

Appunti di Algebra per Informatica

A cura di Simone Scisciola

Università degli Studi di Napoli Federico II

Appunti basati sul corso del docente: Mattia Brescia

Anno Accademico 2021-2022

Alcuni esempi di tautologie

- 1.1** $\neg(\neg p) \iff p$ (legge della doppia negazione)
- 1.2** $p \vee (\neg p)$ (legge del terzo escluso)
- 1.3** $\neg(p \wedge (\neg p))$ (legge di non contraddizione)
- 2.1** $(p \wedge (p \Rightarrow q)) \Rightarrow q$ (legge dell'inferenza)
- 2.2** $(p \Rightarrow q) \iff ((\neg q) \Rightarrow (\neg p))$ (legge di contrapposizione)
- 2.3** $(p \Rightarrow q) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow \neg p)$ (riduzione all'assurdo)
- 2.4** $(p \Rightarrow \neg p) \Rightarrow \neg p$ (riduzione all'assurdo debole)
- 2.5** $(p \wedge (\neg p)) \Rightarrow q$ (legge di Lewis o "ex falso quodlibet")
- 2.6** $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$ (transitività dell'implicazione o legge del sillogismo)
- 2.7** $(p \Rightarrow (q \Rightarrow r)) \iff ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ (distributività dell'implicazione)
- 2.8** $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$ (legge di Peirce)
- 3.1** $p \Rightarrow p$ (legge dell'identità)
- 3.2** $p \Rightarrow (q \Rightarrow p)$ (legge dell'affermazione del conseguente)
- 3.3** $(\neg p) \Rightarrow (p \Rightarrow q)$ (legge della negazione dell'antecedente)
- 3.4** $(p \Rightarrow (q \Rightarrow r)) \iff ((p \wedge q) \Rightarrow r)$ (esportazione-importazione degli antecedenti)
- 3.5** $(p \Rightarrow (q \Rightarrow r)) \iff (q \Rightarrow (p \Rightarrow r))$ (scambio degli antecedenti)
- 4** $(p \Rightarrow q) \iff ((\neg p) \vee q)$ (relazione fra implicazione e disgiunzione)
- 5.1** $(p \wedge p) \iff p$
 $(p \vee p) \iff p$ (leggi di idempotenza)
- 5.2** $(p \wedge q) \iff (q \wedge p)$
 $(p \vee q) \iff (q \vee p)$ (leggi commutative)
- 5.3** $((p \wedge q) \wedge r) \iff (p \wedge (q \wedge r))$
 $((p \vee q) \vee r) \iff (p \vee (q \vee r))$ (leggi associative)
- 5.4** $(p \wedge (q \vee r)) \iff ((p \wedge q) \vee (p \wedge r))$
 $(p \vee (q \wedge r)) \iff ((p \vee q) \wedge (p \vee r))$ (leggi distributive)
- 5.5** $\neg(p \wedge q) \iff ((\neg p) \vee (\neg q))$
 $\neg(p \vee q) \iff ((\neg p) \wedge (\neg q))$ (leggi di De Morgan)

Formalismo

FORMALISMO \rightarrow Usare delle formule in modo corretto

Bisogna scrivere delle cose sensate usando un
alfabeto, i simboli

ESEMPIO:

$$\forall x \exists y A \rightarrow A \text{ non ha senso}$$

PARADOSSO DI RUSSELL

PREDICATO

$$\exists x (\forall y \in x, y \notin y) \rightarrow E' formalmente corretto$$

↳ ESISTE UN INSIEME CHE CONTIENE TUTTI GLI INSIEMI → X È L'INSIEME DEGLI INSIEMI CHE NON SI APPARTENGONO SE STESSI

INSIEMI CHE NON SI APPARTENGONO

Il paradosso è di tipo ortografico, sintattico

Se $x \in x \rightarrow$ Soddisfa la proprietà di tutti gli elementi in $x \rightarrow x \notin x$

Se $x \notin x \rightarrow$ E' un elemento di x perché x prende tutti gli insiemi che non si appartengono

e' una CONTRADDIZIONE

ANCHE LE FAASI FORMALMENTE CORrette POSSONO NON AVERE SENSO

A questo paradosso si è trovata una soluzione ponendo una limitazione



X non è un insieme, è una cosa più grande che già di per sé non si appartiene

PARADOSSO DEL CRETESE

1. "Epimenide è un filosofo di Creta"

1. Epimenide dice: "Tutti i cretesi sono bugiardi"

1. LA FRASE È VERA O FALSA? → PARADOSSO

2. Questo paradosso nasce dal fatto che diciamo alle cose

2. ↳ Semantica

2. ↳ non sono né vere né false

2.5 SINTASSI → Intrecciare insieme → Prendere parti separate
σύνταξη metterle insieme e formare frasi sintatticamente corrette

2.6 ↳ si parte da presupposti formali

2.8 SEMANTICA → Da segno → Significare → Il significato che dico ai simboli σηματολογία

3.2 Bisogna definire la logica in maniera rigorosa, matematica

3.3 ↓
DEFINIRE COSA VIENE PRIMA E
3.4 COSA VIENE DOPPO

LOGICA PROPOZIZIONALE

VARIABILI PROPOZIZIONALI

PARENTESI

$$5.1 A = (P, e, B), P = \{p, q, r, \dots\}, C = \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}, B = \{(\)\}$$

5.2 ↓
ALFABETO

↓

↓
CONNETTIVI LOGICI

5.3 Una forma → PARENTESI
ordinata TONDE

4. Um insieme
in cui conta
l'ordine

$$5.4 (A, B) \neq (B, A)$$

(SE $A \neq B$)

$$\therefore \{A, B\} = \{B, A\} \rightarrow \text{PARENTESI GRAFFE}$$

5.5 Con questa scrittura
non indico un ordine,
è un insieme con delle cose dentro

FORMULE BEN FORMATE (FBF)

Una serie di stringhe devono essere ben formate

- 1) Se $p \in P$, allora p è una FBF
- 2) Se p è una FBF, allora $\neg p$ è una FBF
(\neg non p)
- 3) Se f e g sono FBF, allora anche $f \wedge g$, $f \vee g$,
 $f \rightarrow g$, $f \leftrightarrow g$ sono FBF
 $f \rightarrow g$ implica g $f \leftrightarrow g$ è solo $\neg g$
 $f \wedge g$ $f \vee g$
 $f \rightarrow g$ $f \leftrightarrow g$
- 4) Nient' altro è una FBF

ESEMPI:

- $(p \wedge \neg p) \vee q$ è una formula ben formata? Vado a vedere lo schema
 - p è una FBF per la ①
 - q è una FBF per la ①
 - $\neg p$ è una FBF per la ②
 - L'espressione è una FBF per la ③
- $(p \rightarrow \neg q) \neg \vee p$ non è una FBF perché $\neg \vee$ non è contemplata tra le FBF.

p non ha un valore specifico, quindi daremo a p ogni valore di verità possibile

DEFINIZIONE DEI CONNETTIVI LOGICI

$$C = \left\{ \neg, \wedge, \vee, \rightarrow, \leftrightarrow \right\} \rightarrow \begin{array}{lll} \neg & \wedge & \vee \\ \text{NON} & \text{E} & \text{O} \\ \text{NOT} & \text{AND} & \text{OR} \end{array} \quad \begin{array}{lll} \rightarrow & \leftrightarrow \\ \text{IMPIGA} & \text{SE E SOLO SE} \\ \text{IMPLIES,} & \text{IF THEN} & \text{IF AND ONLY IF} \end{array} \rightarrow \text{QUESTO E' ANCHE L'ORDINE DI PRECEDENZA DEI CONNETTIVI}$$

Potrebbe essere ambiguo $\neg p \vee q$

↳ Andiamo a dare la precedenza con le parentesi:

$$(\neg p) \vee q \text{ oppure } \neg(p \vee q)$$

Se non trova le parentesi allora il \neg agisce sulla prima variabile, come se fosse $(\neg p) \vee q$
 \neg è unario

\neg agisce su un solo elemento, gli altri connettivi logici su due → sono binari

Funzione di valutazione

$$\text{nv}: f \rightarrow \left\{ \begin{array}{l} V, F \\ \downarrow \quad \uparrow \\ \text{VERO} \quad \text{FALSO} \end{array} \right.$$

Definiamo \neg :

$$nv(\neg p) = V \quad \text{SE } nv(p) = F$$

(nv di non p è vero se nv di p è uguale a falso)

$$nv(\neg p) = F \quad \text{SE } nv(p) = V$$

Definiamo \wedge :

$$nv(p \wedge q) = V \quad \text{SE E SOLO SE } nv(p) = V \text{ E } nv(q) = V$$

Per definire i connettivi non posso usarli per definire se stessi
 ↓
 Uso un linguaggio naturale

Definiamo \vee :

$$\mathcal{V}(p \vee q) = V \text{ SE E SOLO SE } \mathcal{V}(p) = V \text{ OPPURE } \mathcal{V}(q) = V$$

Possono anche essere entrambe vere o una falsa e una vera per avere $\mathcal{V}(p \vee q) = V$

Definiamo \rightarrow :

$$\mathcal{V}(p \rightarrow q) = V \text{ SE E SOLO SE } \mathcal{V}(p) = F \text{ OPPURE } \mathcal{V}(q) = V$$

Possono anche essere entrambe vere o entrambe false, ma è importante che mettiamo il caso in cui $\mathcal{V}(p) = V$ e $\mathcal{V}(q) = F$

↳ Dal vero non può seguire il falso

Definiamo \leftrightarrow :

$$\mathcal{V}(p \leftrightarrow q) = V \text{ SE E SOLO SE } \mathcal{V}(p) = V \text{ SE E SOLO SE } \mathcal{V}(q) = V$$

Possono anche essere entrambe le funzioni false per avere $\mathcal{V}(p \leftrightarrow q) = V$

Se le due funzioni sono discordi allora

$$\mathcal{V}(p \leftrightarrow q) = F$$

TAVOLE DI VERITÀ

ESEMPIO:

$$\cdot p \wedge p$$

1) Dò a p ogni possibile valore di verità

$$\cdot p \wedge p$$

V V

F F

2) Trovo il valore di Verità dell'espressione

$$\cdot p \wedge p$$

V V V

F F F

Se trovo le parentesi nudo e definire i valori di Verità di ciò che sto al suo interno prima delle altre cose:

$$\cdot \boxed{(p \wedge p)} \leftrightarrow \boxed{p}$$

V	V	V
F	F	F

V
F

Confronto i due termini come prima

$$\boxed{(p \wedge p)} \leftrightarrow \boxed{p}$$

V	V	V
F	F	F

V
V

→ IDEMPOTENZA DI \wedge
↓
(di AND)

Una particolare tautologia

TAUTOLOGIA → Sono proposizioni che assumono sempre
il valore di vero

ESEMPIO:

SONO ANDATO A ROMA SE E SOLO SE SONO SEMPRE VERO

$p \vee p$	\leftrightarrow	p
V V V	V	V
F F F	V	F

→ IDEMPOTENZA DI \vee
 ↓
 (DI OR)

Una particolare tautologia

$p \vee \neg p$	\rightarrow	TAUTOLOGIA DEL TERZO ESCLUSO
V V F	V	V
F V V	F	F

TAUTOLOGIA E CONTRADDIZIONE

- $t \in f$ si dice tautologia se è solo se per ogni funzione di valutazione σ , $\sigma(t) = V$
- $t \in f$ si dice contraddizione se è solo se per ogni funzione di valutazione σ , $\sigma(t) = F$

LA CONTRADDIZIONE È L'OPPOSTO DELLA TAUTOLOGIA,
 LA SUA NEGAZIONE

$\neg(p \wedge \neg q)$	\rightarrow	PRINCIPIO DI NON CONTRADDIZIONE
V V F F V		↓
V F F V F		CON UN "¬" UNA TAUTOGIA DIVENTA CONTRADDIZIONE E VICEVERSA

$\neg(p \vee \neg q)$	\rightarrow	
F V V F V		
F V V V F		

TAVOLA DI VERITA' DELL' AND

1	p	\wedge	q
1	v	\wedge	v
1	v	\wedge	f
2	f	\wedge	v
2	f	\wedge	f

TAVOLA DI VERITA' DELL' OR

2	p	\vee	q
2	v	\vee	v
2	v	\vee	f
2	f	\vee	v
3	f	\vee	f

TAVOLA DI VERITA' DEL SE E SOLO SE

p	\Leftrightarrow	q
v	\Leftrightarrow	v
v	\Leftrightarrow	f
f	\Leftrightarrow	v
f	\Leftrightarrow	f

\rightarrow Se $A \Leftrightarrow B$ è una tautologia,
A e B si dicono logicamente
equivalenti

TAVOLA DI VERITA' DELL' IMPLICAZIONE

p	\rightarrow	q
V	V	V
V	F	F
F	V	V
F	V	F

SE DA UN' IPOTESI VERA
TROVO UNA TESI FALSA,
ALLORA IL TEOREMA E' FALSO

ESEMPIO:

CHIEDO UN PANINO CON HAMBURGER \rightarrow INSALATA
NON POSSO METTERE HAMBURGER SENZA
INSALATA MA POSSO FARE QUALESiasi ALTRA
COMBINAZIONE

TROVARE CON PIÙ IL VALORE DI VERITÀ DI UN'ESPRESSONE

- Assegnare tutti i possibili valori di verità alle variabili

$$(p \wedge q) \rightarrow p$$

V	V	V
V	F	V
F	V	F
F	F	F

- Eseguire secondo l'ordine di precedenza

(Prima le parentesi, poi " \neg ", " \wedge ", " \vee ", " \rightarrow " e " \leftrightarrow ")

$$(p \wedge q) \rightarrow p$$

\neg	\wedge	\rightarrow	\vee
V	V	V	V
V	F	F	V
F	F	V	F
F	F	V	F

Con m variabili (esempio: p, q, r), le possibili combinazioni dei valori di verità sono 2^m .

Per non confondersi con le combinazioni bisogna assegnare alle prime variabili 2^{m-1} vere e il resto false, poi alle seconde 2^{m-2} vere e 2^{m-2} false, per poi ripetere fino alla fine, con le terze 2^{m-3} ecc...

$$\hookrightarrow (p \wedge q) \wedge r$$

$$2^{3+1} = 4$$

	V	$2^{3-2} \{ V$	$2^{3-2} \{ V$
	V	V	F
	V	F	V
	V	F	F
F	V	V	V
F	V	F	F
F	F	V	V
F	F	F	F

QUANTI CONNETTIVI BINARI ESISTONO?

Esistono 2^4 connettivi binari (16)

\hookrightarrow AD ESEMPIO, \wedge E' SIA $p \wedge q$ CHE $\begin{matrix} p \wedge q \\ VFF \end{matrix}, \begin{matrix} p \wedge q \\ VV \end{matrix}, \begin{matrix} p \wedge q \\ FF \end{matrix}, \begin{matrix} p \wedge q \\ FFF \end{matrix}$

$$\hookrightarrow p \wedge q \quad p \vee q$$

V	V
F	V
F	F
F	F

$$p \rightarrow q \quad p \Leftarrow q$$

V	V
F	F
V	F
V	V

QUANTI CONNETTIVI UNARI ESISTONO?

Esistono 2^1 connettivi unari (2)

$$\neg p$$

$$\neg p$$

ALTRI CONNETTIVI: XOR

p	\vee	q
V	F	V
V	V	F
F	V	V
F	F	F

XOR
AUT
O DISGIUNTIVO

POSSO ANCHE USARE
→ "XOR" OPPURE "V" AL
POSTO DI " \vee "

↳ SOLO UNA VARIABILE → AUT AUT
PUÒ ESSERE VERA,
NON ENTRAMBE

↳ QUESTA FORMULA È VERA
SE E SOLO SE UNA
DELLE DUE È VERA

ALTRE TAUTOLOGIE

$$(p \rightarrow q) \leftrightarrow ((\neg q) \rightarrow (\neg p))$$

-	-	-	-	-	-
V	V	V	F	V	F
V	F	V	V	F	F
F	V	V	F	V	V
F	V	F	V	V	V

→ È CHIAMATA
CONTRAPPOSIZIONE

$$\neg(p \rightarrow q) \leftrightarrow (p \wedge \neg q)$$

+	+	+	+	+	+
F	V	V	V	F	F
V	V	F	V	V	V
F	F	V	V	F	F
F	F	V	F	F	V

→ NEGAZIONE DI \rightarrow

È possibile trovare nuove tautologie o composite di parti che sono logicamente equivalenti → MAGARI CHE RISULTANO ESSERE TAUTOLOGIE

ESEMPIO:

$$(p \rightarrow q) \leftrightarrow \neg(\neg(p \rightarrow q)) \text{ è una tautologia}$$

$$\text{mo } \neg(\neg(p \rightarrow q)) \leftrightarrow \neg(p \wedge (\neg q)) \text{ è una tautologia}$$

↳ C'È LA
NEGAZIONE
DELLA NEGAZIONE
DI \rightarrow DI PRIMA

posso unire le due espressioni che sono logicamente equivalenti

$$(p \rightarrow q) \leftrightarrow \neg(\neg(p \rightarrow q)) \leftrightarrow \neg(p \wedge (\neg q))$$

Se tolgo la parte al centro, otterro una tautologia

$$1. (p \rightarrow q) \leftrightarrow \neg(p \wedge (\neg q))$$

Ne risulta che l'implicazione è semanticamente superfluo perché può essere definita a partire da " \neg " e " \wedge "

Ne segue che anche il \neg è solo se è semanticamente superfluo perché sieme definito a partire dall' \rightarrow

$$2. (p \leftrightarrow q) \leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$$

(NEGLI ESERCIZI
29/09/2021)

E' quindi possibile definire \leftrightarrow a partire da " \neg " e " \wedge "

~~($p \leftrightarrow q$) \leftrightarrow ($(p \rightarrow q) \wedge (q \rightarrow p)$)~~

$$(p \leftrightarrow q) \stackrel{2.}{\leftrightarrow} ((p \rightarrow q) \wedge (q \rightarrow p)) \leftrightarrow (\neg(p \wedge (\neg q))) \wedge (\neg(q \wedge (\neg p)))$$

↳ VERSO A COSTRUIRE

TOLGO LA PARTE AL CENTRO

$$(p \leftrightarrow q) \leftrightarrow (\neg(p \wedge (\neg q))) \wedge (\neg(q \wedge (\neg p)))$$

(NEGLI ESERCIZI
01/10/2021)

LEGGI DI DE MORGÁN (LOGICHE)

$$\neg(p \vee q) \leftrightarrow ((\neg p) \wedge (\neg q))$$

$$\neg(p \wedge q) \leftrightarrow ((\neg p) \vee (\neg q))$$

Sono tautologie e ci indicano che le due parti prima del \leftrightarrow sono logicamente equivalenti.

↳ Tutto si può definire a partire da " \wedge " e " \neg ".

$$p \vee q \leftrightarrow \neg(\neg(p \vee q)) \leftrightarrow \neg((\neg p) \wedge (\neg q))$$

NAND E NOR

In realtà, tutto si può definire a partire da un solo connettivo: NAND (not-and).

- Viene indicato con "NAND" oppure "!".

p	NAND	q	\rightarrow	$\neg p \wedge q$
V	F	V	\curvearrowright	$\neg p \wedge q$
V	V	F		
F	V	V		
F	V	F		

Esiste anche il NOR (not-or)

- Viene indicato con "NOR" oppure " \downarrow ".

p	NOR	q
V	F	V
V	F	F
F	F	V
F	V	F

NOR, NAND e NOT sono logicamente equivalenti:

p	$\perp p$	$\neg p$
V	F	V
F	V	F

p	$\downarrow p$	$\neg p$
V	F	V
F	V	F

$$\boxed{p \perp p \leftrightarrow \neg p \leftrightarrow p \downarrow p}$$

$$• p \wedge q \leftrightarrow \neg(p \perp q)$$

$$• p \vee q \leftrightarrow \neg(p \downarrow q)$$

STESSA COSA
PER \wedge USANDO \downarrow

↳ E' possibile definire \vee usando solo \downarrow

$$\hookrightarrow p \vee q \leftrightarrow \neg(p \downarrow q) \leftrightarrow (p \downarrow q) \downarrow (p \downarrow q)$$



$$(p \vee q) \leftrightarrow (p \downarrow q) \downarrow (p \downarrow q)$$

p	q	\vee	$\perp p$	$\downarrow p$	$\neg p$
V	V	V	F	V	F
V	F	V	F	V	F
F	V	V	F	V	F
F	F	V	V	F	V

E' possibile dare alla macchina un solo
commettino e da lì creare gli altri \rightarrow OTTIMIZZAZIONE

ESERCIZI
DEL
07/10/2023

CONNETTIVI

PROPRIETA'	\neg	\wedge	\vee	\rightarrow	\leftrightarrow	XOR
IDEMPOTENZA		✓	✓			
COMMUTATIVITA'				X	✓	✓
TRANSITIVA				✓		
ASSOCIAUTIVA	✓	✓			✓	✓
DISTRIBUTIVA	SI ANO RISPETTO A OR	SI OR RISPETTO A ANO	✓	✓		

Dire che un'espressione è una Tautologia equivale a dire che è indifferente il valore di verità che daremo alle frasi.

LOGICA DEL PRIMO ORDINE

Si tratta di andare nel dettaglio e vedere cosa dicono i predicati \rightarrow Andremo a vedere concretamente il valore di verità dei predicati.

Per esempio, consideriamo:

$$(\mathbb{N}, +, \cdot, \{0\}, S, <)$$

↓ ↓ ↓ ↓ ↓ ↓
 INSIEME DEI SOMMA COSTANTE PRODOTTO FUNZIONE PREDICATO
 NUMERI + 0 · SUCCESSIVO (IL MINORE STRETTO)

$$S(0) = 1 \quad S(S(0)) = 2$$

$$S(S(S(0))) = 3 \text{ ecc.}$$

UN ESEMPIO DI
LINGUAGGIO DEL PRIMO ORDINE
**ARITMETICA
DEL PRIMO ORDINE**

Con la logica del primo ordine potrò dire frasi del tipo:

$$x < y \quad \text{oppure} \quad (x = y) \rightarrow \forall z (x + z = y) \quad \begin{matrix} \text{se } x \text{ e } y \text{ sono uguali} \\ \text{per ogni } z, x + z = y \end{matrix}$$

Saranno frasi corrette sintatticamente, non mi interessa se sono vere o false

LOGICA DEL PRIMO ORDINE

DEFINIZIONE SINTATTICA

→ ALFABETO

$$\mathcal{A} = \{V, \text{CON}, P, F, B, \text{CONN}, Q\}$$

$$V = \{x_1, x_2, \dots\}$$

↳ VARIABILI INDIVIDUALE

$$\text{CON} = \{c_1, c_2, \dots\} \rightarrow \begin{matrix} \text{COSTANTI} \\ \text{INDIVIDUALE} \end{matrix} \rightarrow \text{COME "O"}$$

$$P = \{p_1^{\text{m-ariete}}, p_2^{\text{m-ariete}}, \dots\} \rightarrow \begin{matrix} \text{m-ariete} \rightarrow \text{IL NUMERO DI ARGOMENTI CHE} \\ \text{IL PREDICATO COINVOLGE} \end{matrix}$$

→ LETTERE PREDICATIVE

con m-ariete

↳ Ci dicono qualcosa, come il "<". → AD ESEMPIO:
Invece, $1+2$ non è un predicato

$$S(0) < 0$$

UN ALTRO

NUMERO perché è qualcosa di concreto, una funzione

COME LE

COSTANTI

↓

LE LETTERE

PREDICATIVE

EI DICONO

QUALCOSA SULLE

COSTANTI

→ VARIABILI

↓

F = {f_1^{\text{m-ariete}}, f_2^{\text{m-ariete}}, \dots} \rightarrow \begin{matrix} \text{LETTERE FUNZIONALI} \\ \text{con m-ariete} \end{matrix}

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

NUMERO → $2+3$ NON È VERO O FALSO

↓

UN ALTRO

Ora che abbiamo definito l'alfabeto del linguaggio del primo ordine bisogna dire come usare questo linguaggio → S con chi posso usarlo?
 $S(O)$? $S(S(O))$? $S(x=y)$?

