c \pmod{n} \Leftrightarrow n \mid b - a$  e  $n \mid c - b$   
 $\Rightarrow n \mid c - b + b - a \Rightarrow n \mid c - a \Leftrightarrow c \equiv a \pmod{n}$

**es**

congruenza modulo 2

$$\mathbb{Z} = \underbrace{\mathbb{Z}}_{\substack{\bar{0} \\ \text{classe di } 0}} \sqcup \underbrace{\mathbb{Z}}_{\substack{\bar{1} \\ \text{classe di } 1}} + \mathbb{Z}$$

$$\mathbb{Z}/\equiv_{\text{mod}_2} = \{2\mathbb{Z}, 2\mathbb{Z}+1\} = \{\bar{0}, \bar{1}\}$$

congruenza modulo 3

$$\mathbb{Z}/\equiv_{\text{mod}_3} = \{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\} = \{\bar{0}, \bar{1}, \bar{2}\}$$

$\bar{0}$	$\bar{1}$	$\bar{2}$
$\frac{0}{3}$	$\frac{1}{3}$	$\frac{2}{3}$
$\frac{3}{6}$	$\frac{4}{6}$	$\frac{5}{6}$
$\frac{6}{9}$	$\frac{7}{9}$	$\frac{8}{9}$

$$\mathbb{Z}/\equiv_{\text{mod}_n} = \mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, n\mathbb{Z}+1, \dots, n\mathbb{Z}+(n-1)\}$$

$$\mathbb{Z}_3 = \{m \in \mathbb{Z} : m \equiv 2 \pmod{3}\} = \{m \in \mathbb{Z} \text{ t.c. } 3 \mid m-2\}$$

$$m=2 \quad m-2=0 \quad 3 \mid 0$$

$$m=5 \quad m-2=3 \quad 3 \mid 3$$

$$m=-1 \quad m-2=-3 \quad 3 \mid -3$$

## Operazioni compatibili con la congruenza

10/10

①  $\forall a, a' \in \mathbb{Z} \quad a \equiv a' \pmod{n} \Leftrightarrow -a \equiv -a' \pmod{n}$

dcm

$$a \equiv a' \Leftrightarrow n \mid a - a'$$

$$n \mid a - a' \Leftrightarrow \exists k \in \mathbb{Z} \text{ t.c. } a' - a = nk \Rightarrow -a + a' = kn \Leftrightarrow -a \equiv_n a' \Leftrightarrow -a' \equiv_n -a$$



②  $a, a', b, b' \in \mathbb{Z} \quad a \equiv_n a' \quad b \equiv_n b' \text{ allora } a+b \equiv_n a'+b'$

dcm

$$a \equiv a' \Leftrightarrow n \mid a - a' \quad b \equiv b' \Leftrightarrow n \mid b - b'$$

$$n \mid a - a' \Leftrightarrow \exists k \in \mathbb{Z} \text{ t.c. } a' - a = nk$$

$$n \mid b - b' \Leftrightarrow \exists k' \in \mathbb{Z} \text{ t.c. } b' - b = nk'$$

addizione termine a termine

$$a' + b' - (a + b) = n(k + k') \Rightarrow n | (a' + b') - (a + b) \Leftrightarrow a' + b' \equiv_n a + b$$



③  $a, a', b, b' \in \mathbb{Z} \quad a \equiv_n a' \quad b \equiv_n b' \rightarrow ab \equiv_n a'b'$

dcm

$$a \equiv_n a' \Leftrightarrow n \mid a - a' \quad b \equiv_n b' \Leftrightarrow n \mid b - b'$$

$$n \mid a - a' \Leftrightarrow \exists k \in \mathbb{Z} \text{ t.c. } a' - a = nk$$

$$n \mid b - b' \Leftrightarrow \exists k' \in \mathbb{Z} \text{ t.c. } b' - b = nk'$$

moltiplicazione delle equazioni

$$(a' - a)(b' - b) = nkk'$$

$$ab' - a'b - ab + ab = nkk' \Rightarrow a'b - ab = nkk' \Rightarrow n | a'b - ab \Leftrightarrow a'b \equiv_n ab$$