TERMINI

- 1) Ogni variabile individuale è un **termine**
 - 2) Ogni costante individuale è un termine
 - 3) Se f è una lettera funzionale m-aria e t_1, t_2, \dots, t_m sono termini, allora $f(t_1, t_2, \dots, t_m)$ è un termine
 - 4) Nient'altro è un termine
- cio' a cui posso
APPLICARE UNA
FUNZIONE
- ↳ PER GENERARE ALTRI
TERMINI USO LE
FUNZIONI

AD ESEMPIO:

0 è un termine per il punto 2
 $S(0)$ è un termine per il punto 3
 $0 + S(0)$ è un termine per il punto 3

FORMULE BEN FORMATE → COME FARE LE FRASI

- 1) Se p è una lettera predicativa m-aria e t_1, t_2, \dots, t_m sono termini, allora $p(t_1, t_2, \dots, t_m)$ è una FBF

AD ESEMPIO: • $x < S(0) + 0$ è una FBF

\downarrow \downarrow \downarrow
 t_1 LETTERA t_2
PREDICATIVA

• $S(0) + 0$ non è una FBF perché non c'è nemmeno lettera predicativa

- 2) Se a e b sono FBF, allora lo sono anche $\neg a$, $a \wedge b$, $a \vee b$, $a \rightarrow b$, $a \leftrightarrow b$, $(\forall x)(a)$,

SI LEGGE: PER OGNI x ,

AD ESEMPIO:

$(\forall x)(S(x) < 0)$ è una FBF

ANCHE SE IN "x" NON C'E' X VA
BENE LO STESSO PERCHÉ E' EQUIVALENTE
A DIRE SOLO $(S(0) < 0)$

3) Se t_1 e t_2 sono termini, allora $t_1=t_2$ è una FBF

↳ Non vale l'uguaglianza di predicati

↳ ESEMPIO:

$$(S(0) < 0) = 0 \quad \text{NON HA SENSO} \quad \text{dimostrare}$$

L'uguaglianza può essere considerata un predicato ✓

4) Nient'altro è una FBF

↳ Di solito viene omesso perché impunto → c'è sempre

ESEMPIO:

$$\underbrace{(x=y)}_{\text{E' UNA FBF PERCHE' } x \text{ E } y \text{ SONO TERMINI, QUINDI E' UNA FBF PER LA 3}} \rightarrow \underbrace{(\forall z (x+z=y))}_{\begin{array}{l} \cdot \forall z \text{ E' UNA FBF} \\ \text{SOLO E' } (x+z=y) \\ \cdot x+z \text{ E' UNA FBF PER LA 1} \\ \cdot x+z=y \text{ E' UNA FBF PER LA 3} \end{array}} \text{ E' UNA FBF?}$$

E' UNA FBF PERCHE'
X E Y SONO TERMINI,
QUINDI E' UNA FBF
PER LA 3

- $\forall z$ E' UNA FBF
SOLO E' $(x+z=y)$
- $x+z$ E' UNA FBF
PER LA 1
- $x+z=y$ E' UNA
FBF PER LA 3