## Operazioni su $\mathbb{Z}/n\mathbb{Z}$

Definiamo  $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$  ricordando che  $\bar{a} = a + n\mathbb{Z} \rightarrow \text{es. } \bar{1} = 1 + 2\mathbb{Z}$

$$-(\bar{a}) := (-\bar{a}) \text{ applicazione } \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

è l'operazione di **opposto** in  $\mathbb{Z}/n\mathbb{Z}$

→ indipendente dalla scelta dei rappresentanti

Dette  $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$  definiamo  $\bar{a} + \bar{b} = \bar{a+b}$  ben definito delle classi  $\bar{a}$  e  $\bar{b}$

segniamo  $a' \in \bar{a}$  ( $\bar{a} \equiv a'$ ) e  $b' \in \bar{b}$

$$\overline{a+b} = \{m : n|m-a-b\} = \{m : n|m-a-b\} \leftrightarrow \overline{a+b} = \overline{a} + \overline{b}$$

l'operazione **addizione** appena introdotta su  $\mathbb{Z}/n\mathbb{Z}$  è ben definita

Definiamo inoltre  $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$   $\bar{a} \cdot \bar{b} = \bar{ab}$  ben definita

**es**

$$\bar{x}, \bar{z} \in \mathbb{Z}/3\mathbb{Z} \quad \bar{x} + \bar{z} = \bar{3} = \bar{0}$$

$$\bar{x} = \bar{4} \quad 1-4=3 \quad 3|3$$

$$\bar{z} = -\bar{4} \quad 2-(-4)=6 \quad 6|3$$

$$\bar{4} + \bar{4} = \bar{4+4} = \bar{0}$$

### Teorema

$(\mathbb{Z}/n\mathbb{Z}, +, -, \cdot, \bar{0}, \bar{1})$  è un anello

### Alcuni sottoinsiemi di $\mathbb{Z}$

- $n\mathbb{Z} = \{m \in \mathbb{Z} \text{ t.c. } \exists k \in \mathbb{Z} \text{ con } m = kn\} = \text{multipli di } n$
- $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$

#### esercizi

$$a, b \in \mathbb{Z}^*, \quad ab \leftrightarrow b \mathbb{Z} \subset a\mathbb{Z}$$

link

supponiamo che  $ab \leftrightarrow \exists k \in \mathbb{Z} \text{ t.c. } b = ka$

= l

sia  $b' \in b\mathbb{Z} \quad \exists l \in \mathbb{Z} \text{ t.c. } b' = lb \text{ ma } b = ka \Rightarrow b' = (lk)a$

dunque  $b' \in a\mathbb{Z}$

link

$b\mathbb{Z} \subset a\mathbb{Z}$  allora  $ab$

supponiamo che  $b\mathbb{Z} \subset a\mathbb{Z}$  vuol dire che  $\forall b' \in b\mathbb{Z} \rightarrow b' \in a\mathbb{Z}$

se  $b \in b\mathbb{Z} \quad \exists k \in \mathbb{Z} \text{ t.c. } b = kb \quad K=1$

allora  $b \in a\mathbb{Z} \quad \exists l \in \mathbb{Z} \text{ t.c. } b = la \Rightarrow ab$

- $a\mathbb{Z} + b\mathbb{Z} := \{m \in \mathbb{Z} \text{ t.c. } \exists k, k' \in \mathbb{Z} \text{ con } m = ka + k'b\}$