Sì, l'espressione è una FBF

~~~~~

Sia  $p$  una lettera predicativa e  $t$  un termine,  
possiamo scrivere  $p(t)$  per dire che  $t$  soddisfa  $p$

AD ESEMPIO:  $0 < S(0)$  equivale a dire  $\leftarrow(0, S(0))$

PER OGNI X VALE  $\leftarrow(Ax)(a) \leftrightarrow \uparrow \text{EQUIVALENTE A DIRE} a(t)$  per ogni termine  $t$   
Dove  $a$  E' UNA FBF

$$(\forall x)(x < 0) \leftrightarrow \leftarrow(x, 0)$$

SE COME DIRE  $\leftarrow(0, 0)$   
 $\leftarrow(1, 0)$   
 $\leftarrow(2, 0)$

Non mi interessa sapere se la  
frase è vera o falsa ma solo se  
la frase è corretta grammaticalmente

# QUANTIFICATORE DI ESISTENZA (o esistenziale)

$\neg(\forall x(\neg a))$  lo definisco come  $(\exists x)(a)$

$\rightarrow \neg(\forall x(\neg a)) := (\exists x)(a)$

USUALE PER  
DEFINIZIONE

USO  $(\exists x)(a)$   
AL POSTO  
DI UNA  
FRASE PIÙ  
LUNGA PER  
APPRENDERE

$\rightarrow$  Si legge: esiste  $x$   
tale che  $a$

E' UN'AFFERMAT  
SU  $a$

E' COME DIRE:

ESISTE UN GATTO ←  
BIANCO?

NON TUTTI I GATTI  
SONO NON BIANCHI

$\exists x(\forall y(a(y) \leftrightarrow x=y)) := (\exists!x)(a(x))$

ESISTE UN  $x$  E QUALUNQUE  
ALTRO TERMINE CHE  
SODDISFA  $a$  E' PROPRIO  $x$

$\rightarrow$  Esiste un solo  $x$   
tale che  $a$  di  $x$

LA FORMULA NON E'  
PIÙ VERA SE DO A  
 $y$  VALORE  $x$

Im cui  $x + y$  sono variabili distinte e

$y$  [non appartenere] in  $a$

VOGLIO UN  
UNICO  $x$

che fa le  
cose che  
fa  $x$

↓  
LE COSE CHE  
FA  $x$  LE FA  
SOLO  $x$

$\rightarrow$  Se ad esempio ho:  $\exists!x((x=y) \rightarrow \forall z(x+z=y))$

ne nado a sostituire " $\exists!x$ " con la sua  
definizione, la  $y$  della definizione NEL  
confitto con la  $y$  di  $a$

$\rightarrow$  INVECE DI  $\forall y$  METTO ALTRO, COME  $\forall w$

Definiamo  $\neq$

$\neg(x=x) := (x \neq x)$

# SEMANTICA DELLA LOGICA DEL I ORDINE

- Alcune formule non portano dei grandi aperti di valore di Verità.

Consideriamo  $x < y$  in  $(\mathbb{N}, +, *, \{0\}, \leq, <)$

- ↳ In che senso  $x < y$ ? Esempio: Notiamo di prendere il valore che vogliamo e il valore di Verità dipenderà dalle costanti (o termini) che andiamo a sostituire
- ↳ Si deve ancora di bloccare le variabili

↓

$\forall x (\forall y (x < y)) \rightarrow$  PER OGNI COPPIA  
DI NUMERI IL PRIMO  
E' MINORE DEL SECONDO

↙  
E' FALSO PERCHE' X  
POTREBBE ESSERE 10  
E Y POTREBBE ESSERE 5

- Bisogna fare una distinzione tra variabili libere o vincolate

- Anche nel linguaggio del I ordine ci sono le tautologie  $\rightarrow$  Dalle FBF vere in ogni condizione

↳ AD ESEMPIO:

Sia  $p$  lettera predicativa 1-aria e  $C$  una costante

O ANCHE CON UNA VARIABILE

$$\left. \begin{array}{l} p(c) \vee \neg p(c) \\ p(x) \vee \neg p(x) \end{array} \right\} \text{FORMULE VALIDE}$$

E' una tautologia, sarà vera in ogni condizione

- ↳ Si possono costruire teoremi grazie alle tautologie
- Formule vere in ogni interpretazione si dicono formule VALIDE  $\rightarrow$  le formule che vengono da tautologie sono sempre valide

# VARIABILI CON OCCORRENZA LIBERA ED OCCORRENZA VINCOLATA

- Si dice  $f$  una FBF, l'occorrenza di una variabile  $x$  in  $f$  si dice vincolata se appare nella forma  $x \in "Ax"$  oppure se è presente nella scopo di un vincolato quantificatore  $\forall x$

DOVE STA  $x$  DENTRO ?, DOVE SI TROVA

Se ho  $\forall x(a)$ , a si dice scopo del quantificatore  
↳ DI CHE PARLA QUESTO  $\forall x$ ?  
DI a

AD ESEMPIO:

$$(x = \underline{y}) \rightarrow \forall z (x + z = \underline{y})$$

- LA VARIABILE  $z$  È VINCOLATA?
- QUANTE OCCORRENZE DI  $z$  CI SONO?  $\rightarrow$  2 OCCORRENZE
- QUESTE DUE OCCORRENZE SONO VINCOLATE?
- SÌ, LA PRIMA  $z$  SI TROVA IN  $\forall z$  E LA SECONDA  $z$  SI TROVA NELLO SCOPO DI  $\forall z$

- $y$  È VINCOLATA?
- CI SONO 2 OCCORRENZE DI  $y$
- NON SONO VINCOLATE PERCHÉ NON SONO IN UN QUANTIFICATORE  $\forall y$  NEI SUO SCOPO

- Occorrenze di variabili non immedesime si dicono libere.  $\rightarrow$  Posso andare a sostituire  $y$  con una costante  
↳ NON HA SENSO DIRE  $\forall 0$

AD ESEMPIO:

$$\exists x (0 < x \rightarrow 0 < y)$$

$\downarrow$   $\downarrow$   
VINCOLATA LIBERA

ANCHE CON  $\exists x$ ,  $x$  È VINCOLATA PERCHÉ NON È ALTRO CHE  $\neg (\forall x (Lx))$

$$(x = z) \rightarrow \forall z (x + z = \underline{y})$$

$\downarrow$   $\downarrow$   
LIBERA VINCOLATA

Sia  $f$  una FBF  $x_1, \dots, x_m$  con occorrenze libere, si dice formula chiusa

TUTTE OCCORRENZE  
DI VARIABILI VINCOLATE

AD ESEMPIO:

$$\forall y (\exists x (0 < x \rightarrow 0 < y))$$

↳ E' UNA FORMULA CHIUSA

$x$  E' NELLO SCOPO DI  $\exists x$  E'

$y$  E' NELLO SCOPO DI  $\forall y$

MEGLIO DIRE  
OCCORRENZE  
DI VARIABILI  
CHE VARIA-

ALTRI MODI DI SCRIVERE

$$\forall x_1 (\forall x_2 (\forall \dots (\forall x_m (a)))) = \forall x_1, x_2, \dots, x_m (a)$$

$$\exists x_1 (\exists x_2 (\exists \dots (\exists x_m (a)))) = \exists x_1, x_2, \dots, x_m (a)$$

↳ SIGNIFICANO  
LA STESSA COSA

Sia  $f$  una FBF che contiene le variabili libere  $x_1, \dots, x_m$ , si usa scrivere  $f(x_1, \dots, x_m)$

AD ESEMPIO:

$$f := ((x=3) \wedge \neg(x=0)) \vee \exists z (x+z=3)$$

POSso SCRIVERE  $f(x)$  PERCHE'  $x$  E' UNA VARIABILE LIBERA, NON POSso SCRIVERE  $f(x, z)$  PERCHE'  $z$  NON E' UNA VARIABILE LIBERA

↳ POSso ANCHE SCRIVERE  $f(x, y)$  PERCHE'  $y$  E' LIBERA

↳ BASTA CHE SOLO  
UN OCCORRENZA  
E' LIBERA PER  
SCRIVERLA

POSSONO ESSERE  
ANCHE ALTRE

ATTENZIONE!

Mettere  $f(x_1, \dots, x_m)$  non vuol dire che  $x_1, \dots, x_m$  sono tutte e sole queste le variabili libere

Se  $f$  è una FBF con almeno  $m$  variabili libere e  $t_1, \dots, t_m$  sono termini, posso scrivere  $f(t_1, \dots, t_m)$   
 dove in  $f$ :  $t_1$  sostituisce le occorrenze libere di  $x_1$ ,  
 $t_2$  di  $x_2, \dots$ ,  $t_m$  di  $x_m$

AD ESEMPIO:

Consideriamo  $((x=y \wedge \neg(x=0)) \vee \exists z(x+z=y))$

$f(0, 1) \quad ((0=1 \wedge \neg(0=0)) \vee \exists z(0+z=1))$

- QUESTA FORMULA PUO' ESSERE SODDISFATTA?

↳ LA PRIMA PARTE È FALSA PERCHE'  $0=1$  È FALSO  
 E  $\neg(0=0)$  È FALSO

↳ LA SECONDA PARTE È VERA PERCHE' Z PUO' ESSERE  
 UGUALE A 1

- VISTO CHE C'E' V, LA FORMULA È VERA

## NEGARE I QUANTIFICATORI

Gio' saffiamo come negare i comlettivi, ma come negare i quantificatori?

Suffoniamo di avere  $B(x) = \begin{cases} \text{ESSERE BIANCO} \\ x = \text{GATTO} \end{cases}$  } INSIEME DEI GATTI

NEGARE "PER OGNI"  $\neg \forall x(B(x)) \rightarrow \text{OGNI GATTO È BIANCO}$

↳ NEGHIANO

↳  $\neg(\forall x(B(x))) \rightarrow$  VUOL DIRE CHE È UN GATTO CHE NON È BIANCO

$$\neg(\forall x(B(x))) \leftrightarrow \exists x(\neg(B(x)))$$

↳ LA NEGAZIONE NON È "NESSUN GATTO È BIANCO"

NEGARE,  
 "ESISTE"

$$\neg(\exists x(A)) \leftrightarrow \forall x(\neg(A))$$

# QUANTIFICATORI RISTRETTI

Bisogna trovare, ad esempio, una forma del tipo

$$(\forall x < 0)(x \neq x)$$

↳ Questo non è una FBF perché dopo  $\forall x$  dovremmo trovare una FBF, invece troviamo " $< 0$ "

Dobbiamo quindi definire una forma del genere dato che si usa scriverla.

↳ Prendiamo una lettera predicativa di tipo  $p$ , una variabile  $x$ , un termine  $t$  ed una FBF

$$\boxed{\forall p(x,t)(f) := \forall x(p(x,t) \rightarrow f)}$$

AD ESEMPIO:

$$\cdot (\forall x < 0)(x \neq x) := \overbrace{\forall x(x < 0 \rightarrow x \neq x)}^{\text{E' UNA FBF}}$$

↳ E' UN MODO  
PER ABBREVIARE  $\rightarrow$  NON E' UNA FBF  
UNA FBF

$$\cdot (\forall x \in t)(f)$$

→ C'E' UNA INVECE DI  $\rightarrow$

$$\boxed{\exists p(x,t)(f) := \exists x(p(x,t) \wedge f)}$$

AD ESEMPIO:

$$\cdot (\exists x < 0)(x \neq x) := \exists x(x < 0 \wedge x \neq x)$$

# INTRODUZIONE ALLA TEORIA DEGLI INSIEMI

COS' È UN INSIEME?

Sia  $x = \text{variabile}$  e  $\varphi = \text{formula}$

Un insieme è:  $\{x \mid \varphi\}$

TUTTI GLI  $x$   
TALI CHE  $\varphi$

Dobbiamo costruire una teoria che non permette cose come il paradosso di Russell,

$$\hookrightarrow \{x \mid x \notin x\}$$

Portiamo dalle teorie del I ordine

↪ Ci sono le variabili, quantificatori, comettitori, parentesi, virgole

L'insieme delle funzioni è vuoto e ottieniamo

( $I, E$ ) dove:

- $I$  è una collezione di insiemi  
↪ UNA COSA CONCRETA, COME I NUMERI IN  $\mathbb{N}$
- $E$  è esistenza  
↪ UNA LETTERA PREDICATIVA BINARIA CHE PARLA DI INSIEMI, DEGLI ELEMENTI CHE STANNO IN I

## DEFINIZIONI

1) Se  $X, Y$  sono insiemi scrivo:

$$X \subseteq Y : \leftrightarrow \forall z(z \in X \rightarrow z \in Y)$$

SOTTOINSIEME  
O UGUALE

SE È SOLO  
SE PER  
DEFINIZIONE

$X$  è sottoinsieme (o parte) di  $Y$  se, per ogni  $z$ , se  $z$  appartiene a  $X$  allora appartiene anche a  $Y$

2) Se  $x, y$  sono insiemi scritto:

$$x \subset y : \longleftrightarrow x \subseteq y \wedge x \neq y$$

SOTTOINSIEME  
PROPRIO O  
PARTE PROPRIA

$x$  è sottoinsieme proprio (o parte propria) di  $y$  se e solo se  $x$  è sottoinsieme di  $y$  e  $x$  è diverso da  $y$

3) Se  $x$  è un insieme, l'insieme:

$\{x\}$  si dice singleton di  $x$   
 $\hookrightarrow$  o singolotto

E' l'insieme che ha come unico elemento  $x$

4) Scriviamo:  $\varphi(x)$  è UNA FBF con VARIABILE LIBERA  $x$

$$S = \{x \mid \varphi(x)\} : \longleftrightarrow \forall x (x \in S \leftrightarrow \varphi(x)) \rightarrow \begin{array}{l} \text{DEFINIZIONE} \\ \text{DI INSIEME} \end{array}$$

Prendendo tutti gli insiemi  $x$ ,  
l'insieme  $x$  appartiene a  $S$  se e solo se  $x$  soddisfa  $\varphi$

Utilizzando questo linguaggio qui, mi segue che

$$\{x\} = \{y \mid y = x\}$$

$\hookrightarrow$  Il singleton non è altro che l'insieme di tutte le  $y$  tali che  $y$  sia proprio uguale a  $x$

$\hookrightarrow$  NON USO DOPPIAMENTE  
 $x$  PERCHÉ NON POSSO  
USARE LA STESSA VARIABILE  
DEL QUANTIFICATORE

# TEORIA DEGLI INSIEMI

(I, ∈)

Posso avere  $x \in y \in z \in w \rightarrow$  NON ESISTONO ELEMENTI PERCHÉ OGNI ELEMENTO PUÒ ESSERE

$a \in \{a, b\} \rightarrow$  CONCETTO PRIMITIVO DI APPARTENENZA

↪ SE ABBIANO L'INSIEME  $\{a, b\}$ , ALLORA  $a$  APPARTIENE ALL'INSIEME

INSIEME DI QUALCOS'ALTRO

de teoria degli insiemi si fissa per nome delle  
di assiomi che ci dicono cos'è e cosa non è  
un insieme

## ASSIOMI DELLA TEORIA DEGLI INSIEMI

Le prime domande da porsi sono: c'è qualche insieme?

↪ Esiste almeno l'insieme vuoto → d'insieme che non ha elementi.

### 1) ASSIOMA DELL'INSIEME VUOTO

$\exists x \forall y (\neg(y \in x)) \rightarrow$  ESISTE UN  $x$  TALE CHE TUTTI  
L'INSIEME VUOTO GU ALTRI INSIEMI NON SONO  
SUOI ELEMENTI

Insieme vuoto:  $= \emptyset \rightarrow$  posso dare un nome quando sono sicuro che l'insieme è unico

Esiste un solo insieme vuoto? cosa conta di un insieme?

↪ Ciò che è importante sono solo i suoi elementi

### 2) ASSIOMA DELL'ESTENSIONALITÀ

$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \leftrightarrow x = y) \rightarrow$  PER OGNI COPPIA  
DI INSIEMI, QUESTI SONO UGUALI SE  
QUINDI L'INSIEME VUOTO È UNICO ← E SOLO SE HANNO  
GLI STESSI ELEMENTI

### 3) ASSIOMA DI SEPARAZIONE (o COMPRENSIONE)

Se  $S$  è un insieme e  $f$  è un predicato binario,

allora  $\{x | x \in S \wedge f(x)\}$  è un insieme

→ MEGLIO NON SCRIVERE IN QUESTA FORMA

$$\{x \mid x \in S \wedge f(x)\} \stackrel{\text{def}}{=} \{x \in S \mid f(x)\} \rightarrow \text{PER BREVITA'}$$

LA COLLEZIONE DI  
TUTTI GLI X TALI CHE DEVE STARE PRIMA  
APPARTENGONO AD S IN UN ALTRO INSIEME  $\rightarrow$  COME IL  
E SODDISFANO  $f(x)$  E POI PUOI AVERE L'INSIEME PARADISO  
CONTRADDIZIONE  
DI RUSSELL

Dato che è impossibile scrivere l'assiooma per  
ogni predicato, devo scrivere l'assiooma in modo  
informale  $\rightarrow$  E' UNO SCHEMA DI ASSIOMI

Questo assiooma ci dice cose non è un insieme

$\hookrightarrow$  Per trovare gli insiemi dobbiamo vedere dentro  
altri insiemi

• Meglio scrivere: Se  $f$  è un predicato vero, allora:

$$\boxed{\forall x \exists y \forall z (z \in y \leftrightarrow z \in x \wedge f(z))}$$

Oltre l'insieme tutto, per ora, non abbiamo altri insiemi

$\hookrightarrow$  Dobbiamo trovare altri insiemi e un modo per  
farlo è con l'insieme delle parti

#### 4) ASSIOMA DELLE PARTI

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \subseteq x) \rightarrow \text{PER OGNI INSIEME ESISTE  
UN INSIEME DELLE PARTI  
TALE CHE TUTTI GLI ELEMENTI  
DI QUESTO NUOVO INSIEME  
SONO TUTTI E SOLO I  
SOTTOINSIEMI DI } x$$

L'INSIEME DELLE PARTI

$$y \subseteq x : \leftrightarrow \forall z (z \in y \rightarrow z \in x)$$

PER OGNI Z, SE Z  
APPARTIENE A Y ALLORA  
APPARTIENE A X

Grazie a questo assiooma possiamo dire che esiste  
un insieme di tutti i sottinsiemi  $\rightarrow$  POSSIAMO PARLARE  
INOLTRE, DI INSIEME  
PRENDENDO UNA  
PARTE DELL'INSIEME

Per ogni insieme, esiste un solo  
insieme delle parti per X a causa  
dell'assiooma dell'estensionalità

Insieme delle parti di X: = P(X)

$\rightarrow$  DUE INSIEMI DELLE PARTI HANNO COME ELEMENTI GLI STESSI ELEMENTI

## 5) ASSIOMA DELLA COPPIA

$\forall A \exists z \forall u \forall v (u \in z \wedge v \in z \rightarrow (u = x \vee u = y)) \rightarrow$  ESISTE UN  
INSIENE CHE  
DI INSIEMI  
CHE HO, SE  
U E' UGUALE A X  
OPPURE E' UGUALE  
A Y ALLORA  
U APPARTIENE  
A Z  
 $\downarrow$   
 $x \in z \wedge y \in z$ ,  
TUTTI GLI ELEMENTI  
SONO O X O Y

## 6) ASSIOMA DELL'UNIONE

$\forall f \exists a \forall x ((x \in f \wedge y \in f) \rightarrow x \in a)$  → SU ELEMENTI  
DI A SONO GLI  
ELEMENTI DEGLI  
ELEMENTI DI f  
 $\downarrow$   
INSIEME  
UNIONE DI f

→ a insieme famiglia

Insieme unione di f: =  $U_f$

L'insieme unione di f è unico  
per extensionalità

L'unione è unaria (o generalista) perché si  
riferisce a un solo insieme



Definiamo  $\notin$ :

$$\neg(z \in x) : \longleftrightarrow z \notin x$$

## UNICITÀ DEL VUOTO

Per vedere che un insieme è unico, prendo due insiemi vuoti  $x$  e  $y$  e mostro che sono uguali

Siamo  $x = y$  insiemini vuoti  $\rightarrow \forall z(z \in x) \rightarrow \forall z(z \in y)$  → VALS TRUE PER  $z$

Sia  $z \in x \rightarrow$  QUESTA COSE È FALSA PERCHÉ  $x$  NON HA ELEMENTI

↪  $z \in x \rightarrow z \in y$  è valida in ogni caso perché  $z \in x$  è falso  
↪  $z \in y \rightarrow z \in x$  è valida in ogni caso perché  $z \in y$  è falso

Di conseguenza, per la tautologia della doppia implicazione,  
avremo che  $z \in x \leftrightarrow z \in y$   $(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$

↪ Di conseguenza, per l'axioma dell'extensionalità,

$$x = y$$

Visto che l'insieme vuoto è unico, allora per definizione  
d'insieme vuoto:  $= \emptyset$

Consideriamo  $z \in x \rightarrow z \in y$ . Questa cosa è valida per ogni  $z$ :

↪  $\forall z(z \in \emptyset \rightarrow z \in \emptyset)$

↪ Questa scrittura è proprio la definizione di  $\emptyset \subseteq x$

Allora abbiamo dimostrato che  $\emptyset \subseteq \emptyset \Leftarrow$

Consideriamo, invece:

$$\forall x \forall z(z \in \emptyset \rightarrow z \in x)$$

SE PRENDI QUALUNQUE  
ELEMENTO  $z$ , SE  $z$   
APPARTIENE A  $\emptyset$  ALLORA  
APPARTIENE A  $x$  ANCHE A  $x$

• PER DIRE SE È VALIDA ALLORA LA  
FORMULA DEVE ESSERE CHUSA

↪ ALTRIMENTI  
VALIDA O  
MENO NON  
VOGL DIRE  
NULLA

↪ LA FORMULA È VALIDA PERCHÉ  
 $z \in \emptyset$  È FALSO



Quindi il vuoto è sottoinsieme di ogni insieme

↪  $\forall x(\emptyset \subseteq x)$

# UNICITÀ DEL SOTTOINSIEME DELLE PARTI

Sia  $X$  un insieme e siano  $U$  e  $W$  insiemi delle parti di  $X$

Per definizione (l'assioma delle parti):

$$\rightarrow \forall z (z \in U \leftrightarrow z \subseteq X) \quad (\underbrace{zeU \rightarrow z \subseteq X \leftarrow z \in U}_{\text{def}})$$

$$\hookrightarrow \forall z (z \in W \leftrightarrow z \subseteq X) \quad \downarrow \quad \hookrightarrow \forall z (z \in U \leftrightarrow z \in W)$$

Quindi, per l'assioma dell'estensionalità  $U = W$

Insieme delle parti di  $X$ :  $= P(X)$

## PARTI DEL VUOTO

Dobbiamo sapere che elementi ha  $P(\emptyset)$  → POSSO PARLARE DI INSIEME PER ASSIOMA

Prendo un qualunque sottoinsieme del vuoto  $\rightarrow X \subseteq \emptyset$

Per definizione:  $X \subseteq \emptyset : \hookrightarrow \forall z (z \in X \rightarrow z \in \emptyset)$

Visto che  $z \in \emptyset$  è falso, affinché l'affermazione sia valida  
dobbiamo dimostrare che  $z \in X$  sia falso

↪ Dobbiamo dimostrare che  $X$  non ha elementi  $\rightarrow X = \emptyset$

Sappiamo (dall'unicità del vuoto) che  $\emptyset \subseteq \emptyset$  e sappiamo  
(dell'unicità del sottoinsieme delle parti) che questa è  
l'unica parte del vuoto

↪ Di conseguenza  $P(\emptyset)$  è il singleton del vuoto:

$$P(\emptyset) = \{\emptyset\}$$

↪ E' UN INSIEME CHE  
HA COME UNICO  
ELEMENTO IL VUOTO

IL VUOTO, INVECE,  
NON HA ELEMENTI

## ESEMPI:

- Costruiamo l'insieme delle parti della parte del tutto

$$\mathcal{P}(\mathcal{P}(\emptyset))$$

$$\hookrightarrow \text{PER DEFINIZIONE } \mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\})$$

- 1) Tra le  $\mathcal{P}(\mathcal{P}(\emptyset))$  c'è sicuramente  $\emptyset$ , perché  $\emptyset$  è parte di qualunque insieme
- 2) Tra le  $\mathcal{P}(\mathcal{P}(\emptyset))$  c'è anche se stesso, perché ogni insieme è parte di se stesso

Premolo  $x \subseteq \{\emptyset\}$ . Per definizione di sottoinsieme:

$$\forall z(z \in x \rightarrow z \in \{\emptyset\}) \rightarrow \text{Dobbiamo vedere quando queste frasi i solidi}$$

Ci sono due possibilità:

- $x$  potrebbe non avere elementi  $\rightarrow x = \emptyset \hookrightarrow$  LA FRASE RISULTA VALIDA PERCHÉ  $Z \in X$  RISULTA ESSERE FALSO
- $x$  e  $\{\emptyset\}$  hanno gli stessi elementi  $\rightarrow x = \{\emptyset\}$  per estensionalità

$$\text{Quindi } \mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$$

$\hookrightarrow$  IN QUESTO MODO SI HA  $Z \in \{\emptyset\} \rightarrow Z \in \{\emptyset\}$ ,  
QUINTO LA FRASE È VALIDA ANCHE SE  $Z \in \{\emptyset\}$  È VERO

$\hookrightarrow$  IL NUMERO DI ELEMENTI DELLE PARTI DELLE PARTI È ESPONZIALE:  
 $2^m$  DOVE  $m$  È IL NUMERO DI VOLTE CHE SI FA LA PARTE DELLA PARTE DI UN INSIEME

- Inoltre, per l'assioma dell'estensionalità  $\rightarrow$  L'INSIEME COPPIA È UNICO  
 $\{\emptyset, \{\emptyset\}\} = \{\{\emptyset\}, \emptyset\} \rightarrow$  Hanno gli stessi elementi

- Dato un insieme  $f$ :  $f = \{\{a,b\}, \{c,d,e\}\}$

Questo insieme ha due elementi:  $\{a,b\}$  e  $\{c,d,e\}$

Per trovare l'insieme formato da  $f$ , dovrà far parte di

$$U_f = \{a, b, c, d, e\}$$

↪  
INSIEME  
FAMIGLIA

### • PARADOSSO DI RUSSELL

Consideriamo il paradosso di Russell:

$$\{x | \neg(x \in x)\}$$

è un insieme?

Per sconfiggerlo, consideriamo che lo sia.

$$\hookrightarrow r = \{x | \neg(x \in x)\} \rightarrow \text{E' UN INSIEME PER SEPARAZIONE}$$

Questo vuol dire che:  $\forall x (x \in r \leftrightarrow \neg(x \in x))$

$$\forall x (x \in r \leftrightarrow \neg(x \in x)) \rightarrow r \in r \leftrightarrow \neg(r \in r)$$

↪ visto che vale per  
TUTTI GLI INSIEMI, posso  
scrivere che:

Sono giunto ad un errore,  
quindi quelle cose non è  
è un insieme

- Dimostrare che  $\{\alpha\} = \{\alpha, \alpha, \alpha, \alpha\}$

Consideriamo la condizione affinché due insiemi siano uguali per estensionalità

$$\hookrightarrow z \in x \rightarrow z \in y$$

Chiamiamo  $x = \{\alpha\}$

$$y = \{\alpha, \alpha, \alpha, \alpha\}$$

Diciamo due casi:

è valido

1)  $z = \alpha \rightarrow$  In questo caso  $z \in x \rightarrow z \in y$  perché sia  $z \in x$  che  $z \in y$  sono veri

2)  $z \neq \alpha \rightarrow$  Anche in questo caso la formula è valida perché  $z \in x$  è falso  $(F \rightarrow V) = V$

Ne segue che  $\{\alpha\} = \{\alpha, \alpha, \alpha, \alpha\}$  per estensionalità

## ALCUNE TAUTOLOGIE

$$\bullet \forall x (p(x) \wedge q(x)) \leftrightarrow \forall x (p(x) \wedge \forall x (q(x)))$$

$\hookrightarrow$  Questa tautologia non vale se il posto di  $\forall$  mettiamo  $\exists$

$\hookrightarrow$  Non è detto che lo  $x$  che verifica  $\exists x (p(x))$  o

$\exists x (q(x))$  sia lo stesso, quindi non vale il  $\leftrightarrow$

PROPRIETÀ  
DISTINUTTIVA

$$\bullet p \text{ XOR } q \Leftrightarrow (p \wedge \neg q) \vee (q \wedge \neg p) \stackrel{?}{\Leftrightarrow} (p \vee q) \wedge (\neg(p \wedge q))$$

$\hookrightarrow$  ESPANSIONE DI XOR

**SEPARAZIONE:** Sia  $f$  un predicato unario, allora

$\downarrow$  NON POSSO QUANTIFICARE I PREDICATI  $\forall x \exists y \forall z (z \in y \leftrightarrow (z \in X) \wedge f(z))$

**ESTENSIONALITÀ:**  $\forall x \forall y \forall z ((z \in X \leftrightarrow z \in Y) \leftrightarrow x = y)$

**Definizione di " $\subseteq$ :**  $x \subseteq y : \leftrightarrow \forall z (z \in x \rightarrow z \in y)$

**ESEMPIO:**  $\xrightarrow{\substack{\text{e' E' UN SOLO} \\ \text{ELEMENTO}}} \text{IL SINGLETON DI } a$

$$\begin{aligned} P(\{\{\emptyset, \{\emptyset\}\}\}) &= P(\{\{a\}\}) = \{\emptyset, \{a\}\} & a \in \{a\} \\ a &= \{\emptyset, \{\emptyset\}\} = P(P(\emptyset)) & a \notin \{\emptyset\} \end{aligned}$$

Preso l'insieme  $a$ ,  $a$  ha sicuramente il ruolo di l'insieme  $a$  come sottoinsieme

$\xrightarrow{\substack{\text{IL SINGLETON} \\ \text{DI QUELL'UNICO} \\ \text{ELEMENTO}}}$

$$P(a) = \{\emptyset, \{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}\}$$

$$\{\{\emptyset, \{\emptyset\}\}, \{\{\{\emptyset\}\}\} \in P(P(a))$$

LE PARTI DELLE PARTI E' DATO DAL SINGLETON DEI SINGOLI ELEMENTI, GLI INSIEMI VACUO E STESSO E LE VARIE COMBINAZIONI

$\hookrightarrow 2^m$  DOVE  $m$  SONO GLI ELEMENTI

Cerchiamo di tradurre (il linguaggio dei predicati) nel linguaggio degli insiemi

OPERATORI INSIEMISTICI

- ↳ Traduco il  $\leftrightarrow$  con  $\ell = \rightarrow$  Grazie a estensionalità
- ↳ Traduco  $\exists$  con  $\subseteq$  → Grazie alla definizione di  $\subseteq$

Siamo  $X$  e  $Y$  due insiemi qualsiasi

$$\bullet X \cap Y = \{z \mid z \in X \wedge z \in Y\} = \{z \in X \mid z \in Y\}$$

ci troviamo DENTRO  $X$   
↳  $f(z)$

QUESTO E' UN INSIEME PRENDO TUTTI GLI ELEMENTI CHE PER L'ASSIOMA DI SEPARAZIONE → SONO SODDISFAZIONE DEL PREDICATO

$$\bullet X \cup Y = \{z \mid z \in X \vee z \in Y\} \rightarrow$$

LA DEFINIZIONE NON VA BENE

QUESTA DEFINIZIONE NON VA BENE PERCHE' DOBBIAMO DEFINIRE L'AMBIENTE IN QUI PRENDONO GLI ELEMENTI

$$X \cup Y := \bigcup \{X, Y\} \rightarrow$$

IN QUESTO CASO L'AMBIENTE E' STATO GLI ELEMENTI DEGLI ELEMENTI DI QUESTA COPIA

USO ASSIOMA DELLA COPPIA E DELL'UNIONE

Da queste definizioni, segue che  $X \cup Y = \{z \mid z \in X \vee z \in Y\}$

↳ E' DETTO IN MODO INFORMATIVO,  
NON E' LA DEFINIZIONE

$$\bullet X \Delta Y := \{z \in X \cup Y \mid z \in X \text{ XOR } z \in Y\} \rightarrow$$

DIFFERENZA SIMMETRICA

TUTTI GLI ELEMENTI CHE STANNO IN  $X$  O STANNO IN  $Y$  MA NON IN NEI DUE

E' UN INSIEME PERCHE' STANNO GIÀ DENTRO L'UNIONE CHE E' UN INSIEME

USIAMO L'ASSIOMA DI SEPARAZIONE

$$\cdot \exists X := \{z \mid z(z \in X)\}$$



SIMILE AL PARADOSSO  
DI RUSSELL

$$\Rightarrow \{x \mid x \notin x\}$$

Non è un insieme per merito un'assiomma

- Notiamo che da qui segue che la collezione di tutti gli insiemi non è un insieme

↳ DIMOSTRAZIONE:

Sia  $f(x)$  il predicato unario " $\neg(x \in x)$ "

Per assurdo, esiste  $I$  (l'insieme di tutti gli insiemi).

Allora, definisco  $R := \{x \in I \mid f(x)\} \rightarrow$  Per ipotesi,  $R$  è un insieme

ma  $R$  non è un insieme  $\rightarrow$  Si è giunti ad un assurdo

↳ SE LO FOSSE POTREMMO  
DEFINIRE UN INSIEME  
COME IL PARADOSSO DI  
RUSSELL CHE GIÀ SAPPIAMO  
NON POTESSE ESSERE UN  
INSIEME

ASSURDO

Quindi l'insieme  $I$  non esiste

↳ SE ESISTESSE POTREMMO  
DEFINIRE AL SUO  
INTERNO QUALcosa CHE  
NON È UN INSIEME

L'INSIEME UNIVERSALE  
(1) IN REALTA' È  
SOLAMENTE UN INSIEME  
CHE PER CONVENIENZA  
HA TUTTO CIO' DI  
CUI ABBIANO  
BISOGNO PER  
FARE LA MATEMATICA

- Da questo segue che, dato un insieme  $X$

$\{z \mid z(z \in X)\}$  non è un insieme

DI MOSTRAZIONE: ↳

Per assurdo, supponiamo che  $\{z \mid z(z \in X)\}$  è un insieme  
e chiamiamolo  $y$ .

Di conseguenza anche  $U\{X, y\}$  è un insieme

Ma  $U\{X, y\}$  sono tutti gli insiemi che stanno in  $X$  o in  $y$

↳ Quindi sono tutti gli insiemi  $\rightarrow U\{X, y\} =$  INSIEME DI TUTTI GLI INSIEMI

ASSUNTA →  $\{X, y\}$  È UN INSIEME  
POICÒ X E Y LO SONO

CIOÈ NON X

Quindi, l'unico modo per trasdurre il  $\setminus$  è che premolo tutti gli elementi da un altro insieme.

$$Y \setminus X = \{z \in Y \mid z \notin X\} = \{z \mid z \in Y \wedge z \notin X\}$$

SETTAZIONE  
INSIEMISTICA

QUESTO È BENE  
PER CLASSEMENTO DI  
SETTAZIONE

Si legge  $y$  meno  $x$

## OPERAZIONI INSIEMISTICHE DALLE TAUTOLOGIE

Visto che c'è una corrispondenza tra linguaggio insiemistico e linguaggio logico proponiamo a trarre le tautologie

### DOPPIA NEGAZIONE

$$\text{TH: } \forall x, y (y \subseteq x \rightarrow x \setminus (x \setminus y) = y)$$

NEG DI  
 $y \setminus x$   
①  
NEG DELLA  
NEG DI  $x = y$   
②

Dimostrazione:

$$\text{Per definizione, } x \setminus (x \setminus y) = \{z \in x \mid z \notin x \setminus y\} =$$

$$= \{z \in x \mid (z \notin x \setminus y)\} \stackrel{\text{DEF}}{=} \{z \in x \mid \neg(z \in x \wedge z \notin y)\} = \neg\neg \text{ DE MORGAN}$$

$$= \{z \in x \mid z \notin x \vee z \in y\} \stackrel{\text{DEF}}{=} \{z \mid (z \in x) \wedge (z \notin x \vee z \in y)\} = \neg\neg \text{ DE MORGAN}$$

DISTRIBUZIONE  
DI  $\wedge$   
RISPETTO  
A  $\vee$

$$= \{z \mid ((z \in x \wedge z \notin x) \vee (z \in x \wedge z \in y))\} = \text{AFFINNARE LA FORMULA SIA VERA}$$

$\hookrightarrow$  SEMPRE FALSA

$$= \{z \mid z \in x \wedge z \in y\} = y$$

QUESTO È L'INSIEME  
DI TUTTI GLI INSIEMI CHE  
APPARTENGONO A  $x$  E  
APPARTENGONO A  $y$

$z \in x$  È  
SUPERFLUO

$\hookrightarrow$  MA  $y$  È SOTTOINSIEME DI  $x$ ,  
QUINDI SE APPARTENGONO A  $x$  PER  
FORZA APPARTENGONO ANCHE A  $y$

# TERZO ESCLUSO ( $p \vee \neg p$ )

T.H.  $\forall x, y (y \subseteq x \rightarrow y \cup (x \setminus y) = x)$

Dimostrazione

TUTTI GLI Z TALI CHE

$$\{z \mid z \in y \vee z \in x \setminus y\} \stackrel{\text{DEFINIZIONE}}{=} \{z \mid z \in y \vee (z \in x \wedge z \notin y)\} =$$

DISTRIBUITIVITÀ  
DI V RISPETTO  $\rightarrow$  COME FOSSE  
UNA MOLTIPLICAZIONE

$A \wedge$  =  $\{z \mid (z \in y \vee z \in x) \wedge (z \in y \vee \neg(z \in y))\} =$

PER  
ESTENSIONALITÀ

$$= \{z \mid z \in y \vee z \in x\} = x$$

DATO CHE  
 $y \subseteq x$  SE  
 $z \in y$ ,  $z$  DEVE PER  
FORZA APPARTENERE  $\rightarrow z \in y$   
ANCHE AD  $x$  SUPERFLUO

GEO INSIEMI CHE  
APPARTENGONO A  
ALL'UNO SONO ALTRI

DEFINIZIONE

TAUTOLOGIA DEL TERZO ESCLUSO ( $p \equiv p \vee q$ )

DATO CHE QUESTA  
SECONDA PARTE È  
UNA TAUTOLOGIA,  
È SUPERFLUA  
PERCHÉ SE LA  
PRIMA PARTE È VERA  
ALLORA TUTTO È  
VERO, SE LA PRIMA  
PARTE È FALSA  
ALLORA TUTTO È  
FALSO

# DOPPIA INCLUSIONE ( $(p \subseteq q) \leftrightarrow (p \rightarrow q \wedge q \rightarrow p)$ )

T.H.  $\forall x, y (x = y \leftrightarrow x \subseteq y \wedge y \subseteq x)$

Dimostrazione

Ricordiamo la tautologia:

$$\forall x (p(x) \wedge q(x)) \leftrightarrow \forall x (p(x)) \wedge \forall x (q(x))$$

PER  
ESTENSIONALITÀ

$$x = y \leftrightarrow \forall z (z \in x \leftrightarrow z \in y) \leftrightarrow$$

TAUTOLOGIA  
DELLA DOPPIA  
IMPLICAZIONE

$$\leftrightarrow \forall z ((z \in x \rightarrow z \in y) \wedge (z \in y \rightarrow z \in x)) \leftrightarrow$$

$$\leftrightarrow \forall z (z \in x \rightarrow z \in y) \wedge \forall z (z \in y \rightarrow z \in x) \leftrightarrow$$

SONO PROPRIAMENTE LA  
DEFINIZIONE DI  
INCLUSIONE

$$\leftrightarrow x \subseteq y \wedge y \subseteq x$$

NON CONTRADDIZIONE  $\neg(p \vee \neg q) \rightarrow (\neg p \wedge q)$

T.H:  $\forall x, y (y \cap x \setminus y = \emptyset)$

DIMOSTRAZIONE  
NEGLI ESERCIZI  
DEL 13/10/2014

IDEMPOTENZA DI  $\cap$   $(p \cap p) \leftrightarrow p$

T.H:  $\forall x (x \cap x = x)$

IDEMPOTENZA DI  $\cup$   $(p \cup p) \leftrightarrow p$

T.H:  $\forall x (x \cup x = x)$

IDEMPOTENZA DI  $\Delta$

T.H:  $\forall x (x \Delta x = \emptyset)$

ASSOCIAZIVITÀ DI  $\cap$   $(p \cap q) \cap r \leftrightarrow p \cap (q \cap r)$

T.H:  $\forall x, y, z ((x \cap y) \cap z = x \cap (y \cap z))$

ASSOCIAZIVITÀ DI  $\cup$   $(p \cup q) \cup r \leftrightarrow p \cup (q \cup r)$

T.H:  $\forall x, y, z ((x \cup y) \cup z = x \cup (y \cup z))$

ASSOCIAZIVITÀ DI  $\Delta$   $(p \Delta q) \Delta r \leftrightarrow p \Delta (q \Delta r)$

T.H:  $\forall x, y, z ((x \Delta y) \Delta z = x \Delta (y \Delta z))$

COMMUTATIVITÀ DI  $\cap$   $(p \cap q) \leftrightarrow (q \cap p)$

T.H:  $\forall x, y ((x \cap y) = (y \cap x))$

COMMUTATIVITÀ DI  $\cup$   $(p \cup q) \leftrightarrow (q \cup p)$

T.H:  $\forall x, y ((x \cup y) = (y \cup x))$

COMMUTATIVITA' DI  $\Delta$   $(p \text{ XOR } q) \leftrightarrow (q \text{ XOR } p)$

T.H:  $\forall x, y ((x \Delta y) = (y \Delta x))$

DISTRIBUTIVITA' DI  $\cap$  RISPETTO A  $\cup$

$$(p \wedge (q \vee r)) \leftrightarrow ((p \wedge q) \vee (p \wedge r))$$

T.H:  $\forall x, y, z (x \cap (y \cup z) = ((x \cap y) \cup (x \cap z)))$

DISTRIBUTIVITA' DI  $\cup$  RISPETTO A  $\cap$

$$(p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge (p \vee r))$$

T.H:  $\forall x, y, z (x \cup (y \cap z) = (x \cup y) \cap (x \cup z))$

ESPLICAZIONE DI  $\Delta$

$$(\text{p XOR q}) \leftrightarrow ((\text{p} \wedge \neg \text{q}) \vee (\text{q} \wedge \neg \text{p})) \leftrightarrow (\text{p} \vee \text{q}) \wedge (\neg (\text{p} \wedge \text{q}))$$

T.H:  $\forall x, y (x \Delta y = (x \cup y) \setminus (x \cap y))$

LEGGI DI DE MORGAN

$$\neg (\text{p} \wedge \text{q}) \leftrightarrow (\neg \text{p} \vee \neg \text{q})$$

$$\neg (\text{p} \vee \text{q}) \leftrightarrow (\neg \text{p} \wedge \neg \text{q})$$

T.H:  $\forall x, y, z ((x \setminus (y \cap z)) = ((x \setminus y) \cup (x \setminus z)))$

T.H:  $\forall x, y, z ((x \setminus (y \cup z)) = ((x \setminus y) \cap (x \setminus z)))$

# CONSIDERAZIONI SULL'ASSIOMA DELL'UNIONE

d'assioma dell'unione è:

$$\forall A \forall X \forall Y ((X \in Y \wedge Y \in A) \rightarrow X \in A)$$

$\forall A \forall X$  non può essere riscritto come  $\forall X \forall A$  perché non esiste una commutatività del  $A$   $\rightarrow$  SE UN'OCCE DI PRENDERE  $X$  CHE STA DENTRO  $Y$  CHE STA DENTRO  $A$  PRENDO  $Y$  CHE STA DENTRO  $X$  E  $Y$  CHE STA DENTRO  $A$  STO PRENDENDO QUALcosa DI SIMILE ALL'INTERSEZIONE

↓  
E' possibile scrivere l'assioma dell'unione con  $\exists$  in modo che sia un po' più agevole e chiaro da capire  $\rightarrow$  SCRITTURA LOGIAMENTE EQUIVALENTE

$$f = \{ \{1, 2, 3\}, \{4\} \}$$

$x$        $y$   
  \  /  
 $\exists y (x \in y \wedge y \in f)$

$$\forall g \exists a \forall x (x \in a \leftrightarrow \exists y (x \in y \wedge y \in g))$$

↳ POSSO SCRIVERE  $\rightarrow U_g := \{x \in a \mid \exists y (x \in y \wedge y \in g)\}$   
PER ESTENSIONALITÀ

↳ HO UNA  
FORMULA  
CHIUSA PER  
L'UNIONE UNARIA

## INTERSEZIONE UNARIA

Sia  $f$  un insieme,

$$U_f := \{x \in U_f \mid \forall y (y \in f \rightarrow x \in y)\}$$

E' SEMPRE PIÙ  
GRANDE DELL'UN

TUTTI GLI  $x$  CHE APPARTENGONO ALL'UNIONE UNARIA TUTTI CHE SE  $y$  APPARTIENE AD  $f$  ALLORA  $x$  APPARTIENE A  $y$

## ESEMPIO:

$$f = \{\{1, 2, 3\}, \{4\}, \{3\}\}$$

NESSUN  $x$   
SODDISFA TUTTE LE CONDIZIONI

$$U_f = \{x \in \{1, 2, 3, 4\} \mid \forall y (y \in f \rightarrow x \in y)\} = \emptyset$$

↳ AD ESEMPIO,  $\rightarrow$  OGNI  $y$  (CIOÈ  $\{1, 2, 3\}$ )  $\rightarrow$  DEVE ESSERE VERO PER  
PRENDIAMO 1 SE  $y \in f$  ALLORA  $1 \in y$ ? SI

QUESTO RAGIONAMENTO PER  $\{4\} \in \{3\}$ ,  $\rightarrow$  1  $\notin$  4, QUINDI  $\{4\}$  NON FA PARTE DI  $U_f$

$$\begin{aligned} \cdot & f = \{\{1, 2\}, \{1\}\} \\ \cap f &= \{1\} \end{aligned}$$

- Se prendo  $f = \emptyset$  dovrà sempre agire nello spazio di  $\cup f$  → Se prendessi tutti gli  $x$  non definire che  $x \in \cup f$ , l'intersezione unaria del tutto risulterebbe essere tutti gli insiemi perché  $\forall y (y \in f \rightarrow x \in y)$  risulta sempre vera

$$\cup \emptyset = \emptyset$$

$$\text{Quindi } \cap \emptyset = \emptyset$$

- $\cap \{x, y\} = x \cap y \rightarrow$  d'intersezione unaria delle copie  $x, y$  è l'intersezione tra  $x$  e  $y$

## DIAGRAMMI DI VENN

I diagrammi di Venn sono un modo per visualizzare concretamente gli insiemi e le operazioni insiemistiche

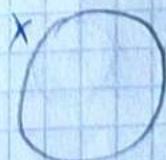
↳ E' un modo informare per verificare le proprietà degli insiemi

Per disegnare gli insiemi (consideriamo  $m$  insiemi) dovranno disegnare  $m$  cerchi in modo da rappresentare tutte le intersezioni possibili

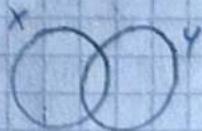
↳ I DIAGRAMMI DI EULER-VENN COMPRENDONO ANCHE GLI INSIEMI CHE NON FANNO PARTE DELLE INTERSEZIONI → DIAGRAMMI ESTERNI

AD ESEMPIO:

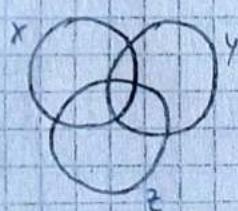
• Un insieme



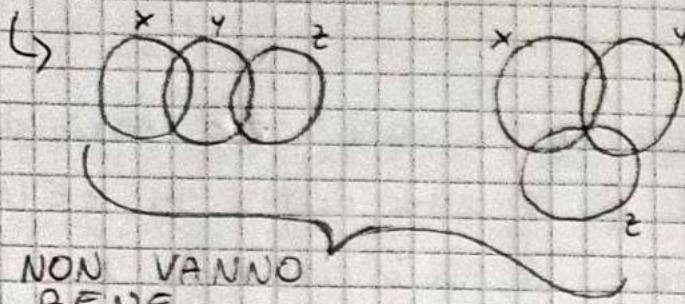
• Due insiemi



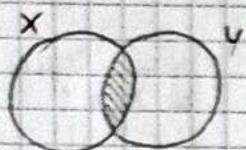
• Tre insiemi



Non è detto che ci sia qualcosa nell'intersezione, ma devo comunque contenerla



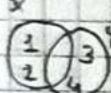
$X \cap Y$



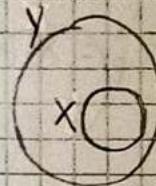
AD ESEMPIO:

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

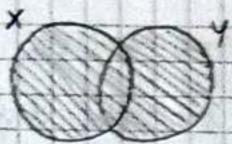
$$Y = \{3, 4\}$$



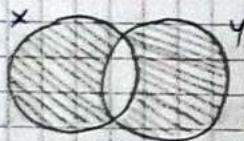
$X \subset Y$



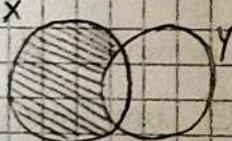
$X \cup Y$



$X \Delta Y$



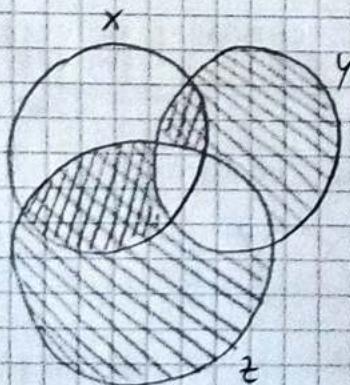
$X \setminus Y$



LA DIFFERENZA SIMMETRICA È L'UNIONE MENO L'INTERSEZIONE

ESEMPIO:

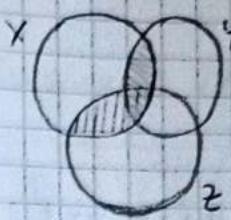
$$\bullet X \cap (Y \Delta Z)$$



$$\diagup \diagdown = Y \Delta Z$$

$$\diagup \diagdown = X \cap (Y \Delta Z)$$

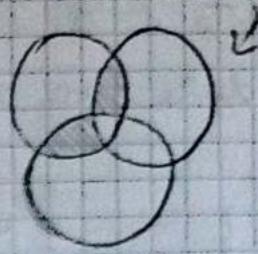
$$\cdot (x \cap y) \Delta (x \cap z)$$



$$= x \cap y$$

$$= x \cap z$$

$$(x \cap y) \Delta (x \cap z)$$



Notiamo che il diagramma di  $x \cap (y \Delta z)$  è lo stesso di  $(x \cap y) \Delta (x \cap z)$

↳ Abbiamo dimostrato in modo informale la distributività di intersezione rispetto a differenza simmetrica

<sup>y</sup> PIÙ IMMEDIATO  
DA VEDERE

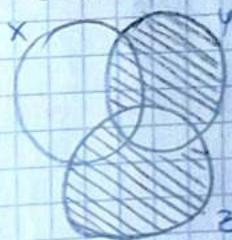
• Possiamo provare a vedere se vale la distributività di unione rispetto a differenza simmetrica

↳ Se è vero avrò questa dimostrazione grafica

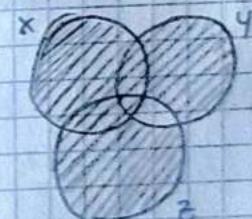
↳ Se non è vero allora posso fornire un controesempio

$$x \cup (y \Delta z)$$

$$y \Delta z$$



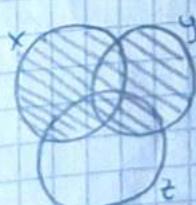
$$x \cup (y \Delta z)$$



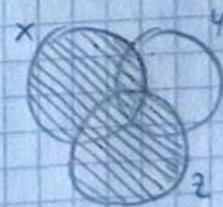
SONO  
DIVERSI

$$(x \cup y) \Delta (x \cup z)$$

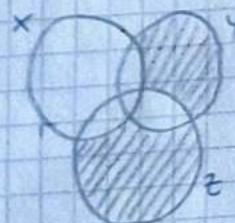
$$x \cup y$$



$$x \cup z$$



$$(x \cup y) \Delta (x \cup z)$$



Notiamo dai diagrammi che non vale la distributività  
di  $\cup$  rispetto a  $\Delta$

↳ Posso dare un esempio di tre insiemi che mostrano ciò  
 $\downarrow$

$$X = \{0, 1\}$$

$$Y \Delta Z = \{1, 2, 3\}$$

$$X \cup (Y \Delta Z) = \{0, 1, 2, 3\}$$

$$Y = \{1, 2\}$$

$$X \cup Y = \{0, 1, 2\} \rightarrow (X \cup Y) \Delta (X \cup Z)$$

→ DIVERSI

$$Z = \{3\}$$

$$X \cup Z = \{0, 1, 3\} \rightarrow \{0, 1, 2\} \Delta \{0, 1, 3\} = \{2, 3\}$$

Questo metodo è tenissimo per trovare insiemi  
concreti per dimostrare che non vale un'uguaglianza

↳ E' un modo informale

# CONTINUO DELLA TEORIA DEGLI INSIEMI

## DEFINIZIONE DELLA COPPIA ORDINATA

Siamo  $x, y$  insiemi

$$(x, y) \stackrel{\text{DEF}}{=} \{\{x\}, \{x, y\}\} \rightarrow \begin{array}{l} \text{NON SAPPIAMO} \\ \text{CHE VALGIA L'ORDINE} \end{array}$$

Cioè che vogliamo delle coppie ordinate è che valga l'ordine  $\rightarrow$  cioè  $(x, y)$  è diverso da  $(y, x)$

↳ Per dire ciò serviranno:

$$\boxed{x \neq y \rightarrow (x, y) \neq (y, x)} \rightarrow \begin{array}{l} \text{DOBBIANO SPECIFICARE} \\ \text{CHE } x \neq y \text{ PERCHÉ È} \\ \text{NORMALE CHE } (x, x) = (x, x) \end{array}$$

## CARATTERIZZAZIONE DELLE COPPIE ORDINATE



## DIMOSTRAZIONE DELLA CARATTERIZZAZIONE DELLE COPPIE ORDINATE

T.H:  $x \neq y \leftrightarrow (x, y) \neq (y, x)$

DIM

Sappiamo dalle tautologie che  $(p \leftrightarrow q) \leftrightarrow (\neg p \leftrightarrow \neg q)$

P posso dimostrare equivalentemente che:

$$x = y \leftrightarrow (x, y) = (y, x)$$

$$\rightarrow (p \leftrightarrow q) \leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$$

P posso sfruttare le tautologie delle doppie implicazione e dimostrare l'uguaglianza prima in un senso e poi nell'altro

LA

PRIMA  
CONDIZIONE  $(\rightarrow)$

SI CHIAMA  
NECESSARIA

IPOTESI

Sia  $x = y \rightarrow$

$$(x, y) \stackrel{\text{DEF}}{=} \{\{x\}, \{x, y\}\} \stackrel{\text{ESTR}}{=} \{\{x\}, \{x\}\}$$

↓  
IMPLICAZIONE  
NECESSARIA

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

SONO  
UGUALI

( $\Leftarrow$ ) Per ipotesi:

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

Dovono essere gli stessi elementi, quindi ho due ipotesi:  
↓

$$\{x\} = \{y\}$$

∨

$$\{x\} = \{y, x\}$$

→ CHE POI È USUALE

$\{x, y\}$  PERCHÉ È UNA COPPIA NON ORDINATA

SONO UGUALI  
'SCIA' HANNO GLI STESSI ELEMENTI

Dato che questi due insiemi sono uguali dovranno essere gli stessi elementi

$$x = y$$

Se è vero questo allora  $y$  deve essere un elemento di  $\{x\}$ , di conseguenza

↓

$$y = x \xrightarrow{\text{così}} \{y, x\} = \{x\}$$

Di conseguenza  $x = y$  è vero sempre  
↳ QUINDI SE  $x \neq y$  ALLORA  $(x, y) \neq (y, x)$

## DEFINIZIONE DELLA TERNA ORDINATA

$$(x, y, z) := ((x, y), z)$$

se si tiene  
ORDINATA SARÀ →  $(x, y, z, t) := ((x, y, z), t)$   
COSÌ VIA

## PRODOTTO CARTESIANO

Il prodotto cartesiano è l'insieme di tutte le copie ordinate di due insiemi

↳ AD ESEMPIO:

$$a = \{0, 1\}$$

$$b = \{1, 2\}$$

$$a \times b = \{(0, 1), (0, 2), (1, 1), (1, 2)\}$$

PRODOTTO  
CARTESIANO  
DI A PER B

# DEFINIZIONE DI PRODOTTO CARTESIANO

- Siamo  $a$  e  $b$  due insiemi, si dice prodotto cartesiano di due insiemi:

$$a \times b := \{ z \in P(P(a \cup b)) \mid \exists x \exists y (x \in a \wedge y \in b \wedge z = (x, y)) \}$$

$\downarrow$   
 $z$  è composto  
dagli elementi  
di  $a$  e  $b$

$\hookrightarrow$  TUTTI gli  $z$  si  
TROVANO NELLE  
PARTI DELLE PARTI  
 $a \cup b$  → AD ESEMPIO:

Se ho:

$$a = \{0, 1\}$$

$$b = \{2, 3\}$$

$$a \cup b = \{0, 1, 2\}$$

$$P(a \cup b) = \{\{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}, \{\}\}$$

$$P(P(a \cup b)) = \{\{\{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}, \{\}\}\}$$

- Se  $a$  ha  $m$  elementi

e  $b$  ha  $n$  elementi,

$a \times b$  avrà  $m \cdot n$  elementi

$$\underbrace{a \times b \times c} = (a \times b) \times c$$

FORMA LE  
TERNE ORDINATE

15/10/2021 (LEZIONE 09)

Correzione esercizi

PERCHÉ SI HABIA QUESTO  
QUESTO È X ALLORA Y DEVE ESSERE PROPRIO X

$$3) \cap \{x\} = \{z \in \bigcup \{x\} \mid \forall y (y \in \{x\} \rightarrow z \in y)\} =$$

QUANTE Y CI SONO CHE SONO PROPRIO X → SOLO X

$$= \{z \in X \mid \forall y (y = x \rightarrow z \in y)\} = \text{SE Y È PROPRIO X ALLORA Z È X}$$

$$= \{z \in X \mid z \in x\} = X$$

$$U\{x\} = \{z \mid \exists y (z \in y \wedge y \in \{x\})\} = \text{Y DEVE ESSERE PROPRIO X PERCHE' E' SOLO X NEI \{X\}}$$

$$= \{z \mid \exists y (z \in y \wedge y = x)\} = \text{QUELLA Y CHE ESISTE E' PROPRIO X}$$

$$= \{z \mid z \in x\} = X \rightarrow \text{L'INSIEME DI TUTTI GLI ELEMENTI CHE APPARTENGONO A X}$$

# PROPRIETÀ CARATTERISTICA DELLE TERNE ORDINATE

$$(\forall x, y, z, x_1, y_1, z_1) ((x, y, z) = (x_1, y_1, z_1) \Leftrightarrow (x = x_1 \wedge y = y_1 \wedge z = z_1))$$

DIM

$$\text{Sia } x = x_1 \wedge y = y_1 \wedge z = z_1$$

$$(x, y, z) \stackrel{\text{DEF}}{=} ((x, y), z) \stackrel{\text{DEF}}{=} \{\{(x, y)\}, \{(x, y), z\}\} \stackrel{\text{DEF}}{=} \\ \stackrel{\text{DEF}}{=} \{\{\{\{x\}, \{x, y\}\}\}, \{\{\{x\}, \{x, y\}\}, z\}\}$$

$$(x_1, y_1, z_1) \stackrel{\text{DEF}}{=} ((x_1, y_1), z_1) \stackrel{\text{DEF}}{=} \{\{(x_1, y_1)\}, \{(x_1, y_1), z_1\}\} \stackrel{\text{DEF}}{=} \\ \stackrel{\text{DEF}}{=} \{\{\{\{x_1\}, \{x_1, y_1\}\}\}, \{\{\{x_1\}, \{x_1, y_1\}\}, z_1\}\}$$

Per ipotesi, visto che  $x = x_1 \wedge y = y_1 \wedge z = z_1$ , possiamo scrivere:

$$(x_1, y_1, z_1) = \{\{\{\{x\}, \{x, y\}\}\}, \{\{\{x\}, \{x, y\}\}, z\}\} \text{ che per} \\ \text{estensionalità è proprio } (x, y, z)$$

Per ipotesi  $(x, y, z) = (x_1, y_1, z_1)$ , di conseguenza

$$\{\{\{\{x\}, \{x, y\}\}\}, \{\{\{x\}, \{x, y\}\}, z\}\} = \{\{\{\{x_1\}, \{x_1, y_1\}\}\}, \{\{\{x_1\}, \{x_1, y_1\}\}, z_1\}\}$$

Affinché ciò sia vero, allora:

$$\{\{\{\{x\}, \{x, y\}\}, z\} = \{\{\{\{x_1\}, \{x_1, y_1\}\}\}\} \vee$$

$$\{\{\{\{x\}, \{x, y\}\}, z\} = \{\{\{\{x_1\}, \{x_1, y_1\}\}\}, z_1\}$$

E ciò può essere vero solo nel caso in cui  $z = z_1$  e

$$\{\{\{x\}, \{x, y\}\} = \{\{\{x_1\}, \{x_1, y_1\}\}\} \text{ cioè quando } x = x_1 \wedge y = y_1$$

## Corrispondenze tra insiemi

Siamo  $a$  e  $b$  insiemi e sia  $g$  un sottoinsieme del prodotto cartesiano di  $a$  in  $b$

$$\hookrightarrow g \subseteq a \times b$$

Le coppie  $(a \times b, g)$  si dice corrispondenza tra  $a$  e  $b$

con grafico  $g$  → vogliano collegare gli elementi di  $a$  e gli elementi di  $b$  in qualche modo  
(CHIAMIAMO LA CORRISPONDENZA "P")

$$P = (a \times b, g) \text{ e siamo } c \in a \text{ e } d \in b$$

→  $P_0$

Per definizione:

$$c P d : \Leftrightarrow (c, d) \in g \rightarrow \text{LA COPPIA } c, d \text{ APPARTIENE AL GRAFICO DI } P$$

c e d sono in relazione (o in corrispondenza)  $P$   
tra loro

↪ UN ESEMPIO DI CORRISPONDENZA E "APPARTENENZA" OPPURE "MINORE O UGUALE"

### ESEMPIO:

$$a = \{0, 1\} \quad b = \{1, 2\}$$

$$P = (a \times b, g)$$

$$g = \{(0, 1), (0, 2), (1, 1), (1, 2)\}$$

↪  $g$  è arbitrario, posso mettere quello che voglio (ovviamente però  $g \subseteq a \times b$ )  