#### es

$$2\mathbb{Z} + 3\mathbb{Z} = \left\{ \begin{array}{l} K \text{ varia, } K=0, -2, 0, 2, 4, 6, 8, \dots \\ K=0, K' \text{ varia } -3, 0, 3, 6, 9, \dots \\ K, K' \text{ variano } 5, 8, 13, 7, -1, 1, \dots \end{array} \right\} = \mathbb{Z}$$

$$\hookrightarrow 2 \cdot 2 + 3 \cdot 3 = 13$$

vedremo che  
 $a\mathbb{Z} + b\mathbb{Z} = \text{MCD}(a, b)\mathbb{Z}$

es  $\text{MCD}(2, 3) = 1$

$$2\mathbb{Z} + 3\mathbb{Z} = 1\mathbb{Z}$$

LEMMA sia  $\mathcal{E} = a\mathbb{Z} + b\mathbb{Z}$   $a, b \neq 0 \Rightarrow$  esiste  $S \in \mathbb{N}^*$  unico t.c.  $\mathcal{E} = S\mathbb{Z}$

dim

per il principio del minimo un sottoinsieme non vuoto di  $\mathbb{N}^*$  ammette un elemento minimo

poniamo  $\mathcal{E}^* = \mathcal{E} \cap \mathbb{N}^* \subset \mathbb{N}^*$

osserviamo che  $\mathcal{E}^*$  non è vuoto  $\mathcal{E}^* \neq \emptyset$  infatti se  $a, b > 0$  esiste una coppia  $(K, K') \in \mathbb{N}^2$  t.c.  $Ka + K'b > 0$

$\in \mathcal{E}^*$

se invece  $a > 0$  e  $b < 0$  allora esiste  $(K, K') \in \mathbb{N} \times \{-\mathbb{N}\}$  t.c.  $Ka + K'b > 0$

ci sono ancora 2 casi ma è chiaro

OSS  $\mathcal{E} = \mathcal{E}^* \cup \{0\} \cup (-\mathcal{E}^*)$   
 $\forall x \in \mathcal{E} \quad -x \in \mathcal{E}$  se  
 $x = Ka + K'b$   
 $-x = -Ka + (-K)b$

se  $\mathcal{E}^*$  è vuoto vuol dire che  $-\mathcal{E} = \emptyset$   
il che vuol dire che  $\mathcal{E} = \{0\}$  impossibile per ipotesi

poniamo  $S = \min(\mathcal{E}^*)$  ben definito in  $\mathbb{N}^*$  (principio del minimo)

osserviamo che:

$S \leq |a|$  e  $S \leq |b|$  infatti  $|a|, |b| \in \mathcal{E}^*$

sia  $S/a$  per divisione euclidea si ha  $a = qS + r$   $r \in \{0, \dots, S-1\}$

notiamo che  $r = a - qS$ , e dato che  $S \in \mathcal{E}^* \subset \mathcal{E} = a\mathbb{Z} + b\mathbb{Z}$

$S = qa + rb \quad q, r \in \mathbb{Z}$

dunque si ha

$$r = a - q(qa + rb) \rightarrow r = a(1-q) + b(-q) \Rightarrow r \in \mathcal{E}^* \Rightarrow r \geq S$$

quindi  $r=0$  e  $S/a$

per la stessa ragione  $S/b$

CONTRADDIZIONE

se  $r \neq 0$  allora  $r \in \mathcal{E}^*$  e quindi deve essere  $\geq S$  dato che  $S$  è il minimo ma è impossibile per la definizione di  $r$

$\forall a, b \in \mathbb{Z} \quad S | ax + by \Rightarrow \mathcal{E} \subset S\mathbb{Z}$  d'altronde  $S \in \mathcal{E} \iff S = ka + kb$

$$\forall k \in \mathbb{Z} \quad lk = (lk)a + (lk')b \Rightarrow lS \subseteq E \Rightarrow S \subseteq E$$



Massimo comune divisore DEF

$(a, b) \in \mathbb{Z}^2$  con  $(a, b) \neq (0, 0)$

$d \in \mathbb{N}^*$  è MCD di  $a$  e  $b$  se si scrive  $d = \text{MCD}(a, b)$

①  $d \mid a$  e  $d \mid b$

②  $d' \in \mathbb{N}^*$  t.c.  $d' \mid a$  e  $d' \mid b \Rightarrow d' \mid d$