↪ C'è ne sono alcuni speciali

Penso chiedermi: È vero che  $1 \leq 1$ ? → cioè, la coppia  $(1, 1)$  appartiene a  $g$ ?

$$a = \{0, 1\} \quad b = \{1\}$$

$$P_1 = (a \times b, g_1)$$

$$g_1 = \{(0, 1)\}$$

0  $\leq 1$ ? Si

3  $\leq 1$ ? No

→ sto considerando ancora la relazione  $\leq$

↪ RICOPRA IL GRAFICO DEL  $\leq$ , QUINDI E' COME SE MI STESSI CHIUDERDO:  
 $1 \leq 1$ ? SI

Quindi, ad esempio:

$$\leq = (\mathbb{N} \times \mathbb{N}, g) \quad \text{Dove } g \text{ è infinito}$$

→ IL PRIMO E' SEMPRE MINORE O UGUALE DEL SECONDO

$$g = \{(0,0), (0,1), (1,0), (0,2), (1,1), (2,0), (0,3), (1,2), (2,1), \dots\}$$

3 è in relazione "minore uguale" con 2?

↪ 3 ≤ 2? No

## VISUALIZZIAMO LA RELAZIONE

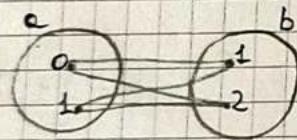
Possiamo descrivere una relazione in vari modi, elencando il grafico

$$\cdot a = \{0, 1\} \quad b = \{1, 2\} \quad P = (a \times b, g) \quad g = \{(0,1), (0,2), (1,1), (1,2)\}$$

TABELLA (ELEMENTI DI a)

| P | 1   2 |   |
|---|-------|---|
|   | 0     | x |
| 0 | x     | x |
| 1 | x     | x |

CON LE LINEE



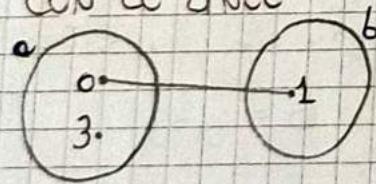
IN QUESTO CASO g È TUTTO IL PRODOTTO CARTESIANO

$$\cdot a = \{0, 3\} \quad b = \{1\} \quad P_1 = (a \times b, g_1) \quad g_1 = \{(0,1)\}$$

TABELLA

| P_1 | 1 |   |
|-----|---|---|
|     | 0 | x |
| 3   | 0 |   |

CON LE LINEE



Possiamo descrivere una relazione in modo concreto con la proprietà del grafico

$$\cdot P = (\mathbb{N} \times \mathbb{N}, g) \text{ mpm}$$

$$(\forall m, n \in \mathbb{N}) ((m, n) \in g \leftrightarrow m \leq n + 1)$$

•  $(0, 5) \in g$ ? No

•  $2 \in P$ ? Si

può essere utile quando g è infinito e ha tanti elementi

RELAZIONE BINARIA  $\rightarrow$  UNA CORRISPONDENZA INTERNA AD UN INSIEME  
 Una corrispondenza tra  $a$  e  $a$  (Sia  $a$  un insieme)  
 si dice relazione binaria  
 $\hookrightarrow (a \times a, g)$

COSA NON È UNA CORRISPONDENZA?

Ad esempio:

$$a = \{0, 3\} \quad b = \{1\} \quad P_1 = (a \times b, g_1) \quad g_1 = \{(0, 1), (0, 3)\}$$

Non è una corrispondenza perché  $g_1 \not\subseteq a \times b$

## L'INSIEME DELLE CORRISPONDENZE

- $\text{CORR}(a, b)$  è l'insieme delle corrispondenze fra  $a$  e  $b$
- $\text{REL}(a) = \text{CORR}(a, a)$  è l'insieme delle relazioni binarie

LE FUNZIONI  $\rightarrow$  LE FUNZIONI SONO PARTICOLARI CORRISPONDENZE

Siamo  $a$  e  $b$  insiemi e sia  $f = (a \times b, g)$  con  
 $g \subseteq a \times b$ .

$\hookrightarrow f$  È UNA CORRISPONDENZA DI  $a$  PER  $b$

$f$  si dice funzione o applicazione tra  $a$  e  $b$

$$\text{se: } (\forall x \in a)(\exists! y \in b)(x f y)$$

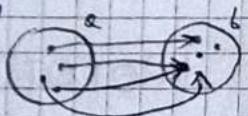
$\hookrightarrow f$  è una funzione se ad ogni elemento di  $a$  è associato uno ed un solo elemento di  $b$

$\hookrightarrow$  SE IN  $a$  C'È UN SOLO ELEMENTO  
 NON ASSOCIAZIONE ALLORA  $f$  NON È UNA FUNZIONE

UN ELEMENTO DI  
 $b$  PUÒ ESSERE  
 ASSOCIAZIONE A PIÙ  
 DI UN ELEMENTO  
 DI  $a$  MA UN  
 ELEMENTO DI  $a$   
 NON PUÒ ESSERE  
 ASSOCIAZIONE A  
 PIÙ ELEMENTI DI  $b$

$$f: a \rightarrow b$$

$\hookrightarrow f$  È UNA FUNZIONE CHE  
 VA DA  $a$  A  $b$



ATTENZIONE:

$g$  non è la funzione, è il grafico delle funzione

a si dice dominio di  $f$

b si dice codominio di  $f$

Se  $(x, y) \in g$ , scrivo  $y = f(x)$  → SE MI VIENE CHIESTA COS'E' IL GRAFICO DELLA FUNZIONE NON POSSO DIRE CHE E' L'INSIEME DELLE COPIE ORDINATE  $x, y$

DEVO PERTA DIRE CHE E' UN SOTTOINSIEME DI  $a \times b$

## IMMAGINE DI $f$

$$\text{Im } f = \{ y \in b \mid (\exists x \in a)(f(x) = y) \} = \{ f(x) \mid x \in a \}$$

↳ E' UN SOTTOINSIEME DEL CODOMINIO

↓  
ESISTE UN CERTO  $x$  TALE CHE LA COPIA  $x, y$  STA NEL GRAFICO

NOTAZIONE ALTERNATIVA

↑  
SOTTINTENDO CHE  $f(x) \in b$

↳ PER SCRIVERE PIU' VELOCEMENTE

## DESCRIZIONE ESPlicita DI UNA FUNZIONE

MAPS TO,  
ASSOCIA

$$f: x \in a \mapsto f(x) \in b$$

DESCRIZIONE ESPlicita DI UNA FUNZIONE

↳ SI POSSONO SCRIVERE COSE MOLTO COMPLESSE →

IN MODO SEMPLICE

↳ A VOLTE PUO' ESSERE DIFFICILE DA SCRIVERE MA COSI LO CAPISCE SUBITO

AD ESEMPIO:

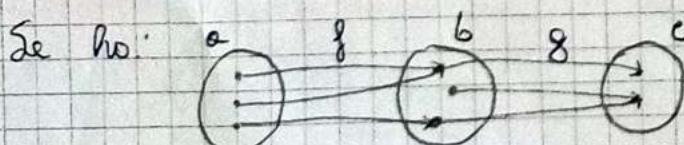
$$f: x \in \mathbb{N} \mapsto x+1 \in \mathbb{N} \rightarrow f \text{ SARÀ } \{(0, 1), (1, 2), (2, 3), (3, 4) \dots\}$$

"Una corrispondenza tra due insiemi  $a$  e  $b$  si dice funzione ben posta se è una funzione"

↳ DEFINIZIONE INFORMATIVA, COLLOQUIALE

↳ TALVOLTA DELLE COSE SEMBRIANO FUNZIONI MA NON LO SONO

## PRODOTTO RELAZIONALE (o TRA CORRISPONDENZE)



↳ E IOE' LA COMPOSIZIONE DI UN PUNTO DI VISTA DELLE RELAZIONI

Siamo  $a, b, c, d$  insiemi e siamo  $\rho = (a \times b, g_1)$ ,  $\sigma = (c \times d, g_2)$  corrispondenze

Definisco  $P^r = (\alpha \times \delta, g_3)$  con  $g_3$  definita con queste proprietà:

$$(\forall x \in \alpha)(\forall y \in \delta)((x, y) \in g_3 \leftrightarrow \exists z ((x, z) \in g_1 \wedge (z, y) \in g_2))$$

Il prodotto relazionale è associativo

↳ c'è un elemento  
in mezzo che  
collega le due  
relazioni

$z$  si  
trova  
sia in  
 $b$  che  
in  $c$   
perché  
deve  
appartenere  
alla coppia  
 $(x, z) \in g_1$   
 $\wedge (z, y) \in g_2$

ESEMPI:

- $U =$  Insieme degli esseri umani

$$P = (U \times U, g_1)$$

$$x P y \leftrightarrow x \text{ è padre di } y$$

↳ cioè "la coppia  $x, y$  STA NEL GRAFICO"

$$O = (U \times U, g_2)$$

$$(x, y) \in g_2 \leftrightarrow x \text{ è fratello di } y$$

$$P^2 = P P \quad x P^2 y \leftrightarrow \exists z (x P z \wedge z P y)$$

$$\hookrightarrow x P^2 y \leftrightarrow x \text{ è nonno di } y$$

$$P^r = P \quad x P^r y \leftrightarrow \exists z (x P z \wedge z P y)$$

$x$  è il padre del fratello di  $y$

$$O P = x \text{ è lo zio di } y$$

- $\subseteq$  in  $P(N)$   $\rightarrow \subseteq$  è una relazione binaria  
quindi ho bisogno delle  $P(N)$

$$x \subseteq^2 y \leftrightarrow \exists z (x \subseteq z \wedge z \subseteq y) \leftrightarrow x \subseteq y \rightarrow \text{TRANSITIVITÀ DELL'INCLUSIONE}$$

↳ l'inclusione quadrata  
è uguale all'inclusione

•  $f: m \in \mathbb{N} \rightarrow m+1 \in \mathbb{N} \rightarrow$  QUESTA E' PROPRIO  
 $\sigma = \leq$  SU  $\mathbb{N}$  UNA FUNZIONE

$$m \text{ PO' } m \leftrightarrow \exists z (m \neq z \wedge z \sigma m) \leftrightarrow \exists z (m+1 = z \wedge z \leq m)$$

$\downarrow$

$\begin{array}{l} z \text{ E' IL} \\ \text{ SUCCESSIVO} \\ \text{ DI } m \end{array}$        $\begin{array}{l} z \text{ E' MINORE} \\ \text{ O UGUALE} \\ \text{ DI } m \end{array}$        $\begin{array}{l} \text{E' COME} \\ \text{ DIRE } m < m \end{array}$

AD ESEMPIO:

3 PO' 4? Si

2 PO' 4? Si

4 PO' 4? No

Corso esercizi 20/10/2021 (LEZIONE 10)

(G STAMPA UNA COPIA DEI ELEMENTI IN OGNI ELEMENTO)

4) VIII.  $P = (\mathbb{P}_2(\mathbb{N}) \times \mathbb{N}, (g))$  LA PROPRIETÀ CHE DEFINISCE  $g$

$$(\forall \{a, b\} \in \mathbb{P}_2(\mathbb{N})) (\forall m \in \mathbb{N}) ((\{a, b\}, m) \in g \Leftrightarrow a^b = m)$$

$$P: \{a, b\} \in \mathbb{P}_2(\mathbb{N}) \mapsto a^b \in \mathbb{N}$$

$\{2, 3\} \in P$  ? Si

Non è una funzione perché a uno stesso insieme

$\{3, 2\} \in P$  ? Si

elemento  $m$  associa due diversi

FUNCTIONE COMPOSTA → DA DUE FUNZIONI E' ANCORA UNA FUNZIONE

$$f: a \rightarrow b, g: b \rightarrow c$$

PRODOTTO RELAZIONALE

Definisce  $g \circ f = \begin{cases} f \\ g \end{cases}$  (COMPOSTA DI  $f$  E  $g$ )

descrizione esplicita

$$g \circ f: x \in a \mapsto g(f(x)) \in c$$

VISTO CHE  $f$  È UNA FUNZIONE (1-1)

VISTO CHE  $g$  È UNA FUNZIONE (1-1)

VISTO CHE  $g$  È UNA FUNZIONE (1-1)

FUNCTIONE IMMERSIONE DI  $a$  IN  $b$

Se  $a \subseteq b$ , la funzione  $g: x \in a \mapsto x \in b$  (IMMERSIONE)

↪ L'ELEMENTO  $x$  DI  $a$  LO VAI A VEDERE DENTRO  $b$  MA E' SEMPRE OLTRELL'ELEMENTO  $x$

FUNCTIONE IDENTITÀ DI  $a$

$Id_a: x \in a \mapsto x \in a$  (IDENTITÀ DI  $a$ )

↪ AD  $x$  ASSOCIO LO STESSO  $x$  ED E' SEMPRE APPARTENENTE AD  $a$

FUNCTIONE RESTRIZIONE DI  $f$  AD  $S$

Sia  $S \subseteq a$ ,  $f|_S: x \in S \mapsto f(x) \in b$  (RESTRIZIONE DI  $f$  AD  $S$ )

ESEMPIO:

$$f: x \in \mathbb{Z} \rightarrow x+1 \in \mathbb{Z}$$

RESTRIZIONE SU DOMINIO

↓  
VIGNE TRASPORTATA  
E INIEKTIVITÀ

$$f|_{\mathbb{N}}: x \in \mathbb{N} \rightarrow x+1 \in \mathbb{Z}$$

## FUNZIONE PROLUNGAMENTO DI $f$

$g: b \rightarrow c$  si dice prolungamento di  $f$  su  $b$ :

$$\exists s \subseteq b: g|_s = f$$

↳ E' IL CONTRARIO  
DELLA RESTRIZIONE

↓  
ALLARGHIANO  
IL DOMINIO

## FUNZIONE SURIETTIVA

Se  $\text{Im } f = b$ ,  $f$  si dice suriettiva

↳ Dalla definizione di immagine, si deduce che:

$$f \text{ è suriettiva} \Leftrightarrow (\forall y \in b)(\exists x \in a(f(x) = y))$$



metto un  
quando f → suriettiva

QUANDO OGNI ELEMENTO  
DEL DOMINIO È IMMAGINE DI  
ALMENO UN ELEMENTO DEL DOMINIO

→ NELLA DEFINIZIONE  
DI  $\text{Im } f$  AVEMMO IN  
MODO GENERICO "LE Y", OBA  
LE Y DEVONO ESSERE TUTTE

## FUNZIONE NON SURIETTIVA

$$\neg(f \text{ è suriettiva}) \Leftrightarrow (\exists y \in b)(\forall x \in a(f(x) \neq y))$$

↳ INGESSARE LA  
SURIETTIVITÀ

## FUNZIONE RIDOTTA DI $f$ AD $S$

Se  $s \subseteq b$ ,  $\text{Im } f \subseteq s$

$g: x \in a \mapsto f(x) \in s$  si chiama ridotta di  $f$  ad  $s$ .

↓  
RESTRIGO IL  
DOMINIO A  
QUALcosa SU  
PIÙ VICINO  
ALL' IMMAGINE

↓  
L' IMPORTANTE E' CHE  
CONTENGA ANCORA L' IMMAGINE  
ALTRIMENTI NON E' PIÙ  
UNA FUNZIONE

## FUNZIONE COSTANTE

Sia  $\bar{y} \in b$

$g: x \in a \mapsto \bar{y} \in b$  si dice funzione costante  
con valore  $\bar{y}$

UNA FUNZIONE COMPOSTA DA DUE FUNZIONI SURGETTIVE E' SURGETTIVA  
 Siano  $f$  e  $g$  surgettive, allora  $g \circ f$  è surgettiva

DIM

RIPETTA CHE SO DIMOSTRO PER UNA Y

PERCHE' HO  $\forall y \rightarrow$  DEVE ESISTERE QUALSiasi  $x$  → DIMOSTRO UNA  
 SIA  $y \in c$  E LE DIMOSTR TUTTE

Poiché  $g$  è surgettiva,  $\exists z \in b : g(z) = y$   $\xrightarrow{z \in b}$  e

Poiché  $f$  è surgettiva,  $\exists w \in a : f(w) = z$

Segue che  $g \circ f(w) = g(f(w)) = y$   $\xrightarrow{\text{DATO CHE } z \in b}$

$\underbrace{g(z)}$

HO TROVATO UN ELEMENTO IN  $a$  CHE HA, MEDIANTE  $g(f(w))$ , IMMAGINE Y

## FUNZIONE INIETTIVA

$f$  si dice iniettiva  $(\forall x, y \in a)(f(x) = f(y) \rightarrow x = y)$

$(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$

Per la tautologia della contraposizione,

$\downarrow f$  è iniettiva  $\leftrightarrow (\forall x, y \in a)(x \neq y \rightarrow f(x) \neq f(y))$

QUANDO ELEMENTI  
DISTINTI DEL DOMINIO  
HANNO IMMAGINI DISTINTE



ESSO METTERE  
 → EQUIVALENTE  
 EL  $\leftrightarrow$   
 PERCHE' IL  
 VERSO  
 CONTRARIO  
 DELLA FRECCIA  
 E' LA DEFINIZIONE  
 DI FUNZIONE

## FUNZIONE NON INIETTIVA

$\neg(f$  è iniettiva)  $\leftrightarrow (\exists x, y \in a)(f(x) = f(y) \wedge x \neq y)$

INDICARE  
 L'INIETTIVITÀ

ESEMPIO: QUANDO  $f$  È INIETTIVA O SURGETTIVA

$\circ f : a \rightarrow b$   $a = \{x\}$   $f = (a \times b, G)$   $G = \{(x, y)\}$

$\exists ! y \in b : f(x) = y$

DOMINIO DI  
UN SOLO ELEMENTO

NON PUO' ESSERE  
NIENT'ALTRO

Anemolo un solo elemento, la funzione è già forse iniettiva  
 La funzione può essere surgettiva o anche b ha un solo elemento

$\circ f : X \in a \mapsto \{x\} \in P(a)$   $a = \{0, 1\}$

$\rightarrow$  NEL CASO UNICO CI SONO 4 ELEMENTI  $\rightarrow P(a) = \{\{0\}, \{1\}, \{0, 1\}, \emptyset\}$

$f(x) = f(y) \leftrightarrow \{x\} = \{y\} \leftrightarrow x = y \rightarrow$  È iniettiva

La funzione è iniettiva ma non surgettiva poiché ci sono  
 degli elementi di  $P(a)$  che non sono immessi  $\rightarrow$  Ad esempio:  $\emptyset$

$$\bullet f: X \in P(N) \mapsto X \cap (N \setminus \{0\}) \in P(N)$$

P.A. → PER ASSURDO

$$\text{Suppongo che } \exists x : f(x) = \{0\} \leftrightarrow x \cap (N \setminus \{0\}) = \{0\}$$

FALSO

Quindi la funzione non è suriettiva

↪ C'è UN ELEMENTO FEL  
COPRIMARIO CHE NON E' ASSOCIA  
A NULLO

↪ INSERIRE DI TUTTI  
GLI ELEMENTI CHE  
APPARTENGONO A N  
E CHE A N \ {0}

È iniettiva?

$$\rightarrow \text{IMMAGINI UGUALI} \Rightarrow f(x) = f(y)$$

$$X \cap (N \setminus \{0\}) = Y \cap (N \setminus \{0\})$$

$$\text{Supponiamo che } \bar{x} = \{0, 1\} \quad \bar{y} = \{1\}$$

SUPPONIAMO CHE X E Y  
DIFFERISCONO  
SOLA PER LO  
ZERO

$$f(\bar{x}) = \{1\} = f(\bar{y})$$

Due elementi diversi hanno la stessa immagine, quindi f non è iniettiva

$$\bullet f: X \in P(N) \mapsto N \setminus X \in P(N) \rightarrow A UNA PARTE X DI$$

N ASSOCIA IL  
COMPLEMENTO DI X  
IN N

È iniettiva?

ELEMENTO  
GENERICI

$$\text{Suppongo che } N \setminus X = N \setminus Y \leftrightarrow N \setminus (N \setminus X) = N \setminus (N \setminus Y) \leftrightarrow X = Y$$

La funzione è iniettiva

FALSO LO  
STESO INSIEME

È suriettiva?

Bando  $y \in P(N)$

$$\text{Se } (x = N \setminus y)$$

$$f(x) \stackrel{\text{def}}{=} N \setminus x = N \setminus (N \setminus y) = y$$

La funzione è suriettiva

## FUNZIONE BIETTIVA

$f$  si dice biettiva se è sia iniettiva che suriettiva.  
Se  $f$  e  $g$  sono biettive,  $g \circ f$  è biettiva.

UNA FUNZIONE COMPOSTA DA DUE FUNZIONI INIEKTIVE  
E' INIETTIVA?  $\rightarrow (\forall x, y \in a) (f(x) = f(y) \rightarrow x = y)$

Se  $f$  e  $g$  sono iniettive,  $g \circ f$  è iniettiva.

DIM

Siamo  $w, z \in a$ :  $g \circ f(w) = g \circ f(z)$  allora

Visto che:

$$g(f(w)) = g(f(z))$$

- $g$  è iniettiva, quindi  $f(w) = f(z) \rightarrow$  perche'  $g(f(w)) = g(f(z))$
- $f$  è iniettiva, quindi  $w = z \rightarrow$  perche'  $f(w) = f(z)$

Da ciò segue che  $g \circ f$  è iniettiva.

SE  $g \circ f$  E' INIETTIVA,  $f$  E' INIETTIVA?

Se  $g \circ f$  è iniettiva allora  $f$  è iniettiva.

DIM

Siamo  $z, w \in a$ :  $f(z) = f(w)$  allora; per la definizione di

funzione di  $g$ ,  $g(f(z)) = g(f(w))$ ,  $\stackrel{\text{DEF}}{=} g \circ f(z) = g \circ f(w)$ ; ma

$g \circ f$  è iniettiva per ipotesi, quindi  $z = w$  oppure  $f(z) = f(w)$

$\hookrightarrow$  Quindi  $f$  è iniettiva.

PER LA  
DEFINIZIONE  
DI FUNZIONE  
DI  $g$

SE  $g \circ f$  E' SURIETTIVA,  $g$  E' SURIETTIVA?

Se  $g \circ f$  è suriettiva, allora  $g$  è suriettiva

DIM

$\rightarrow$  esistenziale  
di  $g$

Sia  $y \in b$ , perche'  $g \circ f$  è suriettiva  $\exists x \in a : g \circ f(x) = y$

allora  $g$  è suriettiva

$\rightarrow$  ABBIANO TROVATO UN ELEMENTO  
DEL DOMINIO DI  $g$  TALE CHE  $g$  PER  
QUELLO ELEMENTO DIA  $y$

$g(f(x)) \rightarrow g(x) \in b$ , cioè  $x$   
DOMINIO DI  $g$

$\rightarrow$  QUESTO ELEMENTO  
E'  $f(x)$

SE  $g \circ f$  È INIETTIVA,  $g$  È INIETTIVA? SE  $g \circ f$  È SURIETTIVA,  $f$  È SURIETTIVA?

- Se  $g \circ f$  è iniettiva,  $g$  non è iniettiva.
- Se  $g \circ f$  è suriettiva,  $f$  non è suriettiva.  
↳ ESEMPIO:

$$a = \{1\}, b = \{3, 2\} \rightarrow \text{E' UN CONTROESEMPIO}$$

$$f: 1 \in a \mapsto 1 \in b \quad (\text{INIEZIONE})$$

$$\begin{cases} g: 1 \in b \mapsto 1 \in a \\ 2 \in b \mapsto 1 \in a \end{cases} \quad (\text{FUNZIONE COSTANTE})$$

$$g \circ f: x \in a \mapsto x \in a \quad g \circ f = \text{Id}_a$$

Le identità sono sempre iniettive  $\rightarrow g \circ f$  è iniettivo

Ma  $g$  non è iniettiva e  $f$  non è suriettiva

Correzione esercizi 20/10/2021 (LEZIONE 11)

Q) VII.  $p: m \in \mathbb{N} \mapsto \{m\} \in P(\mathbb{N})$  è una funzione

Prendo  $m, n \in \mathbb{N}$  e suppongo che  $p(m) = p(n) \rightarrow m = n$

$$\text{Se } \{m\} = \{n\} \rightarrow$$

Quindi la funzione è iniettiva

$\{0, 1\} \subseteq \text{Im } p$ , quindi la funzione non è suriettiva

VIII.  $\{a, b\} \ni m \longleftrightarrow a^b = m$

Im già ha che  $(\{2, 3\}, 8) \in g$  ma anche  $(\{3, 2\}, 9) \in g$   
quindi questa non è una funzione

$$\text{III. } (m, m) \in g \Leftrightarrow m + m \in \mathbb{N} \quad m + m \Leftrightarrow m + m \in \mathbb{N}$$

$$(0, 1) \in g? \text{ Si perché } 0+1 \in \mathbb{N}$$

$$(0, 2) \in g? \text{ Si perché } 0+2 \in \mathbb{N}$$

Tutte le coppie appartengono al grafico, quindi  $g = \mathbb{N} \times \mathbb{N}$

Per vedere se si ha una funzione c'è bisogno di vedere che tutti gli elementi a sinistra sono associati a due diversi elementi  
non sono associati a due diversi elementi

↳ In questo caso, la definizione di funzione è:  $(\forall m \in \mathbb{N})(\exists! m \in \mathbb{N})(m, m) \in g$

↳ Questo non è una funzione perché esistono più  $m$  tali che  $(m, m) \in g$

$$\text{VII. } p: (l, m) \in \mathbb{N} \times \mathbb{N} \mapsto l^m \in \mathbb{N} \quad (l, m) \neq m \Leftrightarrow l^m = m$$

$$(\forall x \in (\mathbb{N} \times \mathbb{N}))(\exists! m \in \mathbb{N})(x, m) \in g \rightarrow p = \underbrace{((\mathbb{N} \times \mathbb{N}) \times \mathbb{N}, g)}_{\text{DOMINIO E IMMAGINE}}$$

$$(\forall (l, m) \in (\mathbb{N} \times \mathbb{N}))(\exists! m \in \mathbb{N})(l^m = m)$$

↳ Questo è una funzione perché ad ogni coppia viene associata una ed un solo  $m$

↳ DIPENDE DA CONE  
DEFINISCONO  $0^{\circ}$  → POSSIAMO DEFINIRLO

La funzione è suriettiva!

$$(0, 0, m) \in g \Leftrightarrow 0^{\circ} = m$$

Sic  $m \in \mathbb{N}$

$$p((m, 1)) = m^1 = m$$

Si, è suriettiva perché ogni coppia ha un'immagine

La funzione è iniettiva?

$$\begin{cases} (l_1, m_1) \in \mathbb{N} \times \mathbb{N} \\ (l_2, m_2) \in \mathbb{N} \times \mathbb{N} \end{cases} \quad \left\{ \begin{array}{l} l_1^{m_1} \\ l_2^{m_2} \end{array} \right\} l_1^{m_1} = l_2^{m_2}$$

$$\text{Non è iniettiva perché } p((0, 1)) = p((0, 2))$$

$0^{\circ}$  → UGUALE A 1  
PERCHÉ PER LA FUNZIONE

$x \in \mathbb{R} \rightarrow x^0 \in \mathbb{R}$   
QUESTA È UNA FUNZIONE COSTANTE  
UGUALE A 1  
TRANNÉ CHE A 0

$0^{\circ} = 1$  PER CONTINUITÀ

5)

$$P: m \in \mathbb{Z} \rightarrow \begin{cases} -\frac{m}{2} & \text{SE } m \text{ è pari} \\ \frac{m+1}{2} & \text{SE } m \text{ è dispari} \end{cases} \in \mathbb{Z}$$

E' una funzione.

E' iniettiva?

Siamo  $m, n \in \mathbb{Z}$  vogliamo vedere che " $f(m) = f(n) \Rightarrow m = n$ "

$$f(-1) = 0 = f(0)$$

$\rightsquigarrow$  SE CONSIDERIAMO  
I PARI

$$f(-3) = -1 = f(2) \rightarrow \text{STESSA IMMAGINE}$$

Quindi la funzione non è iniettiva

E' suriettiva?  $\rightarrow$  SE FOSSE STATO  $m \in \mathbb{N}$  ALLORA SAREBBE STATO

$$m \in \mathbb{Z} \rightarrow -\left(\frac{-2m}{2}\right)$$

$$f(-2m) = m$$

Quindi la funzione è suriettiva

# APPPLICAZIONE (ANTI)IMMAGINE

Sia  $f: a \rightarrow b$

$$\{y \in b \mid \exists z \in a \text{ s.t. } f(z) = y\} \in P(b)$$

tutte le immagini degli elementi di questo  $x$

Definisco  $\bar{f}: x \in P(a) \mapsto \{f(x) \mid x \in x\} \in P(b) \rightarrow$  IMMAGINE

$\bar{f}: y \in P(b) \mapsto \{x \in a \mid f(x) \in y\} \in P(a) \Rightarrow$  APPLICAZIONE  
ANTIIMMAGINE

ESEMPI:

•  $\bar{f}(\emptyset) = \emptyset \rightarrow$  TUTTE LE IMMAGINI DEGLI ELEMENTI CHE STANNO NEL VUOTO

$\bar{f}(b) = \emptyset \rightarrow$  TUTTI GLI  $x$  DEL DOMINIO, TALI CHE  $f(x) \in \emptyset$

•  $\bar{f}(a) = \text{Im } f \rightarrow$  L'IMMAGINE DI  $a$  STESSO  $\rightarrow$  SONO TUTTI  $f(z)$  CON  $z \in a$

•  $\bar{f}(\{x\}) = \{f(x)\} \rightarrow$  SONO TUTTI GLI  $f(z)$  TALI CHE  $z \in \{x\}$ , EICE'  $z$  E' PROPRIO  $x$   $\rightarrow$  QUINDI PRENDO L'INSIEME DEGLI  $f(z)$ , EICE' VISTO CHE DEL SOLO  $f(x)$ , SARÀ L'UNICO CON SOLO  $f(x)$

•  $\bar{f}(b) = a \rightarrow$  TUTTI GLI ELEMENTI CHE SE LI PRECIO L'IMMAGINE STO IN  $b$

$\hookrightarrow \bar{f}(\text{Im } f) = a$

• Se  $y \in b \setminus \text{Im } f$ , allora  $\bar{f}(\{y\}) = \emptyset$

•  $f: m \in \mathbb{N} \mapsto \{m\} \in P(\mathbb{N})$

$\bar{f}(\{\emptyset, 1\}) =$  Tutte le immagini composte degli elementi di  $\{\emptyset, 1\}$   $= \{\{\emptyset\}, \{1\}\}$

$P(P(\mathbb{N}))$

$\bar{f}(\{\{2\}, \{3, 5\}, \{6\}\}) =$  Tutti gli  $x \in \mathbb{N}$  tali che  $\{2, 5\} \in P(x)$   
di tale elemento è un elemento dell'insieme  $\{\{2\}, \{3, 5\}, \{6\}\}$

NON ESISTE

UN ELEMENTO

DI  $m$  CHE HA

COME IMMAGINE

$\{3, 5\}$

$\hookrightarrow \bar{f}(3) = \{3\} \notin \{\{2\}, \{3, 5\}, \{6\}\}$

# CARATTERIZZAZIONI DI INIETTIVITÀ, SURIETTIVITÀ, BIETTIVITÀ A PARTIRE DA $f$

- $f$  è iniettiva se e solo se:  $\forall y \in P(b), f(y) \neq \emptyset \Leftrightarrow$  non c'è un solo elemento.

$$\hookrightarrow f \in \text{Im}(a, b) \Leftrightarrow (\forall y \in P(b)) (f(y) = \emptyset \vee (\exists! x \in a) (f(y) = x))$$

funzione iniettiva

DIM → VOGLIANO DIMOSTRARE  
QUESTO SE E SOLO SE

E' UN SOTTOINSIEME DI  $a$

ESISTE UN  
UNICO ELEMENTO  
IN  $a$  CHE HA  
DIVERSI

( $\rightarrow$ ) | Supponiamo che  $f$  sia iniettiva |  
Sia  $y \in P(b)$  e suppongo che  $f(y) \neq \emptyset$ .  
Dalla definizione,  $\exists x \in a : f(x) \in y$

c'è l'or. quindi se  
dimostro che c'è un solo  
ELEMENTO VA BENE  
LO STESSO

Sia  $z \in a : f(z) \in y$  e  $f(x) = f(z)$

DEVO FAMOSIFICARE  
CHE SE LO  
PRENDO NO  
VUOL DIRE  
HA UN SOLO  
ELEMENTO

Dall'iniettività segue che  $z$  deve essere proprio uguale a  $x$   
Quindi,  $z = x$ , di conseguenza  $f(y) = \{x\}$

( $\leftarrow$ ) Premo  $x, y \in a$  e suppongo che  $f(x) = f(y)$  → voglio far vedere che  $x = y$

Premo  $f(\{f(x)\})$

QUINDI  $f(y)$  HA  
UN SOLO ELEMENTO  
LO PRESO IL SOTTOINSIEME  
CHE HA UN ELEMENTO TALI CHE UN  
UNICO IMAGING VADA NELL'  
SINGLETON  $f(x)$ , CHE PUR E' ANCORA  
UN SINGLETONE PERCHÉ  $f(x) = f(y)$

Sia  $x$  che  $y$  appartengano a  $f(\{f(x)\})$ , ma  $f(\{f(x)\})$  ha un solo elemento quindi  $x = y$

$\hookrightarrow$  Quindi la funzione è iniettiva perché altrimenti che  $x \neq y$  allora  $x = y$

- $f$  è suriettiva se e solo se  $(\forall y \in P(b) \setminus \{\emptyset\}) (f(y) \neq \emptyset)$

→ SE  $f$  È SURIETTIVA ALLORA E' CHIARO CHE  $\forall y \in P(b)$  TUTTI GLI ELEMENTI DI  $b$  SONO ASSOCIAZI AD ALMENO UN ELEMENTO DI  $a$  QUINDI  $f(y) \neq \emptyset$

→ SE  $f(y) \neq \emptyset$  ALLORA  $\forall z \in b$ , VISTO CHE  $f(\{z\}) \neq \emptyset$ ,  $\exists x \in a : f(x) = z$  QUINDI  $f$  È SURIETTIVA

- $f$  è biellita se e solo se  $\forall y \in P(b) \setminus \{\emptyset\}$  allora  $f(y)$

contiene esattamente un elemento → DEVE VALERE CHE  $f(y) \neq \emptyset$  E CHE HA UN SOLO ELEMENTO

# SEZIONE, RETRAZIONE E INVERSA DI $f$

Sia  $f: a \rightarrow b$  e  $g: b \rightarrow a$

- Se  $g \circ f = id_b$ ,  $g$  si dice sezione di  $f$
- Se  $g \circ f = id_a$ ,  $g$  si dice retrazione di  $f$
- Se  $g$  è sia sezione che retrazione di  $f$ ,  $g$  si dice inversa di  $f$

ESEMPI:

•  $f: m \in \mathbb{N} \mapsto \{m\} \in P(\mathbb{N})$

C'è una retrazione?

$\hookrightarrow$  Voglio che una volta effettuate le composizioni mi dia l'identità di  $a$

$\hookrightarrow$  g, per essere  
una funzione  
DEVE ESSERE DEFINITA  
SU TUTTE LE PARTI DI  $N$

$\hookrightarrow$  g:  $P(N) \rightarrow N$

"SERVE AFFINCIÈ POTEVO ANCHE HADDOLO IN  
8 SIA UNA FUNZIONE  
1 SE NON È UN SINGLETON"

$\left\{ \begin{array}{ll} 0 & \text{SE } n \text{ HA } 0 \text{ O PIÙ DI UN ELEMENTO} \\ m & \text{SE } (\exists m \in \mathbb{N})(n = \{m\}) \end{array} \right.$

"SIEDE, SE È UN SINGLETON DI UN ELEMENTO, ASSOCIA QUELL'ELEMENTO"

•  $g \circ f(m) = g(f(m)) = g(\{m\}) = m \rightarrow g \circ f = Id_N \rightarrow$  g è una retrazione di  $f$

$\hookrightarrow$  È UNA SEZIONE?

$\rightarrow g \circ g(\emptyset) = g(g(\emptyset)) = g(\{0\}) = \{0\}$

$\hookrightarrow$  PROVO IL CASO IN CUI N NON È UN SINGLETON

$\downarrow$   
DAL VUOTO  
SIANO ARRIVATI  
AL SINGLETON  
DI ZERO

$\rightarrow$  g NON È UNA SEZIONE DI g

$\downarrow$   
NON È DETTO CHE NON CI SIANO ALTRE g CHE SIANO SEZIONI

$\downarrow$   
g è una retrazione ma non una sezione.

Anche se  $g$  non è una sezione di  $f$ , non significa che non ci siano altre funzioni che lo sono.

↳ In questo caso, però, non ce ne sono più due.



COME SI VEDE SE ESISTONO SEZIONI (O RETRAZIONI)?



Ragioniamo per assurdo.

P.A. c'è una sezione  $g$  di  $f$ .

Cioè  $f \circ g = \text{Id}_b \rightarrow$  l'identità di  $b$  è biettiva,  
quindi è ovviamente anche suriettiva.

LA PRIMA  
FUNZIONE E' BIETTIVA  
8:8 ↴

Affinché  $f \circ g$  sia suriettiva, è necessario che  $f$  sia suriettiva, ma questo è un assurdo.

↳ perché  $f$  non è suriettiva  $\rightarrow f \circ g$  non può essere biettiva e quindi non si ha  $\text{Id}_b$ .

## TEOREMA SULL'INIECTIVITÀ

$f: a \rightarrow b$  è iniettiva se e solo se:

$a = \emptyset \vee \exists$  retroazione di  $f$



DIM

• ( $\leftarrow$ ) Vogliamo vedere che  $a = \emptyset$  oppure esiste retroazione  $f$  è iniettiva.

• Supponiamo che  $a = \emptyset$

↳ la condizione di iniettività è banalmente verificata.

↳ PER LA DEFINIZIONE DI INIECTIVITÀ,  $(\forall x, y \in a) (\underbrace{f(x) = f(y)}_{\text{implicazione}} \rightarrow x = y)$



$(\forall x) (\forall y) (x \in a \wedge y \in a \rightarrow (f(x) = f(y) \rightarrow x = y))$

FBF DI INIECTIVITÀ

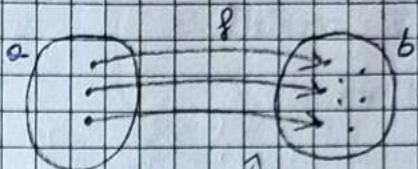
SEMPRE FALSO, QUINDI L'IMPLICAZIONE E' SEMPRE VERA E LA FRASE E' SEMPRE VERIFICATA

• Se  $(\exists g : b \rightarrow a)(g \circ f = \text{Id}_a)$  allora, visto che  $\text{Id}_a$  è biettiva, anche  $g \circ f$  è biettiva. In particolare  $g \circ f$  è iniettiva e quindi ciò significa,  $f$  è iniettiva.

• ( $\rightarrow$ ) Se  $f$  è iniettiva.

Suppongo  $a \neq \emptyset$ , cioè che  $\exists x \in a \rightarrow$

Questo lo chiamiamo  $\bar{x}$



$f$  è iniettiva ma l'immagine non è tutta non c'è univocità

• GLI ELEMENTI DELL'

IMMAGINE, CHE QUINDI VENGONO DA ELEMENTI DI  $a$ . LI RIMANDO A QUEGLI ELEMENTI DI  $a$  DA CUI  $\rightarrow$  DI RITORNO VENGONO.

• GLI ELEMENTI CHE NON SONO IN  $\text{Im } f$ , LI RIMANDO AD  $\bar{x}$

SE DEVO FAR VEDERE CHE UNA COSA IMPLICA UNA DISGIUNZIONE POSSO LEGGERE UNA DELLE DUE E FAR VEDERE CHE VALE L'ALTRA

LA FUNZIONE  
NON DICE  
ESSERE PER  
FORZA  
INIETTIVA

Definisco  $g : b \rightarrow a$

↳ Sicché  $f$  è per ipotesi iniettiva ed  $a \neq \emptyset$ , quindi  $(\exists x \in a)(f(x) = y)$ , necessariamente  $f(\{y\}) \neq \emptyset$

In particolare, dato che  $f$  è iniettiva,  $f(\{y\})$  ha un solo elemento che dipende da  $y \rightarrow$  chiamalo questo elemento  $x_y$ , quindi se  $y \in \text{Im } f$ ,  $f(\{y\}) = \{x_y\}$

$$g : x \in b \mapsto \begin{cases} x_y & \text{SE } y \in \text{Im } f \\ \bar{x} & \text{SE } y \notin \text{Im } f \end{cases}$$

QUESTA PARTE CI SERVE PER DEFINIRE LA FUNZIONE  $g$

→ Dobbiamo vedere se  $g$  è una retroazione, cioè:

$$\hookrightarrow g \circ f(x) = \text{Id}_a$$

$$g \circ f(x) = g(f(x)) = x \rightarrow \begin{array}{l} \text{POSSO SCRIVERE } x \text{ PERCHÉ} \\ f(x) \in \text{Im } f \text{ SEMPRE, QUINDI} \\ x_y \text{ È PROPRIO } x \end{array}$$

$\hookrightarrow g(x) \in \text{Im } f$ ?

CERTO PER → SIAMO NEL →  $g$  ASSOCIA  $x_y$ , DICHI<sup>E</sup> DEFINIZIONE PRIMO CASO L'ELEMENTO DA QUI PROVIENE  $f(x)$

QUESTO CASO NON  
CI SERVE PER  
VEDERE SE  $g$  È  
UNA RETROAZIONE  
PERCHÉ TUTTI  
GLI ELEMENTI DI  
 $a$  VANO PER  
FORZA NELL'  
IMMAGINE DI  $f$

# TEOREMA SULLA SURBIETTIVITÀ

$f: a \rightarrow b$  è suriettiva se e solo se esistono sezioni di  $f$

DIM

( $\leftarrow$ ) Per ipotesi, esiste una sezione di  $f$

$$(\exists g: b \rightarrow a) (f \circ g = \text{Id}_b)$$

Dato che  $f \circ g$  è suriettiva,  $f$  è suriettiva

$\hookrightarrow f \circ g$  è biettiva perché  $\text{Id}_b$  è biettiva

STESO  
RAZIONAMENTO  
DEL TEOREMA  
PRECEDENTE

( $\rightarrow$ ) Sia  $f$  suriettiva



Come prima, voglio creare una funzione  $g$  che manda gli elementi di  $b$  (cioè l'insieme immagine dato che  $f$  è suriettiva) verso gli elementi di  $a$  da cui provengono

Per costruire la funzione  $g$  ho il problema della scelta

$\hookrightarrow$  Potrei scegliere un elemento in  $b$  che è assegnato a più di un elemento di  $a \rightarrow$  Dovrò scegliere uno ed escludere gli altri

È possibile costruire  $g$  grazie all'ASSIOMA DELLA SCELTA

Abbiamo visto qualche lezione fa che:

$f$  è suriettiva  $\Leftrightarrow$   $\forall y \in b \quad (\forall x \in a) (f(x) = y)$

c'è sempre  
UN ELEMENTO  
DI  $a$  CHE HA  
COME IMMAGINE  $y$

Esiste, per l'assioma della scelta, una funzione:

$$\Phi: \{y\} \in P(b) \mapsto x \in a \quad (x \in \{f(x)\})$$

$\Phi(y)$   $\mapsto$   
E' UNA  
SCELTA

QUESTA FUNZIONE

QUIA NON SI PUÒ  
DIMENTICARE IL DIFETTO  
DEI DIVERSI ASSIOMI  
QUINDI SERVE UN ASSIOMA  
A PARTE

TALE CHE VAGLIA?

ASSIOMA DELLA

SCELTA PIÙ PERFECCA

DI ORDINARE GLI

INSIEMI IN UN MODO

DA FARE UN PIANO

NON E' UN MODO  
CON LA  
FUNZIONE

DELLA SCELTA

PER SCEGLIERE  $x$ , HAGGIAMO  
FOSSO PRENDERE IL PRIMO  
DELL'INSIEMA MA A VINTO

E' POSSIBILE DETERMINARLO  
PERCHE' TUTTI GLI INSIEMI SONO

Grazie all'assenza delle sezioni possiamo definire  $g$ .  
 Definisco  $g$ :  $y \in b \mapsto g(f(\{y\})) \in a$

AD Y ASSOCIO UN CERTO ELEMENTO CHE STA NELL'ANTIIMMAGINE DEL SINGLETON DI Y

$\rightarrow$  Voglio vedere se  $g$  è una sezione di  $f$ .

$$(g \circ g(y) = g(g(y)) = g(f(\{y\}))) = y$$

PER DEFINIZIONE,

Quindi  $g \circ g = \text{Id}_b$

$f(\{y\})$  È UN CONTO  
X È APPARTIENE A  
 $f(\{y\})$ , MA  $f(x)$  È  
PROPRIO Y, QUINDI:



### TEOREMA (corollario)

$f: a \rightarrow b$  è biettiva se e solo se ha un'immagine.

Sia  $f: a \rightarrow b$ , sono equivalenti:  $\rightarrow$  UNO IMPLICA L'ALTRO

1)  $f$  è biettiva

2)  $f$  ha un'immagine

3)  $f$  ha sezioni e retrosezioni

4)  $f$  ha una e una sola sezione

5)  $(\forall y \in b)(\exists! x \in a)(y = f(x))$

3)  $\rightarrow$  4)

5)  $\leftarrow$  1) SONO LA STESSA COSA, QUINDI 5)  $\leftrightarrow$  1)

Se  $f$  ha una retrosezione  $r$  è una sezione  $s$ , allora  $r = s$ . In particolare  $r$  è l'unica retrosezione, l'unica sezione e l'unica immagine di  $f$ .

DIM

Portiamo con il dicitore una delle tre.

$r$  è una retrosezione?

$r \circ f = \text{Id}_a$ , quindi  $(r \circ f) \circ r = \text{Id}_b$

Ma  $\text{Id}_a \circ \sigma = \sigma$  dato che  $\text{Id}_a$  non fa nulla agli elementi, li lascia così come sono.

Per associatività,  $(\tau \circ g) \circ \sigma = \tau \circ (g \circ \sigma) = \tau \circ \text{Id}_b$

Dato che  $\text{Id}_b$  non cambia nulla nella relazione,

$$\tau \circ \text{Id}_b = \tau$$

$$\hookrightarrow (\tau \circ \text{Id}_b)(y) = \tau(\text{Id}_b(y)) = \tau(y)$$

E STESSA COSA FA ANCHE  $\text{Id}_a \circ \sigma$

Di conseguenza  $\tau = \sigma$

$\hookrightarrow$  SE CI SONO DUE INVERSE, COINCIDONO

PERCHÉ ENTRAMBE SONO SIA SEZIONE CHE RETRAZIONE

$\hookrightarrow 5)$

DIM  
Suppongo che  $(\exists x_1, x_2 \in a)(x_1 \neq x_2 \wedge f(x_1) = f(x_2))$   $\hookrightarrow$  CHE LA 5) SUPPONANO  
NON VA MAI VERSO UNA STessa IMMAGGIO  
PERCHÉ NON INIEZIONE

$f$  è suriettiva perché già sappiamo che esiste una sezione per ipotesi (da notare ipotesi è l'affermazione 4)

Se suppongo che  $f$  non è iniettiva, vuol dire che esistono  $\hookrightarrow$  più sezioni

Prendo una sezione  $g$ :  $g(f(x_1)) = x_1$

$\hookrightarrow$  DUE SEZIONI DIVERSE

E prendo un'altra sezione  $\bar{g}$  tale che:

$$y \in b \mapsto \begin{cases} g(y) & \text{se } y \neq f(x_1) \\ x_2 & \text{se } y = f(x_1) \end{cases}$$

Ho dimostrato 4)  $\rightarrow$  5) con non 1)  $\rightarrow$  non 4)  $\hookrightarrow$  COMPARAZIONE

COME TROVARE L'INVERSA DI  $f$ ?

ESEMPPIO:

Prendo  $f: m \in \mathbb{Z} \mapsto m+1 \in \mathbb{Z}$

$$y = m+1 \rightarrow y-1 = m \rightarrow$$

AGGIUNGO UNA FRAZIONE CHE  
AD Y ASSORBI DI NUOVO M

Definisco  $g: m \in \mathbb{Z} \mapsto m-1 \in \mathbb{Z}$   $\hookrightarrow$  E' L'INVERSA!  
VEDIAMO

$$(f \circ g)(m) = f(g(m)) = f(m-1) = m \rightarrow g \in \text{SEZIONE?} \quad g \in$$

$$(g \circ f)(m) = g(f(m)) = g(m+1) = m \rightarrow g \in \text{RETRAZIONE} \quad \text{INVERSA}$$

Correzione esercizi 26/10/2023 (LEZIONE 13)

2.II)  $f: m \in \mathbb{N} \mapsto 3m-2 \in \mathbb{Q}$

$g: m \in \mathbb{Q} \mapsto 3m+2 \in \mathbb{N}$  Non è una funzione perché

$$g \circ g(m) = 6m \rightarrow \text{Non è un'identità di } b$$

Se prendo  $x = \frac{m+2}{3}$

$$g(x) = 3\left(\frac{m+2}{3}\right) - 2 = m$$

$$\begin{cases} y = 3m-2 \\ m = \frac{y+2}{3} \end{cases}$$

$\hookrightarrow g: m \in \mathbb{Q} \mapsto \frac{m+2}{3} \in \mathbb{N}$   $\rightarrow$  SE PRENDO  $m = -3$  PERO'  $g(-3) = -\frac{1}{3}$

NON APPARTIENE AD  $\mathbb{N}$

$$g \circ g(m) = g(g(m)) = g\left(\frac{m+2}{3}\right) = \frac{3m-2+2}{3} = m$$

QUINDI  $g$  NON E' UNA FUNZIONE

$$g \circ f(m) = g(f(m)) = g\left(\frac{m+2}{3}\right) = 3\left(\frac{m+2}{3}\right) - 2 = m$$

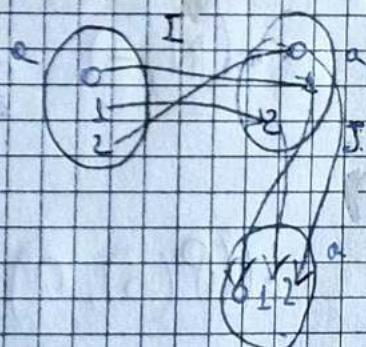
$g$  non è invertibile

2.IV)  $\Omega = \{0, 1, 2\}$

$$I: \Omega \rightarrow \Omega$$

$$I(0) = 1 \quad I(1) = 2 \quad I(2) = 0$$

$$g = \{(0, 1), (1, 2), (2, 0)\}$$



$$J: \Omega \rightarrow \Omega \rightarrow \text{PER PROVARE L'INVERSA}$$

BASTA INVERTIRE IL GRAFICO

$$J(0) = 2 \quad J(1) = 0 \quad J(2) = 1$$

$$I \circ J(0) = I(J(0)) = I(2) = 0 \quad \text{ecc.}$$

# OPERAZIONI SU INSIEMI

## STRUTTURE ALGEBRICHE

- Sia  $S$  un insieme non vuoto e sia  $*: S \times S \rightarrow S$

\* si dice della operazione interna di  $S$  (BINARIA)

- Per ogni  $x, y \in S$ ,  $x * y = *(x, y)$

cos'è UNA STRUTTURA ALGEBRICA?

Se  $S$  è un insieme tale che  $S \neq \emptyset$  e  $*$  è un'operazione di  $S$ , dico che:

$(S, *)$  è una STRUTTURA ALGEBRICA AD UNA OPERAZIONE (BINARIA INTERNA)

↳ ESEMPIO:

•  $(\mathbb{N}, +)$  è una struttura algebrica

•  $(\mathbb{N}, -)$  non è una struttura algebrica perché non è interna a  $\mathbb{N}$   
 $\hookrightarrow 2 - 3 = -1 \notin \mathbb{N}$

IL "-" NON VA DA  $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$

NON È UNA FUNZIONE

•  $((P(S), \cap)$  è una struttura algebrica

PROPRIETÀ COMMUTATIVA

Se  $S \neq \emptyset$  e  $*$  è un'operazione di  $S$ ,

$*$  si dice commutativa se:

$$(\forall x, y \in S)(x * y = y * x)$$

→ UNA FUNZIONE CHE VA DA  $S \times S$  A  $S$

Y APPLICABILE A DUE ELEMENTI ALLA VOLTA  
IL DOMINIO È IL PRODOTTO CARTESIANO

## PROPRIETÀ ASSOCIATIVA

Se  $S \neq \emptyset$  e  $*$  è un'operazione binaria di  $S$ ,  
 $*$  si dice associativa se:

$$(\forall x, y, z \in S)((x * y) * z = x * (y * z))$$

## SEMIGRUPPO

Se  $S \neq \emptyset$ ,  $*$  è un'operazione binaria, interna e associativa di  $S$ ,

$(S, *)$  si dice semigruppo

ESEMPIO:  $(\mathbb{N}, +) \rightarrow \mathbb{Z} \quad +$  è associativo

## ELEMENTO NEUTRO A DESTRA

$\exists e \in S$  si dice elemento neutro a destra (di  $(S, *)$ ) se:

$$(\forall x \in S)(x * e = x)$$

$\hookrightarrow e$  sta a destra

SE È COMMUTATIVA  
NON RISOGNA  
SPECIFICARE A DESTRA  
O A SINISTRA

## ELEMENTO NEUTRO A SINISTRA

$\exists e \in S$  si dice elemento neutro a sinistra (di  $(S, *)$ ) se:

$$(\forall x \in S)(e * x = x)$$

ESEMPIO:

$\bullet$  In  $(\mathbb{Z}, -)$ ,  $0$  è un elemento neutro a destra ma non a sinistra

$$(1) - 0 = 1 \quad \text{ma} \quad 0 - (1) = -1 \neq 1$$

## ELEMENTO NEUTRO o UNITA'

$\forall e \in S$  si dice elemento neutro se è neutro a destra  
e a sinistra  $\rightarrow$  ESEMPIO: In  $(\mathbb{N}, *)$ ,  $1$  è ELEMENTO NEUTRO.

L'ELEMENTO NEUTRO  
DI SOLITO VIENE  
CHIAMATO "UNITA"

## TEOREMA (DELL'UNICITA' DEGLI ELEMENTI NEUTRI)

T.H: Sia  $(S, *)$  struttura algebrica con  $*$  operazione binaria interna,

Se  $d \in S$  è neutro a destra e  $l \in S$  è neutro a sinistra, allora  $d = l$ .

In particolare  $l$  è l'unico elemento neutro, l'unico elemento neutro a destra, l'unico elemento neutro a sinistra, di  $(S, *)$

DIM  $\underline{l * d = l}$ , ma  $\underline{l * d = d}$ , quindi  $\underline{l = d}$

PER DEFINIZIONE

PER DEFINIZIONE

↳ Però, è possibile avere due elementi neutri (o più) a destra, MA QUESTO vuol dire che non ci sono elementi neutri a sinistra, altrimenti sarebbero uguali MONDO DE

- Un semigruppo con elemento neutro si dice monoidale.

↳ ESEMPIO:

- $(\mathbb{N}, +)$  è un monoidale perché  $0$  è un elemento neutro

• Un'altra notazione del monoidale è  $(S, *, \mu)$  dove  $\mu$  è l'elemento neutro  $\rightarrow$  SI VIENE DATO ESPlicitamente L'ELEMENTO NEUTRO

↳ ESEMPIO:

- $(\mathbb{N}, +, 0)$

- $(\mathbb{Z}, +, 0)$

- $(\mathbb{N}, \cdot, 1)$

- $(P(S), \cap, S)$  Perché  $(\forall x \in P(S))(S \cap x = x)$

CON  
 $x \subseteq S$   
PERCHÉ  
 $x \in P(S)$

- $(P(S), \cup, \emptyset)$

## ESEMPIO:

• Monoido delle parole su un alfabeto. Gli elementi si a  
ALFABETO INSIEME DI CARATTERI SI DICONO LETTERE

Premoto  $A = \{ \dots \}$  → AD ESEMPIO:  $A = \{ a, b, c, d, e, \dots, z \}$

$$S = \{ x \mid (\exists m \in \mathbb{N}) ((\exists x_1, \dots, x_m \in A) (x = x_1 x_2 \dots x_m)) \}$$

METTO UN CARATTERE VICINO ALL'ALTRO

↳  $S$  è l'insieme delle parole (finita) su  $A$

→ Esiste la parola nuda (con  $m=0$ ) che dice  $\emptyset$

COME FORMO IL MONOIDE?

$$* = ((S \times S) \times S, g)$$

↓  
cerc funzione  
SERVIRÀ PER:

$$(\forall x_1, x_2, x_3 \in S) ((x_1, x_2), x_3) \in g \iff x_3 = x_1 x_2$$

METTERE UNA VERSO L'ALTRA

$$*: (x_1, x_2) \in S \times S \mapsto x_1 x_2 \in S$$

↳ ESEMPIO:

$$\cdot CA * SA = CASA$$

$(S, *, \emptyset)$  è un monoido

\* si dice giustapposizione o concatenazione

↳ Operazione non commutativa ma associativa.

Corrispondenza esercizi 27/10/2021 (LEZIONE 19)

•  $\alpha: (x,y) \in \mathbb{Z} \times \mathbb{Z} \mapsto x+y+1 \in \mathbb{Z}$

$\alpha$  è commutativa? cioè  $x\alpha y = y\alpha x$

Sì, è commutativa perché  $x+y+1$  è commutativa

$\alpha$  è associativa? cioè  $(x\alpha y)\alpha z = x\alpha(y\alpha z)$

Sì, è associativa

ELEMENTO NEUTRO di  $\alpha$ ? cioè  $u \in \mathbb{Z}: (\forall x \in \mathbb{Z}) \alpha u = x$

L'ELEMENTO NEUTRO è  $-1$  perché  $x-1+1 = x$

$$\hookrightarrow u = -1 \quad -1 \alpha x = x \Leftrightarrow x\alpha -1 = x$$

•  $\beta: (x,y) \in \mathbb{Z} \times \mathbb{Z} \mapsto -x-y \in \mathbb{Z}$

COMMUTATIVITÀ? Sì

ASSOCIAZIONALITÀ? Sì

ELEMENTO NEUTRO?  $(\forall x \in \mathbb{Z})(-1 \beta x = x)$

↪ L'ELEMENTO NEUTRO È  $-1$

•  $\gamma: (x,y) \in \mathbb{Z} \times \mathbb{Z} \mapsto 2 \cdot x \cdot y \in \mathbb{Z}$

COMMUTATIVITÀ? Sì

ASSOCIAZIONALITÀ? Sì

ELEMENTO NEUTRO? No perché  $\frac{1}{2} \in \mathbb{Q}$  ma non è un numero intero, quindi non posso moltiplicare per  $\frac{1}{2}$

•  $\delta: (x,y) \in \mathbb{N} \times \mathbb{N} \mapsto x \cdot 10^y \in \mathbb{N}$

COMMUTATIVITÀ? No, perché  $(1,2) \delta = 100 \neq 2,1 \delta = 20$

ASSOCIAZIONALITÀ? No

ELEMENTO NEUTRO? A sinistra non esiste, a destra è 0

## OPERAZIONE OPPOSTA

Sia date  $\alpha: (x,y) \in S \times S \mapsto x \alpha y \in S$

l'operazione opposta di  $\alpha$  sarà  $\bar{\alpha}$ :

$$\bar{\alpha}: (x,y) \in S \times S \mapsto y \bar{\alpha} x \in S$$

### DEFINIZIONE DI OPERAZIONE OPPOSTA

Sia  $(S, \alpha)$  una struttura algebrica ed una operazione binaria.

l'operazione  $\bar{\alpha}: (x,y) \in S \times S \mapsto \bar{\alpha}(y,x) \in S$

si dice **operazione opposta** di  $\alpha$

l'operazione opposta è una operazione di operazioni  
(o anche, operazione di relazioni).

↳ In particolare, l'operazione opposta è **duale**, infatti  
fatto due volte ci viene date le stesse cose  
di partenza  $\rightarrow$  Infatti, l'operazione opposta è chiamata  
**operazione duale**



$$(\bar{\alpha}): (x,y) \in S \times S \mapsto y \bar{\alpha} x = x \alpha y \in S^*$$

Per verificare che le funzioni  $\alpha$  e  $(\bar{\alpha})$  sono la stessa  
funzione, è necessario verificare che siano le stesse  
coppie:

$$\alpha = ((S \times S) \times S, g) \quad (\bar{\alpha}) = ((S \times S) \times S, (\bar{g}))$$

Due funzioni sono uguali se hanno lo stesso dominio  
lo stesso codominio e lo stesso grafico.

Quindi  $\alpha = (\bar{\alpha})$  dato che hanno anche lo stesso grafico.<sup>①</sup>

• Se  $\alpha$  è commutativa, allora  $\alpha = \bar{\alpha}$ .

$$\hookrightarrow y \alpha x = x \bar{\alpha} y = y \bar{\alpha} x = x \alpha y$$

• Gli elementi neutri di  $\alpha$ , in  $\bar{\alpha}$  si scambiano.

↳ AD ESEMPIO:

Se  $d$  è un elemento neutro a DX di  $(S, \alpha)$ , cioè  $(\forall y \in S)(y \alpha d = y) \leftrightarrow (\forall y \in S)(d \bar{\alpha} y = y)$ , quindi  $d$  è elemento neutro a SX di  $(S, \bar{\alpha})$ .

Questi principi vengono detti principi di dualità.

↳ DA QUI CAPPANO CHE È INUTILE DEMONSTRARE UNA LEGGE ANCHE PER LE OPERAZIONI OPPOSTE DATO CHE POI TUTTO SI RIFLETTE

• L'operazione oposta puo' essere definita come operazione unaria sull'insieme delle operazioni su  $S$ .

↳ È UN SOTTOINSIEME  
DELLE  $\mathcal{P}(\mathcal{P}(\mathcal{P}(S \times S \times S)))$

## INSIENE DELLE OPERAZIONI DI $S \times S$ IN $S$

L'insieme delle operazioni di  $S \times S$  in  $S$  lo chiamo

$\text{MAP}(S \times S, S) \rightarrow$  È UN INSIEME PERCHÉ LE  
OPERAZIONI SONO DELLE  
FUNZIONI CON COPPIE APPARTENENTI  
ALLE  $\mathcal{P}(\mathcal{P}(\mathcal{P}(S \times S)))$

↓  
INSIEME DELLE  
OPERAZIONI BIOPPIE  
INTERNE IN  $S$

SONO TUTTI GLI  $x \in \mathcal{P}(\mathcal{P}(\mathcal{P}(S \times S)))$   
TAI CHE SODDISFANO QUELLA COSA

## OPERAZIONE "SEGNATO"

Definisco l'operazione segnato

LE FUNZIONI SONO SEMPRE  
INSIEMI E IN OJANTO TALI POSSONO  
ESSERE MANCATI DA ALTRE PARTI

$\neg : \alpha \in \text{MAP}(S \times S, S) \mapsto \bar{\alpha} \in \text{MAP}(S \times S, S) \rightarrow$  SONO SEMPRE  
OPERAZIONI  
OPERAZIONE  
UNARIA

La dualità del segnato si esprime dicendo

Che  $\neg^{-1} = \neg \rightarrow$  SEGNATO ALLA MENO → L'INVERSA DEL SEGNATO  
 $\neg$  È UGUALE A SEGNATO È ANCORA SEGNATO

Visto che  $\neg$  ha un inverso, allora è biunivoco.

# PARTI STABILI

Dato la struttura algebrica  $(S, *)$  con  $S \neq \emptyset$  e  $*$  un'operazione binaria interna di  $S$ , considero un certo sottoinsieme  $T \subseteq S$  ↴