LEMMA se  $d$  soddisfa ① e ② allora  $d$  è unicamente determinato

dim

supponiamo che  $d_1, d_2$  soddisfino ① ②

mostriamo che  $d_1 = d_2$

si ha  $d_2 \mid d_1$  e  $d_1 \mid d_2 \Rightarrow \{d_1, -d_1\} = \{d_2, -d_2\} \Rightarrow d_1 = d_2$   $\rightarrow$  su  $\mathbb{N}^*$  la relazione di divisibilità è antisimmetrica quindi  $alb, bla \Rightarrow a=b$

per ②



Terminologia se  $\text{MCD}(a, b) = 1$  si dice che  $a, b$  sono primi tra loro (coprimi)

LEMMA dato  $a\mathbb{Z} + b\mathbb{Z} = S\mathbb{Z}$  con  $a, b \neq 0$  allora  $S = \text{MCD}(a, b)$

dim

$$S\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \supseteq a\mathbb{Z} \Rightarrow S \mid a$$

$$S\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \supseteq b\mathbb{Z} \Rightarrow S \mid b$$

condizione ① di MCD  
verificata

sia  $d' \in \mathbb{N}^*$  t.c.  $d' \mid a, d' \mid b$

$$d' \mid a \Leftrightarrow a \in d'\mathbb{Z}$$

$$d' \mid b \Leftrightarrow b \in d'\mathbb{Z}$$

$$S\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subseteq (d'\mathbb{Z} + d'\mathbb{Z}) \Rightarrow d' \mid S$$



Algoritmo di Euclide (MCD)

dati:  $a, b > 0$  serve a trovare  $S = \text{MCD}(a, b)$

$$a = q_0 b + r_0 \quad 0 \leq r_0 < b$$

$$b = q_1 r_0 + r_1 \quad 0 \leq r_1 < r_0$$

$$r_0 = q_2 r_1 + r_2 \quad 0 \leq r_2 < r_1$$

:

$$r_{n-2} = q_n r_{n-1} + r_n \quad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n + 0 \quad \text{e}$$

es

$$a = 3522 \quad b = 321$$

$$3522 = 10 \cdot 321 + 312$$

$$321 = 1 \cdot 312 + 9$$

$$312 = 34 \cdot 9 + 6$$

$$\boxed{9 = 1 \cdot 6 + 3} \quad 3 = \text{MCD}(3522, 321)$$

$$6 = 2 \cdot 3 + 0$$

$$\text{inoltre } 6\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \Rightarrow \exists u, v \in \mathbb{Z} \quad 3 = 3522u + 321v$$

come calcolo  $u$  e  $v$ ?

### Identità di Bezout

dati  $a, b \neq 0$   $\exists x, y: ax + by = \text{MCD}(a, b)$

coeffienti di Bezout

es

saliamo nelle iterazioni dell'algoritmo di Euclide e prendiamo il resto

$$3 = 9 - 1 \cdot 6$$

$$6 = 312 - 34 \cdot 9$$

↓

$$3 = 9 - 1(312 - 34 \cdot 9) \Rightarrow 3 = 9 - 312 + (34 \cdot 9)$$

$$\Rightarrow 3 = 9 \cdot 35 - 312$$

$$9 = 321 - 312$$

↓

$$3 = (321 - 312) \cdot 35 - 312$$

$$3 = 321 \cdot 35 - 312 \cdot 36$$

$$312 = 3522 - 10 \cdot 321$$

↓

$$3 = 321 \cdot 35 - (3522 - 10 \cdot 321) \cdot 36 \Rightarrow 3 = 321 \cdot 35 - 3522 \cdot 36 + 36 \cdot 10 \cdot 321$$

↓

$$3 = 321(35 + 360) - 3522 \cdot 36$$

$$\text{dunque } 3 = (-36) \cdot 3522 + (395) \cdot 321$$

↓

↓

↓

↓