- Cosa succede se restringo  $*$  a  $T \times T$ ?

$T$ , sottoinsieme di  $S$ , si dice forte chiusa (o stabile) di  $(S, *)$  se l'immagine di  $*|_{T \times T}$  appartiene ancora a  $T$ .

↳ NON È DETTO CHE YADA IN T

Quindi se:  $\forall x, y \in T, *|_{T \times T}(x, y) \in T$

↳ LA RESTRIZIONE → POSSO FARE DI  $*$  A  $T \times T$   
LA RESTRIZIONE PERCHÉ  $T \times T \subseteq S \times S$

## ESEMPIO:

- Considero  $(\mathbb{N}, +)$  e prendo come sottoinsieme di  $\mathbb{N}$  lo 0. Quindi  $T = \{0\}$ .

↳ 0 è una forte stabile di  $(\mathbb{N}, +)$ ? Vediamo

$$\text{Im } +|_{\{0\} \times \{0\}} \subseteq \{0\}$$



Si, perché la somma di 0+0 è sempre 0  $\in \{0\}$

Quando abbiamo un monoido, il singleton dell'unità è sempre una parte stabile

GL'ELEMENTO NEUTRO

↳ 1 è una parte stabile di  $(\mathbb{N}, +)$ ?

$1+1=2$ , ma  $2 \notin \{1\}$ , quindi  $\{1\}$  non è una parte chiusa in  $(\mathbb{N}, +)$

Le somme dei numeri pari è ancora pari, quindi i numeri pari sono una parte chiusa in  $(\mathbb{N}, +)$

• Se  $t$  è una parte stabile, allora posso scrivere:  
 $\rightarrow$  SEMPRE DI  $(S, *)$

$(t, *)$   $\rightarrow$  E' UN ABUSO DI NOTAZIONE  
 PERCHE QUESTO \* IN REALTA'  
 E' UNA RESTRIZIONE DI \*  
 USATO IN  $(S, *)$

• Se  $t$  è una parte stabile,  $*_{\text{txt}}$  è un'operazione di  $t$ .

$$*_{\text{txt}} = ((\text{Ext}) \times t, g) \quad \text{dove } g \text{ è:}$$

$$g = \{(x, y, z) \in t^3 \mid *_{\text{txt}}(x, y) = z \} \rightarrow g \text{ SONO TUTTE LE TERNE}$$

$y$   
 $\text{Ext} \times t \rightarrow$  TERNE  
 ORDINATE

$\downarrow$   
 L'IMMAGINE DELLE PRIME  
 DUE E' UGUALE ALLA  
 TERZA COORDINATA

•  $*_{\text{txt}}$  si dice operazione indotta da  $*$  su  $t$

ESEMPIO:

• Chi è  $+_{\{\{0\}\} \times \{\{0\}\}}$ ?

$$+_{\{\{0\}\} \times \{\{0\}\}} = ((\{\{0\}\} \times \{\{0\}\}) \times \{\{0\}\}, \{\{(0, 0, 0)\}\})$$

$\rightarrow$  SCRITTO  
 E' SPPLICATAMENTE

$\downarrow$   
 g SONO TUTTI GLI  
 $(x, y, z) \in \{\{0\}\} \times \{\{0\}\} \times \{\{0\}\}$   
 TALI CHE  $+_{\{\{0\}\} \times \{\{0\}\}}(0, 0)$  SIA  
 UGUALE A 0

• Consideriamo un ento  $m \in \mathbb{N}$  e:

$$m \cdot \mathbb{N} = \{m \in \mathbb{N} \mid (\exists k \in \mathbb{N})(m = k \cdot m)\} \rightarrow$$

HO PRESO TUTTI GLI  
 $m$  CHE SONO  
 MULTIPLI DI  $m$

$m \cdot \mathbb{N}$  è una parte stabile  
 qualunque sia  $m$ !

$\downarrow$   
 SE  $m \in \mathbb{N}$ ,  $m \cdot \mathbb{N}$   
 SONO I NUMERI PARI

$\hookrightarrow$  Devo mostrare che le somme di due elementi  
 che si trovano in  $m \cdot \mathbb{N}$  siano ancora in  $m \cdot \mathbb{N}$

Siamo  $x, y \in m \cdot \mathbb{N}$

Per definizione  $(\exists k_1, k_2 \in \mathbb{N})(x = k_1 \cdot m \wedge y = k_2 \cdot m)$ .

$$x + y = k_1 \cdot m + k_2 \cdot m = (k_1 + k_2) \cdot m$$

Quindi  $x + y \in m \cdot \mathbb{N}$  perché è ancora un multiplo di  $m$ . Quindi  $m \cdot \mathbb{N}$  è una parte stabile.

↳ Quindi ci sono tante parti stabili quante sono i numeri naturali

Anche  $\{0\}$  rientra in  $m \cdot \mathbb{N}$  perché  $1m \cdot 0 \cdot \mathbb{N} = 0 \in \{0\}$

Si può dimostrare che  $m \cdot \mathbb{N}$  sono tutte e sole le parti stabili del monoido  $(\mathbb{N}, +)$ .

### PERCHE' LE PARTI CHIUSE SONO IMPORTANTI?

Le parti stabili sono importanti perché ci permettono di studiare qualcosa un po' grande, misteriosa, a partire da delle sue parti un po' più semplici.

### UNA PARTE CHIUSA E' UNA SOTTO(STRUTTURA)

Se  $S$  è una struttura algebrica e  $T$  è una sua parte chiusa, allora possiamo scrivere:

$T \subseteq S \rightarrow$  SI LEGGE:  $T$  E' UNA  
SOTTO(STRUTTURA)  
DI  $S$

### ESEMPIO:

- $(\mathbb{N}, +)$  è un monoido, quindi  $m \cdot \mathbb{N}$  è un sottomonoido
- $(\mathbb{N} \setminus \{0\}, +)$  è un semigruppo, quindi  $m \cdot \mathbb{N} \setminus \{0\}$  è un sottosemigruppo

## PROPRIETA' CONSERVATE NELLE PARTI STABILI

- Le proprietà commutative sono conservate per le parti stabili  $\rightarrow$  L'OPERAZIONE SU C' HA LA FINE E' LA STESSA CHE HO IN S
- Le proprietà associative sono conservate per le parti stabili
- L'elemento neutro non è una proprietà conservata perché sottoinsieme non conservarsi.  
↳ ESEMPIO:  
 $(\mathbb{N}, +)$  è un semigruppo che ha un elemento neutro, ma  $\mathbb{N} \setminus \{0\}$  è un sottosemigruppo senza elemento neutro  $\rightarrow$  I sottosemigruppi possono perdere degli elementi

## INVERTIBILITÀ

Sia  $(S, *)$  una struttura algebrica con elemento neutro  $n$ .

- Se  $x \in S$  e  $(\exists y \in S)(x * y = n)$ ,  $y$  si dice inverso destro di  $x$ .  $x$  si dice invertibile a destra.
- Se  $x \in S$  e  $(\exists y \in S)(y * x = n)$ ,  $y$  si dice inverso sinistro di  $x$ .  $x$  si dice invertibile a sinistra.
- Se  $x \in S$  e  $(\exists y \in S)(x * y = n = y * x)$ ,  $y$  si dice inverso di  $x$ .  $x$  si dice invertibile.

ESEMPIO:

In  $(\mathbb{Q}, \cdot)$ ,  $\frac{1}{3}$  è l'inverso di 3 perché  $\frac{1}{3} \cdot 3 = 3 \cdot \frac{1}{3} = 1$   
dato che 1 è l'unità di  $(\mathbb{Q}, \cdot)$

# TEOREMA (SULL'UNIETÀ DELL'INVERSA)

T.H: Sia  $(S, *)$  una struttura algebrica con elemento neutro  $n$ , sia  $x \in S$ .

Se  $x$  è invertibile a destra e a sinistra, allora  $x$  è invertibile ed ha un'unica inversa a sinistra e un unico inverso a destra.

DIM

Sia  $l$  l'inverso sinistro di  $x$  e  $d$  l'inverso destro di  $x$ .

$$l * x = n \rightarrow (l * x) * d = n * d = d$$

Per l'associazività, (TUTTE LE STRUTTURE ALGEBRICHE CHE FAREMO SONO ASSOCIAZIVE)  
 $l * (x * d) = l * n = l$

Quindi  $l = d$

Visto che l'inverso è unico, lo indichiamo con  $x^{-1}$

$x^{-1}$  è l'inverso  
di  $x$

## GRUPPO E GRUPPO ABELIANO

Un semigruppo in cui tutti gli elementi sono invertibili si dice **gruppo**.

Un gruppo la cui operazione è commutativa si dice **gruppo abeliano**.

↳ Se  $(g, *)$  è un gruppo commutativo, si dice **gruppo abeliano**

Un monoido  $(m, *)$  si dice **gruppo** se tutti gli elementi di  $m$  sono invertibili  $\rightarrow$  ESEMPIO:  $(\mathbb{N}, +)$  NON È UN GRUPPO

## ELEMENTO SIMMETRICO, INVERSO E OPPOSTO

Un elemento invertibile si dice anche simmetrizzabile.

Soltamente, l'inverso di un elemento ( $0$ , anche il simmetrico di quell'elemento), viene chiamato "opposto" se ci troviamo in un monade in mensione additiva.

### ESEMPIO:

In  $(\mathbb{Z}, +)$ ,  $-2$  è l'opposto di  $2$ , anche se non è sbagliato dire che è il simmetrico o l'inverso additivo di  $2$ .

↓

Soltamente, dire che un numero è l'inverso di un altro si ha quando ci troviamo in una mensione moltiplicativa.

COSA CI INDICA IL FATTO CHE ABBIANO UN INVERSO? d'essere un inverso ci indica che se faccio il prodotto di qualcosa allora posso anche tornare indietro.

↓

Altro tipo struttura con delle simmetrie.

↳ Posso applicare delle funzioni a queste "cose" per lasciare lo stato così com'è (ad esempio lo stato di una figura)

↓

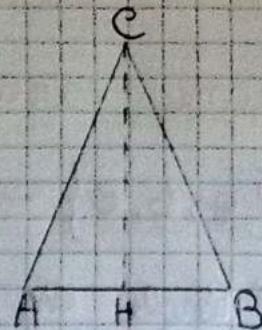
### ESEMPIO:

Premendo un triangolo isoscele  $ABC$ , quindi con  $AH = HB$

UNA FIGURA,  
UNO STATO  
ecc.

Vogliamo trattare tutti i movimenti del piano che lascino il triangolo  $ABC$ , uguale a se stesso.

CIOE LA FIGURA "TRIANGOLI".



↳ AD ESEMPIO:

- la traslazione del triangolo di 1 cm a sinistra non lascia il triangolo uguale a se stesso (cioè sovrapponibile)
  - la riflessione del piano intorno all'altreto lascia il triangolo uguale a se stesso
  - la traslazione nulla e la rotazione nulla lascia il triangolo così com'è
- AD OGNI PUNTO ASSOCIA SE STESO

Quindi, l'insieme delle simmetrie di un triangolo isoscele è un gruppo. Perché?

↳ Se compongo due applicazioni che lasciano il triangolo uguale a se stesso, il triangolo rimarrà uguale a se stesso  $\rightarrow$  la composizione è associativa e si ha un'identità, quindi l'insieme delle simmetrie è un monade.

↳ Ogni simmetria ha quelle inverse

(AD ESEMPIO, la riflessione ha come inversa la riflessione stessa)

RIFLETTI UNA VOLTA E HO IL TRIANGOLI CON A E B INVERTITI, RIFLETTI DI NUOVO E HO A E B AL LORO POSTO

Sto dicendo che le strutture con tutte le funzioni che sono simmetrie, con la composizione, è un gruppo.

In particolare, è un gruppo abeliano, infatti riflessione controso identità sono uguale a identità controso riflessione ecc.

# Correlazione esercizi 29/10/2021 (LEZIONE 15)

2.  $A = \{a, b, c\} \rightarrow$  L'OPERAZIONE E' LA GIUSTAPOSIZIONE

•  $I_1 =$  "Parole che contengono una sola 'a'"

$I_1$  non è una parte chiusa perché fra i due elementi dell'insieme  $I_1$ , la loro giustaposizione non si trova in  $I_1$ .

$\hookrightarrow a \in I_1$  ma  $aa \notin I_1 \rightarrow$  parte non chiusa

"LA PAROLA "a"  
HA UNA SOLO a  
ANCHE "b" ECC.."

LA COMPOSIZIONE DI DUE PAROLE  
CON UNA SOLO a NON DÀ UNA  
PAROLA CON UNA SOLO a

•  $I_2 =$  "Almeno una 'a'"

Prendo qualunque  $x, y \in I_2$ . Cioè sto dicendo che:

$\exists x_1, \dots, x_m \in A: x = x_1 \dots x_m$  e

$\exists y_1, \dots, y_n \in A: y = y_1 \dots y_n$  e che almeno

se uno di questi  $x_i$  e di questi  $y_j$  è una 'a'. Cioè:

DIMOSTRARE

PER TUTTI I

ALLORA

DEVO OSSERARE

GENERICI

$((\exists i, j \in \mathbb{N})(1 \leq i, j \leq m)) (x_i = a = y_j) \rightarrow$  SIA X CHE Y HANNO ALMENO UNA A PERCHE' APPARTENGONO A  $I_2$

Faccio la giustaposizione XY. Quindi:

SE DEVO

DIMOSTRARE

EHE E'

UNO EHE

NON VA

ALLORA

USO UN

CONTROESSEMPO (cioè  $x_i$ ) allora  $XY \in I_2$

$XY = x_1 x_2 x_3 \dots x_m y_1 y_2 y_3 \dots y_n$  ma dato che

almeno un elemento di X ha una "a"

Di conseguenza  $I_2$  è una parte chiusa.

Inoltre,  $I_2$  è anche un sottogruppo perché associativo, ma non un sottomonide dato che non c'è l'elemento neutro (la parola vuota non appartiene ad A)

6.  $(P(N), \Delta)$  è un gruppo? è abeliano?

→ Vediamo quale può essere l'elemento neutro.  
E' il vuoto  $\rightarrow X \Delta \emptyset = (X \cup \emptyset) \setminus (X \cap \emptyset) = X \setminus \emptyset = X$

Per l'esplorazione delle differenze simmetriche,  
 $(\forall x, y)(X \Delta Y = (X \cup Y) \setminus (X \cap Y))$ . Le differenze simmetriche  
sono commutative perché lo sono  $X \cup Y$  e  $X \cap Y$ .  
Inoltre, abbiamo già visto che sono associate.  
 $\hookrightarrow (\forall x, y, z)((X \Delta Y) \Delta Z = X \Delta (Y \Delta Z))$

Quindi mostriamo che  $(P(N), \Delta)$  è un monade  
commutativo.

↳ Bisogna vedere se ci sono gli elementi inversi, cioè,  
nagliamo trovare un  $Y$  che per ogni  $X$  dia  
l'insieme vuoto. Cioè:  $X \Delta Y = \emptyset$

↓

Questo elemento è  $X$  stesso perché  $(\forall x \in N)(x \Delta x = \emptyset)$   
Inoltre, visto che  $\Delta$  è commutativo,  $X$  è l'unico  
inverso perché è sia inverso destro che inverso  
sinistro.

↳ Quindi  $(P(N), \Delta)$  è un gruppo abeliano perché  
ogni elemento  $X$  ha un'inversa  $Y$  ed è un  
gruppo commutativo

$$S. \quad a = \{1, 2, 3\}$$

$$\boxed{\text{MAP}_{\text{BI}}(a, a) := \text{Sym}(a)}$$

d'insieme delle applicazioni biettive di  $a$  in  $a$

d'insieme simmetrico di  $a$

Consideriamo l'insieme delle funzioni biettive di  $a$  in  $a$  ( $\text{MAP}_{\text{IN}}(a, a)$ )

↓

Prendo l'operazione "composizione", quindi:

COMPOSIZIONI  
DI FUNZIONI  
UNIFORME  
E' ANCORA  
INIEZIONE  
  
E' DUE  
APPLICAZIONI  
DI A IN C  
SMENTI  
POSSO COMBINARLE  
PER FORMARE  
UNA NUOVA  
APPLICAZIONE  
DA B IN C

↳ Questo è un monoidre perché l'elemento neutro è  $\text{Id}_a$  e tale è associatività per la composizione di funzioni.

In  $\text{MAP}_{\text{IN}}(a, a)$  ci sono anche tutte le applicazioni biettive, quindi  $(\text{MAP}_{\text{BI}}(a, a), \circ)$  è un sottomonoidre di  $(\text{MAP}_{\text{IN}}(a, a), \circ)$

↓

Inoltre, risiamo già che ogni applicazione biettiva ha l'inverso, quindi:

$(\text{Sym}(a), \circ)$  è un gruppo ma non abbiamo dato che  $\circ$  non è commutativo

AD ESEMPIO:  $\alpha: a \rightarrow a$

↓  
"gruppo"  
"esso"

$$\begin{aligned} \alpha(1) &= 2 \\ \alpha(2) &= 3 \\ \alpha(3) &= 1 \end{aligned}$$

$$\begin{aligned} \alpha^{-1}(1) &= 3 \\ \alpha^{-1}(2) &= 1 \\ \alpha^{-1}(3) &= 2 \end{aligned}$$

Prendo poi  $\beta: a \rightarrow a$

$$\begin{aligned} \beta(1) &= 2 \\ \beta(2) &= 1 \\ \beta(3) &= 3 \end{aligned}$$

↓  
de loro composizione:

$$\begin{aligned} (\alpha \circ \beta)(1) &= (\alpha(\beta(1))) = \alpha(2) = 3 \\ (\beta \circ \alpha)(1) &= (\beta(\alpha(1))) = \beta(2) = 1 \end{aligned}$$

$\Rightarrow \alpha \circ \beta \neq \beta \circ \alpha$

## ELEMENTO NEUTRO E INVERSO NELLE SOTTOSTRUTTURE

Gli elementi neutri e gli inversi possono anche non trasportarsi nelle sottostrutture

AD ESEMPIO:

- Consideriamo le strutture:

$(\mathbb{Z}, +)$  che è un monoide

La parte chiusa  $(\mathbb{N} \setminus \{0\}, +)$  è un sottogruppo di  $(\mathbb{Z}, +)$  ma non ha più l'elemento neutro  $\rightarrow$  non è un sottomonoide

$$(\mathbb{N} \setminus \{0\}, +) \triangleleft (\mathbb{Z}, +)$$

2) INTERSEZIONE DI PARTI CHIUSE È ANCORA UNA PARTE CHIUSA

Sia  $(S, *)$  una struttura algebrica e sia  $t$  un sottoinsieme delle parti di  $S$  ( $t \subseteq P(S)$ ) tale che  $\forall x \in t$ ,  $x$  è una parte chiusa di  $S$ .  
L'intersezione unaria di  $t$  ( $\cap t$ ) è una parte chiusa di  $S$

AD ESEMPIO:

$t$  è un insieme di alcuni sottoinsiemi di  $\mathbb{N}$

Dato la struttura algebrica  $(\mathbb{N}, +)$ , posso prendere  $t = \{2\mathbb{N}, 3\mathbb{N}\} \subset P(\mathbb{N})$ .

Voglio che, visto che  $2\mathbb{N}$  e  $3\mathbb{N}$  sono parti chiuse di  $\mathbb{N}$ ,  $\cap t = 2\mathbb{N} \cap 3\mathbb{N}$  sia ancora una parte chiusa di  $\mathbb{N}$

DIM  $\rightarrow$  Devo far vedere che  $\forall x, y \in \mathbb{N}, x * y \in \mathbb{N}$   
cioè elementi degli elementi di  $\mathbb{N}$

Prendiamo  $x, y \in \mathbb{N}$ . Per definizione di  $\mathbb{N}$ ,

$(\forall z \in \mathbb{N})(x, y \in z)$  Ne ogni  $z \in \mathbb{N}$  è una parte

chiusa, quindi  $x * y \in z$  per la definizione di parte chiusa.

$\hookrightarrow (\forall z \in \mathbb{N})(x * y \in z)$ , quindi per definizione  $x * y \in \mathbb{N}$

$\downarrow$   
 $\mathbb{N}$  è una parte chiusa

## DEFINIZIONE DI SOTTOGRUPPO

Se  $(g, *)$  è un gruppo,  $S$  è un sottogruppo  
di  $g$  (cioè  $S \leq g$ ) se  $S$  ha gli inversi

$\hookrightarrow$  ESSERE UN SOTTOGRUPPO SIGNIFICA ESSERE UNA  
PARTE CHIUSA CHE HA ANCHE GLI INVERSI

## SOTTOSTRUTTURE GENERATE

All'istante visto che all'interno di una struttura  
ci sono tante sottostrutture

$\hookrightarrow$  Voglio trovare le più piccole sottostrutture che  
contengono un certo sottoinsieme

### AD ESEMPIO:

Prendo  $(\mathbb{N}, +)$  in questo mondo.

$\hookrightarrow$  Voglio il "più piccolo"  $S \leq \mathbb{N}$  tale che  $2 \in S$

$\hookrightarrow$  Visto che è un sotomonoido allora deve essere  
una parte stabile  $\rightarrow$  Ci deve stare  $2, 4, 6$  ecc...

$\downarrow_{2+2}$   $\downarrow_{2+2+2}$   
"Il più piccolo" lo codifico nel senso dell'intersezione

$\hookrightarrow$  Voglio l'intersezione di tutte le strutture  
che contengono  $2 \rightarrow$  In questo caso il

sotomonoido è "I NUMERI PARI"

## SOTTOSTRUTTURA GENERATA DA $t$

Sia  $(S, *)$  una struttura astratta e prendo un sottoinsieme di  $S$  ( $t \subseteq S$ ). La sottostruzione generata da  $t$  (si scrive  $\langle t \rangle$ ) è:

$$\langle t \rangle := \bigcap \{ X \in P(S) \mid X \subseteq S \wedge t \subseteq X \} (=: \bigcap_{X \subseteq S, t \subseteq X} X)$$

E' UNA DEFINIZIONE

E' UNA SOTTOSTRUZIONE  
DELLO STESSO TIPO DI S

UN ALTRA  
NOTAZIONE E'

↳ Ora allora definito cosa significa essere "il più piccolo", ma come facciamo a trovare tutte le sottostruzioni che contengono  $t$ ?

↳ Abbiamo delle caratterizzazioni, di seguito riportate per monoidi e per gruppi

## CARATTERIZZAZIONI DELLE STRUTTURE GENERATE

### MONOIDI

$$\langle t \rangle = \{ X \in S \mid (\exists m \in \mathbb{N})(\exists x_1, \dots, x_m \in t)(X = x_1 * \dots * x_m) \}$$

NON SONO DEFINIZIONI,  
 $\langle t \rangle$  E' PROPRIO QUESTO  
IN QUESTI CASI

STO DICENDO CHE  $\langle t \rangle$ , cioè l'intersezione  
unaria di tutte le parti di  $S$ , ecc. (DEFINIZIONE)  
SONO TUTTI GLI ELEMENTI CHE APPARTENGONO  
A S TALI CHE SI SCRIVANO COME COMPOSIZIONE  
DI  $m$  ELEMENTI CHE APPARTENGONO A  $t$

### GRUPPI

$$\langle t \rangle = \{ X \in S \mid (\exists m \in \mathbb{N})(\exists e_1, \dots, e_m \in \{-1, 1\})(\exists x_1, \dots, x_m \in t)(X = x_1^{e_1} * \dots * x_m^{e_m}) \}$$

LA DIFFERENZA TRA MONOIDI E NEL MONOIDE  
GRUPPO E' CHE CI SONO O NENO → SI TOLGONO LE E  
LE INVERSE

$x^{-1}$  RAPPRESENTA L'INVERSA DI  $x$

### DIMOSTRAZIONE DELLA CARATTERIZZAZIONE DEI MONOIDI

Per dimostrare che  $\langle t \rangle = \{ X \in S \mid (\exists m \in \mathbb{N})(\exists x_1, \dots, x_m \in t)(X = x_1 * \dots * x_m) \}$   
esiamo la doppia inclusione, dalla tautologia della  
doppia implicazione.

↳ Per far vedere che due insiemi sono uguali dobbiamo vedere che  $\langle t \rangle \subseteq \{ X \in S \mid (\exists m \in \mathbb{N})(\dots) \}$  e viceversa,  
per vedere che  $\{ X \in S \mid (\exists m \in \mathbb{N})(\dots) \} \subseteq \langle t \rangle$

( $\subseteq$ ) Vediamo prima che  $\langle t \rangle \subseteq \{x \in S | (\exists m \in N)(\dots)(\dots)\}$

Per comodità, chiamiamo:

$$b = \{x \in S | (\exists m \in N)(\exists x_1, \dots, x_m \in t)(x = x_1 * \dots * x_m)\}$$

$\langle t \rangle$  è una P(S) perché è l'intersezione di certe P(S) che contengono  $t$ .  
Faccio vedere che b è una parte chiusa di S.  
Infatti, se  $x, y \in b$ , allora  $x = x_1 * \dots * x_m$  e  $y = y_1 * \dots * y_n$ .  
Allora  $x * y = (x_1 * \dots * x_m) * (y_1 * \dots * y_n) = x_1 * \dots * x_m * y_1 * \dots * y_n \in b$ , quindi  $b$  è chiusa.

Premo  $x, y \in b$ .

Per la definizione di  $b$ ,  $x * y \in b$

↪ Infatti,  $(\exists m \in N)(x = x_1 * \dots * x_m)$  ed  $(\exists n \in N)(y = y_1 * \dots * y_n)$ ,  
quindi  $(\exists m \in N)(\exists n \in N)$  dove  $x * y = x_1 * \dots * x_m * y_1 * \dots * y_n$ ,  
quindi queste cose ( $x * y$ ) sta ancora in  $b$ .

DA SOLITO SI FOLGLIE ALTA  
DEFINIZIONE CHE LA STANZA VUOTA  
E' L'ELEMENTO NEUTRO

↪ Posso anche definire il caso in cui  $m=0$ , quindi  
cioè che  $0 \in b$  e questo sarà l'elemento neutro.

Di conseguenza  $b$  è una sottostruzione di  $S$  ( $b \leq S$ )

Se  $b \leq S$  allora sto dicendo che  $b$  è uno  
degli insiemi di cui faccio l'intersezione unaria.

↪ Infatti,  $b$  contiene  $t$  ( $t \subseteq b$ ) perché se prendo  
 $m=1$ , allora da definizione  $(\exists x_1 \in t)(x = x_1)$ ,  
quindi  $x \in t \rightarrow b$  dunque l'insieme degli elementi  
di  $t$  che, per estensionalità, è proprio  $t$ .

Quindi  $\langle t \rangle \subseteq b$  perché  $b$  è uno degli insiemi di  
cui faccio l'intersezione.

( $\supseteq$ ) Vogliamo dimostrare che  $\{x \in S | (\exists m \in N)(\dots)(\dots)\} \subseteq \langle t \rangle$

Vogliamo quindi dimostrare che tutte le sottostruzione  
di  $S$  che contengono  $t$ , contengono anche  $b$ .

↪ Dovò far vedere che  $(\forall x \leq S)(t \subseteq x \rightarrow b \subseteq x)$ ,

perché da ciò segue che  $b \subseteq \langle t \rangle$  → Dato che  $x$  è una  
sottostruzione di  $S$  e  $b$  fa parte di  $x$ .

Sia  $X$  una parte di  $S$  e che contenga  $t$   
 $\hookrightarrow X \subseteq S \wedge t \subseteq X$   $\hookrightarrow$  C'È UNA GENERICA SOTTOSTRUTTURA CHE CONTIENE  $t$ .

Prendo poi un generico elemento di  $b$   
 $\hookrightarrow Y = Y_1 * \dots * Y_m : Y_1, \dots, Y_m \in T$

Poiché  $X$  è una parte chiusa, allora  $g \in X$ .

Dato che un generico elemento di  $b$  appartiene ad  $X$ ,  
vuol dire che  $b \subseteq X$ .

Ho quindi fatto vedere che per una qualunque  
sottostruttura di  $S$  che contiene  $t$ , contiene anche  $b$ .  
Di conseguenza  $b \subseteq \langle t \rangle$

### ESEMPI:

Nell'esempio di prima, dare obbligatoriamente il monoido  $(\mathbb{N}, +)$

$\langle 2 \rangle$  sono tutti gli elementi di  $\mathbb{N}$  che sono somma di 2 ripetuto  $m$  volte, cioè i numeri pari.

Infatti,  $t = \{2\}$ , di conseguenza 2 è l'unico elemento di  $t$ .

$\hookrightarrow x_1, x_2, x_3, \dots, x_m$  sono sempre 2.

$$X = x_1 + x_2 + x_3 + \dots + x_m = 2 + 2 + 2 + \dots + 2 \text{ in } m \text{ volte}$$

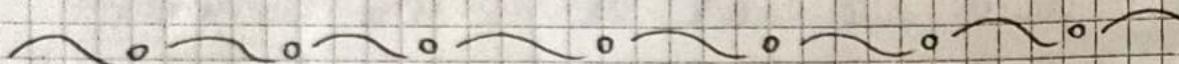
# NOTAZIONI DELLA SOTTOSTRUTTURA GENERATA

Le sottostrutture generate da  $t$  si può indicare sia con il senso le " $\{ \}$ "

↳  $t$  è UNA PARTE DI  $S \rightarrow$  UN SOTTOINSIEME

## ESEMPIO:

- Possedere sia  $\langle \{1\} \rangle$  che  $\langle 1 \rangle$
- Anche  $\langle \{a, b, c\} \rangle$  che  $\langle a, b, c \rangle$  sono equivalenti.



## ESEMPI:

- Nel monoido  $(\mathbb{N}, +)$ :

$\langle \{1\} \rangle = \mathbb{N}$  perché sono tutte le ripetizioni dell'operazione "+" con gli elementi che fanno in  $\{1\}$  (cioè 1)  
↳ È la somma di 1 per  $m$  volte con  $m$  che varia → ESEMPIO:  
$$\begin{aligned} 1 &= 1 \\ 2 &= 1+1 \\ 3 &= 1+1+1 \end{aligned}$$

$$\langle 2 \rangle = 2 \cdot \mathbb{N} \quad (\text{Tutti i numeri pari})$$

- Nel monoido  $(\mathbb{N}, \cdot)$ :

$\langle 1 \rangle = \{1\}$  perché sono tutte le possibili ripetizioni di  $1 \cdot 1 \cdot 1 \cdot 1 \cdots \cdot 1$   
↳ Inoltre questo è un sottomonoido perché contiene anche l'elemento neutro

Corsozione esercizi 02/11/2021 (LEZIONE 16)

T.H.

3)  $\langle t \rangle = \{x \in g \mid (\exists m \in \mathbb{N})(\exists \varepsilon_1, \dots, \varepsilon_m \in \{-1, 1\})(\exists x_1, \dots, x_m \in t)(x = x_1^{\varepsilon_1} * \dots * x_m^{\varepsilon_m})\}$

HP:  $(g, *)$  è un gruppo  
 $t \neq \emptyset$

$\rightarrow$  SE  $\varepsilon = -1$ , QUELLI  $x^{-1}$  RAPPRESENTA L'INVERSA

Sottoinsiemi  $\langle t \rangle$   $\stackrel{\text{DEF}}{=} \bigcap \{x \in \mathcal{O}(g) \mid t \subseteq x \wedge x \leq g\}$

la dimostrazione è uguale a quelle del coro del monade con la differenza che tra  $t \neq \emptyset$

Voglio far vedere che l'insieme  $\langle t \rangle$  e  $\{x \in g \mid (\exists m \in \mathbb{N})$  sono uguali

$\hookrightarrow$  do vedo con le doppie inclusioni

DIM

( $\subseteq$ ) Dico per vedere che:

$$\langle t \rangle \subseteq \{x \in g \mid (\exists m \in \mathbb{N})(\exists \varepsilon_1, \dots, \varepsilon_m \in \{-1, 1\})(\exists x_1, \dots, x_m \in t)(x = x_1^{\varepsilon_1} * \dots * x_m^{\varepsilon_m})\}$$

Voglio far vedere che una di quelle sottostruzione di  $g$ , di cui  $\langle t \rangle$  è l'intersezione tra tutte queste sottostruzione,

è proprio l'insieme  $\{x \in g \mid (\exists m \in \mathbb{N})(\exists \varepsilon_1, \dots, \varepsilon_m \in \{-1, 1\})(\dots)\}$

$\hookrightarrow$  Di fatto, me segue che poi  $\langle t \rangle \subseteq \{x \in g \mid (\exists m \in \mathbb{N})(\dots)\}$

$$b = \{x \in g \mid (\exists m \in \mathbb{N})(\exists \varepsilon_1, \dots, \varepsilon_m \in \{-1, 1\})(\exists x_1, \dots, x_m \in t)(x = x_1^{\varepsilon_1} * \dots * x_m^{\varepsilon_m})\}$$

dove:

• Esere una parte di  $g \rightarrow$   $E$  una cosa ovvia

• Contenere  $t \rightarrow$   $E$  ovvio perché  $x$  ha  $m+1$  ad  $\varepsilon=1$ , ovvero che  $b$  sono tutti i solo gli elementi  $x_i \in t$ , quindi  $x \in t$

• E' una sottostruzione di  $g \rightarrow$  Stesso ragionamento delle dimostrazioni della caratterizzazione dei monadi

Q.indi  $\langle t \rangle \subseteq b$

POSSO AVERE  
ANCHE LE COMBINAZIONI  
TUTTI UN SOLO ELEMENTO

(2) Dato forti vedere che  $\forall x \in S \exists y \in S$   $y \subseteq x$ ,  
 TUTTI gli  $\leftarrow$  altri  $(\forall x \in S)(\forall y \in S)(y \subseteq x)$ ; quindi preso  
 ELEMENTI di  $S$  una qualsiasi forte chiusa di  $S$  contiene  $L$ ,  
 Questa contiene anche  $b$ .

$\downarrow$   
 se  $a \in b$ ,  $b$  è una forte chiusa perché un qualunque  
 ELEMENTO di elemento di  $b$  non è altro che la composizione  
 a STAMPO  
 SIA IN  $b$  di qualunque elemento di  $t$  si trovi a  $\exists o = 1$   
 CHE IN  $c$

$\hookrightarrow$  Cioè sono o l'elemento stesso o il suo inverso,  
 quindi per ogni sottogruppo di  $S$ , l'elemento  $b$  c'è  
 ovvio dato che c'è lo suo inverso.

$\hookrightarrow$  ESEMPIO:

$x, y, z \in S$  dato  $S \leq g$  ( $S$  è un sottogruppo di  $S$ )

Quindi  $x \in S$ , ma anche  $x^{-1} \in S$ , ed anche  $x^{-1}yz$

Quindi se ho degli elementi che appartengono a  $t$ , tutti i  
 Combinazioni di questi elementi appartengono ad  $S$ .

$\hookrightarrow b$  è contenuto in tutti i sottogruppi di  $S$  che contengono  $t$

Quindi  $b \subseteq \langle t \rangle$

ELEMENTI NON  
ACCETTA UN GRUPPO

Inoltre, sappiamo che  $\langle t \rangle$  ha l'elemento neutro  
 perché ci viene assicurato dal fatto che  $t \neq \emptyset$

$\hookrightarrow$  visto che  $t \neq \emptyset$ ,  $\exists x \in t$

Essere di conseguenza, un certo  $t * t^{-1} \in b$

$\downarrow$

Ma questo  $t * t^{-1}$  è proprio l'unita, quindi  $t * t^{-1} = 1_S$

Visto che  $\langle t \rangle$  è una forte chiusa, ha l'elemento  
 neutro e ha gli inversi, è anche lui un gruppo

# ELEMENTI SIMMETRIZZABILI

Cominciamo con  $U_{(S)}$ , l'insieme degli elementi simmetrizzabili di  $S$  per riguardo  $\rightarrow$  cioè tutti gli elementi della traiettoria che sono invertibili.

$(U_{(S)}, *)$  è un gruppo?  $\rightarrow$  • C'è il dell'elemento neutro perché se  $x \in U_{(S)}$  allora  $x^{-1} \in U_{(S)}$

OPPOSIZIONE  $\rightarrow$  SIGNIFICA NESSA DIFERENZA IN PARTE, STABILE

• L'associatività risulta da  $*$  è associativo  $\rightarrow$   $x$  è invertibile perché  $S$  è non omogeneo.

• È una parte chiusa.

Perché  $U_{(S)}$  è una parte chiusa?  $\rightarrow$  Dobbiamo dimostrare che per ogni coppia di elementi simmetrizzabili, il loro prodotto è simmetrizzabile.

Prendiamo  $x \in S$  simmetrizzabili (cioè invertibili).

Per definizione:  $(\exists w, z \in S)(x * w = I_S \wedge y * z = I_S)$

ELEMENTO NEUTRO

Esiste un certo elemento che composto con  $x * y$  dà l'unità  $I_S$ , ed è  $z * w$ .

$$\hookrightarrow x * y * (z * w) \stackrel{\text{ASSOCIAtività}}{=} x * (y * z) * w = (x * I_S) * w = x * w = I_S$$

Di conseguenza  $x * y \in U_{(S)}$ , quindi  $U_{(S)} \leq S$

↪ E' UNA PARTE CHIUSA

• Inoltre, dato che  $x$  è simmetrizzabile e  $w$  è il suo simmetrico, allora anche  $w \in U_{(S)}$ , quindi ogni elemento ha l'inverso

↪  $w$  È SIMMETRIZZABILE E IL SUO SIMMETRICO È  $x$

$\hookrightarrow (U_{(S)}, *)$  è un gruppo

ESEMPI:

•  $U((\mathbb{N}, +)) = \{0\}$   $\rightarrow$  È L'UNICO ELEMENTO AD AVERE L'OPPOSTO.

•  $U((\mathbb{Z}, +)) = \mathbb{Z}$   $\rightarrow$  TUTTI GLI ELEMENTI HANNO OPPONSI.

•  $U((\mathbb{Z}, \cdot)) = \{-1, 1\}$   $\rightarrow$  AD ESEMPIO, L'INVERSO DI  $2 \in \mathbb{Z}$  È  $1/2$  MA NON STA IN  $\mathbb{Z}$ , SOLO L'INVERSO DI  $\pm 1 \in \mathbb{Z}$  STA IN  $\mathbb{Z}$ .

# MOLTIPLICAZIONE

Sia  $g$  un gruppo del tipo " $(g, \cdot)$ "

$$xy := x \cdot y$$

È UN ABUSO DI  
NOTAZIONE PERCHÉ  
 $\rightarrow g$  NON È IL GRUPPO,  
MA INDICO CON  
 $g$  IL GRUPPO  $(g, \cdot)$

## UNITÀ DEL GRUPPO E DEL SOTTOGRUPPO

Sia  $h$  un sottogruppo di  $g$  ( $h \leq g$ )

↳ Di conseguenza,  $(h, \cdot)$  è un gruppo e ~~anche~~ anche  
lui l'unità

↳ Esiste  $1_h \in h$  e, in particolare, l'unità  
del sottogruppo è proprio l'unità del gruppo

DIM (1) → UN MODO PER VEDERLO

Premendo l'unità di  $g$  e la moltiplico con l'unità di  $h$

$$\hookrightarrow 1_g \cdot 1_h = 1_h \rightarrow \text{DATO CHE } 1_g \text{ È L'ELEMENTO NEUTRO DI } g$$

Visto che  $1_h$  è l'unità di  $h$ , posso scrivere che:

$$\hookrightarrow 1_h \cdot 1_h = 1_h$$

Quindi  $\underset{\substack{\downarrow \\ \text{SONO CANCELLABILI}}}{1_h \cdot 1_h} = 1_g \cdot \underset{\substack{\downarrow \\ \text{SONO CANCELLABILI}}}{1_h} \rightarrow 1_h = 1_g$

DIM (2) → UN ALTRO MODO PER VEDERLO

$$\text{Consideriamo } xy = 1_h$$

↳ Di conseguenza  $y$  è l'inverso di  $x$ , ma l'inverso  
di  $x$  è unico, di conseguenza vale che:

$$xy = 1_g$$

Quindi  $1_g = xy = 1_h$ , quindi  $1_g = 1_h$

## SOTTOSTRUTTURA GENERATA DALL'ELEMENTO NEUTRO

La sottostruttura generata dall'elemento neutro è l'elemento neutro stesso.

$$\langle u \rangle = \{u\} \quad \text{di } (S, *, u)$$

ESEMPIO:

$$\text{In } (N, +)$$

$$\langle 0 \rangle = \{0\} \quad \text{perché } 0+0+0+\dots+0=0$$

## SOTTOMONOIDE DA UN MONOIDE

ESEMPIO:

Consideriamo  $(N, \circ)$  un qualsiasi monoido.

Vogliamo trovare il sottomonoido generato da 0

↳  $\langle 0 \rangle$  deve comunque restare un monoido; quindi anche se  $0 \circ 0 \circ 0 \circ 0 \dots \circ 0 = 0$ , non posso scrivere che  $\langle 0 \rangle = \{0\} \rightarrow$  Devo aggiungere l'elemento neutro all'insieme  $\langle 0 \rangle$  affinché sia un monoido.

$$\langle 0 \rangle = \{0, 1\}$$

## STRUTTURE CICLICHE

$(S, *)$  è una struttura ciclica se:

$$(\exists x \in S)(S = \langle x \rangle) \xrightarrow{\text{SONO LE STRUTTURE}} \text{GENERATE DA POTENZE}$$

↳ Sono delle strutture particolari che sono generate da un solo elemento

ESEMPIO:

## ESEMPIO:

Consideriamo  $(\mathbb{Z}, +)$  come gruppo.

- Il sottogruppo generato da 1 è:

$\langle 1 \rangle = \mathbb{Z}$  perché è l'insieme di tutte le somme dei possibili combinazioni della 1 o  $1^{-1}$  (cioè -1)

ESEMPIO:  $2 = 1+1$   
 $5 = 1+1+1+1+1$   
 $-1 = 1^{-1}$   
 $-3 = 1^{-1} + 1^{-1} + 1^{-1}$

- $\langle 2, 3 \rangle = \mathbb{Z}$  notiamo che in  $\langle 2, 3 \rangle$  abbiamo  $5 = 3+2$ , abbiamo  $-2 = 2^{-1}$ , ma soprattutto abbiamo  $1 = 3+2^{-1} \rightarrow$  anche  $0 = 2+2+2+3^{-1}+3^{-2}$   
↳  $1 \in \langle 2, 3 \rangle$  e visto che  $\langle 2, 3 \rangle$  è una forte chiesa, allora contiene anche  $\langle 1 \rangle$   
Quindi  $\langle 1 \rangle \subseteq \langle 2, 3 \rangle$ , ma dato che  $\langle 1 \rangle = \mathbb{Z}$ , allora anche  $\langle 2, 3 \rangle = \mathbb{Z}$

c'è una combinazione dei due numeri che ci dà 1 perché sono due numeri coprimi (non hanno divisori comuni oltre l'1)  
↳ questo lo si dimostra con il teorema di Eulero  
↓

Se prendo un sottogruppo di  $\mathbb{Z}$  con due numeri coprimi allora genera tutta  $\mathbb{Z}$ .

- $\langle 2, 4 \rangle = 2\mathbb{Z}$  (sono ancora i numeri pari)

Quindi  $\mathbb{Z}$  è un gruppo ciclico, IN è un monide ciclico.

## CANCELLABILE A SINISTRA

Se  $\mathcal{g}$  è un semigruppo e  $x \in \mathcal{g}$ ,  $x$  si dice cancellabile a sinistra se:

$$(\forall y, z \in \mathcal{g})(\exists y : xz \rightarrow y = z) \rightarrow^{\text{def}} \text{scappicazione}$$

## CANCELLABILE A DESTRA

Se  $\mathcal{g}$  è un semigruppo e  $x \in \mathcal{g}$ ,  $x$  si dice cancellabile a destra se:

$$(\forall y, z \in \mathcal{g})(\exists z : yx = zx \rightarrow y = z)$$

## CANCELLABILE

Se  $\mathcal{g}$  è un semigruppo e  $x \in \mathcal{g}$ ,  $x$  si dice cancellabile se è cancellabile a destra e cancellabile a sinistra.

## NON CANCELLABILE A SINISTRA

$x$  non è cancellabile a sinistra se:

$$(\exists y, z \in \mathcal{g})(xy = xz \wedge y \neq z)$$

## NON CANCELLABILE A DESTRA

$x$  non è cancellabile a destra se:

$$(\exists y, z \in \mathcal{g})(yx = zx \wedge y \neq z)$$

## RELAZIONE TRA ELEMENTI INVERTIBILI E CANCELLABILI

Se  $x$  appartiene agli invertibili di  $g$ , allora è cancellabile.

↪ Se  $x \in U(g)$ , con  $g$  semigruppo, allora è cancellabile.

DIM

Dato che  $x$  è invertibile, allora, per definizione:

$$(\exists \bar{x} \in g)(\bar{x}\bar{x} = 1_g \wedge \bar{x}x = 1_g)$$

Siamo  $y, z \in g$ .  $\underline{xy = xz} \rightarrow$  voglio FAR VEDERE CHE  $x$  è CANCELLABILE, QUINDI CHE  $y = z$

Avrò che:  $y = 1_g \cdot y = \bar{x}\bar{x}y = \bar{x}\bar{x}z = 1_g \cdot z = z$

Con lo stesso procedimento si puo' dimostrare che vale la cancellabilità a destra.

↪ Quindi  $x$  è cancellabile  $\rightarrow$  Tutti gli invertibili sono cancellabili.

- Inoltre, se  $x$  è invertibile solo a destra, sarà cancellabile solo a destra; se  $x$  è invertibile solo a sinistra, sarà cancellabile solo a sinistra.

## TRASLAZIONE

Sia  $(S, \cdot)$  un semigruppo e  $x \in S$ . Definisco:

$$\sigma_x: z \in S \mapsto xz \in S \quad (\text{TRASLAZIONE SINISTRA})$$

↪ SIGMA

$$\delta_x: z \in S \mapsto zx \in S \quad (\text{TRASLAZIONE DESTRA})$$

↪ DELTA

↪ SE C'E' UN ELEMENTO  $z \in S$ , APPLICO  $x$  SULLA DESTRA

## RELAZIONE TRA TRASLAZIONE E CANCELLABILITÀ

Sappiamo che  $x$  si dice cancellabile (ad esempio a sinistra) se:  $(\forall y, z \in g)(xy = xz \rightarrow y = z)$

Ma  $xy$  è proprio uguale a  $\alpha_x(y)$  e  $xz$  è proprio uguale a  $\alpha_x(z)$   $\rightarrow \alpha_x(y) = \alpha_x(z) \rightarrow y = z$

$\hookrightarrow$  Quindi,  $(\forall y, z \in g)(\alpha_x(y) = \alpha_x(z) \rightarrow y = z)$

Ma queste è proprio la definizione di funzione iniettiva. Ne segue che:

- $x$  è cancellabile a sinistra se e solo se  $\alpha_x$  è iniettiva.
- $x$  è cancellabile a destra se e solo se  $\delta_x$  è iniettiva.

## INVERSA DI $\alpha_x$ È $\delta_x$

Se  $x \in U(s)$ , posso trovare l'inversa di  $\alpha_x$

$\hookrightarrow$  L'inversa di  $\alpha_x$  è  $\alpha_{x^{-1}} \rightarrow$  L'INVERSA DI  $\alpha_x$  È  $\alpha_{x^{-1}}$  DELL'INVERSA DI  $x$

$$\boxed{\alpha_{x^{-1}} = \alpha_x^{-1} \quad \text{e} \quad \delta_{x^{-1}} = \delta_x^{-1}}$$

### DIM

Dato che  $x$  è invertibile, se faccio la composizione di  $\alpha_{x^{-1}}$  e  $\alpha_x$ , ottengo l'identità

$$\hookrightarrow (\alpha_{x^{-1}} \circ \alpha_x)(z) = \alpha_{x^{-1}}(\alpha_x(z)) = \alpha_{x^{-1}}(x \cdot z) = x^{-1} \cdot (x \cdot z) = z$$

$\hookrightarrow \alpha_{x^{-1}}$  È L'INVERSA SINISTRA  $\rightarrow$  PER LO STESSO PROCEDIMENTO,  $\alpha_x^{-1}$  È ANCHE L'INVERSA DESTRA

- Dato che  $\alpha_x$  e  $\delta_x$  sono invertibili, allora sono biette

# RELAZIONE TRA ELEMENTI CANCELLABILI E INVERTIBILI

2 PAGINE PRIMA

Allora dimostrato che se  $x$  è invertibile, allora è cancellabile

↳ Il contrario non vale, infatti essere cancellabile non implica essere invertibile

CONTROESEMPIO:

Consideriamo  $(\mathbb{Z}, \cdot)$

Se  $m \neq 0$ , abbiamo che:

$$(\forall x, y \in \mathbb{Z})(mx = my \rightarrow x = y) \rightarrow \begin{array}{l} \text{DEFINIZIONE DI} \\ \text{CANCELLABILE A} \\ \text{SINISTRA} \end{array}$$

ma  $m$ , quasi sempre, non è invertibile

↳ ESEMPIO:

$$\cdot 2x = \cdot 2y \rightarrow 2 \text{ è cancellabile ma} \\ \text{non è invertibile in } \mathbb{Z}$$

# TAVOLE DI CAYLEY

Le permettono di visualizzare cosa succede nelle strutture algebriche con un'operazione.



Premolo  $(S, *)$  con  $S \neq \emptyset$

AD ESEMPIO:

$$\bullet S = \{a, b\}$$

• La tavola di Cayley ci permette di definire l'operazione  $*$

|   |   | $*$ |   |
|---|---|-----|---|
|   |   | a   | b |
| a | a | a   | b |
|   | b | b   | a |

DA QUI CAPIAMO:

- $a * a = a$
- $a * b = b$
- $b * a = b$
- $b * b = a$

•  $A * (a, a)$  associa a,  
 $A * (a, b)$  associa b  
ecc...

+ Dalla tavola di Cayley possiamo ricavare delle informazioni sulla struttura algebrica  $(S, *)$

↳ Notiamo che  $a * a = a$  e  $a * b = b$ , quindi a è neutro a sinistra



Un elemento è neutro a sinistra se la riga corrispondente si conserva, resti uguale

Un elemento è neutro a destra se la colonna corrispondente resti uguale a quelle degli elementi

↳ a è l'unità di  $(S, *)$

↳ Inoltre, dato che  $a * a = a$ , a è l'antone di se stesso

|   |   | $*$ |   |
|---|---|-----|---|
|   |   | a   | b |
| a | a | a   | b |
|   | b | b   | a |

Notiamo inoltre che  $b * b = a$ , cioè  $b * b$  dà l'elemento neutro

↳ b è invertibile → PER LA DEFINIZIONE DI INVERTIBILITÀ

+ Di conseguenza,  $(S, *)$  è un gruppo abeliano

• È COMMUTATIVO  
PERCHÉ

$$a * b = b * a$$

• HA L'UNITÀ

• TUTTI GLI ELEMENTI SONO INVERTIBILI

+ Consideriamo  $(S, *)$  e  $S = \{a, b, c\}$

- $a$  è l'elemento neutro
- Alimché  $b$  sia invertibile  
a sinistra, allora:  
 $(\exists x \in S)(x \cdot b = 1)$

↳ Una delle colonne, per  
 $b$ , deve dare  $a$  ↳  $c * b = a$   
↓

|   |   |   |   |
|---|---|---|---|
| * | a | b | c |
| a | a | b | c |
| b | b | c | a |
| c | c | a | b |

NON ci POSSONO  
ESSERE SPAZI  
VUOTI PERCHE'  
ALTRIMENTI \*NON SAREBRE  
UN'OPERAZIONE  
↓  
L'OPERAZIONE E'  
DEFINITA SU TUTTE  
LE COPPIE DEL  
DOMINIO  $S \times S$

$X$  è invertibile a sinistra se nella colonna  
di  $x$  c'è l'elemento neutro

$X$  è invertibile a destra se nella riga di  
 $x$  c'è l'elemento neutro

- \* è commutativa se, cambiando righe e colonne,  
la tavola resta uguale ↳ SE HO CHE  $b * c = a$ , VOGLIO  
ANCHE CHE  $c * b = a$   
↓ MASSICE  
TABELLA

\* è commutativa se la tavola è simmetrica  
rispetto alla diagonale principale

- $X$  è cancellabile a sinistra quando  $0_X$  è invertibile  
↳  $0_X$  è la riga che sta su  $x$  →, considerando }  $0_X(a) = b$  }  $0_X(b) = c$   
}  $x = b$  }
- ↳ Dato che è invertibile, tutti gli elementi della riga sono diversi

↓

$X$  è cancellabile a sinistra se sulla riga di  $X$   
tutti gli elementi appaiono una sola volta

$X$  è cancellabile a destra se sulla colonna di  
 $X$  tutti gli elementi appaiono una sola volta

Correzione esercizi 03/11/2021 (LEZIONE 17)

1.  $(S, *)$

$C = \text{Cancelabili a sinistra}$

Premo  $x, y \in C$ . Voglio far vedere che anche la loro  
composizione appartiene a  $C$ . cioè che  $x * y \in C$ , cioè:

$$\hookrightarrow (\forall w, z \in S)((x * y) * z = (x * y) * w \rightarrow z = w)$$

DEFINIZIONE  
DI CANCELA  
BILATERAL  
MENTE

Dobbiamo vedere che  $C$  è forte chiusa di ogni  
gruppo obbliamo

$\hookrightarrow$  Prendi  $w, z \in S$ , so che per l'assoluto  
 $x * (y * z) = x * (y * w)$ . Visto che  $x$  è cancellabile,  
posso scrivere che  $y * z = y * w$ .

Visto che anche  $y \in C$ , allora  $z = w$ , quindi  
 $C$  è una forte chiusa.

10.  $S = \{x, y, u\}$

$* \in u \times y$

|     |     |     |     |
|-----|-----|-----|-----|
| $u$ | $u$ | $x$ | $y$ |
| $u$ | $u$ | $x$ | $y$ |
| $x$ | $x$ | $y$ | $u$ |
| $y$ | $y$ | $u$ | $x$ |

La tabella nostra che  
 $(S, *)$  è anche associativa  
perché ad esempio avendo  
l'elemento neutro,  $(u * x) * y$  è  
uguale a  $(x * y) * u$

$u$  è l'elemento neutro → riga e colonna di  
u sono invariate

•  $(S, *)$  è commutativa → perché simmetrica  
rispetto alla diagonale

• Tutti gli elementi sono cancellabili → fanno una sola volta in  
tutta riga e colonna

•  $(S, *)$  è un gruppo obbliamo → lo notiamo perché  
 $x * y = u$  è anche  
 $y * x = u$ , quindi  $y$  è  
l'inverso di  $x$  è viceversa

9.  $S = \{x, y, u\} \rightarrow$  la struttura  $(S, *)$  non è un monoidale, ma ha l'elemento neutro

$$* \begin{matrix} u & x & y \\ u & u & x & y \\ x & x & u & x \end{matrix}$$

$$\begin{matrix} u & u & x & y \\ y & y & y & u \end{matrix}$$

$$\begin{matrix} x & x & u & x \\ y & y & y & u \end{matrix}$$

x si ripete nella riga di x e y si ripete nella riga di y

•  $u$  è l'elemento neutro

• Perché  $y \neq u$ , ma  $x * y = x = x * u$ ,

•  $x$  non è cancellabile a sinistra

↳ Anche  $y$  non lo è dato che  $y * u = y * x$

PERCHE' NON E' UN MONOIDALE!

• Notiamo che:

$$y = u * x = (x * x) * y$$

$$\hookrightarrow x * x = u$$

a destra

niente si ripete nella colonna

• Tutti gli elementi sono cancellabili

Assumiamo per scontro che sia associativa. Quindi:

$$(x * x) * y = x * (x * y) = x * x = u \quad \hookrightarrow (x * x) * y \neq x * (x * y)$$

→ Quindi  $(S, *)$  non è un monoidale perché non è associativo

## POTENZE DI UN ELEMENTO $\rightarrow$ SI POSSONO DIMOSTRARE PER INDUZIONE

Sia  $(S, *)$  un semigruppo

$$\bullet (\forall x \in S)(\forall m, m \in \mathbb{Z})(x^m \in S \wedge x^m \in S \rightarrow x^m \cdot x^m = x^{m+m})$$

$$\bullet (\forall x \in S)(\forall m, m \in \mathbb{Z})(x^m \in S \wedge x^m \in S \rightarrow (x^m)^m = x^{m \cdot m})$$

↳ Dato che  $(S, *)$  è un semigruppo,  $x$  non è detto che abbia gli inversi  $\rightarrow$  Devo specificare che:

$x^m \in S$  e che  $x^m \in S \rightarrow$  ad esempio, se uscire  $m = -1$ ,  $x^{-1} \in S$

↳ Se  $S$  è un gruppo, questa parte non serve anche toglierla perché gli inversi ci sono sicuramente

# DEFINIZIONI DELLE POTENZE

- $x^m := x * x * \dots * x$  per  $m$  volte  $\rightarrow \forall m \in \mathbb{N} \setminus \{0\}$

- $x^0 := 1_S$  se c'è l'elemento neutro  $\rightarrow m=0$

- $x^{-m} := (x^m)^{-1}$  se abbiamo le inverse  $\rightarrow \forall m \in \mathbb{N} \setminus \{0\}$   
 $\hookrightarrow$  cioè  $(S, *)$  è un gruppo.

GENERALI PER OGNI STRUTTURA

Se in matrici additive, le potenze si dicono multipli.

Vale anche la proprietà commutativa delle potenze perché:

$$x^m \cdot x^n = x^{m+n} = x^{n+m} = x^n \cdot x^m \quad \begin{array}{l} \text{E POTENZE} \\ \text{COMMUTAZIONE TRA DI LORO PERCHE' COMMUTA LA SOMMA DEGLI ESPONENTI} \end{array}$$

Ogni semigruppo ciclico è commutativo.  
 Seiop ehe  $(\exists x \in S)(S = \langle x \rangle)$

Il semigruppo generato dal generato da  $x * x * x * \dots * x$  per  $m$  volte, che non è altro che  $x^*$  che è commutativo

AD ESEMPIO:

Il gruppo  $(S, *)$  con  $S = \{x, y, u\}$  e  $* \in \{u|x, y\}$

è un gruppo ciclico di ordine 3

↓

$x * x = y$  e  $x * y = u$ , quindi tutti gli elementi del gruppo sono potenze di  $x$

$$\hookrightarrow x = x^1$$

$$\cdot y = x * x = x^2$$

$$\cdot u = x * y = x * x * x = x^3$$

• Si dice  $m \in \mathbb{Z}$  im  $(\mathbb{Z}, +)$

I MULTIPLI  
DI  $m$  IN  $\mathbb{Z}$

$$m \cdot \mathbb{Z} = \{ m \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(m = k \cdot m) \} \subseteq \mathbb{Z}$$

↳ E' l'unita quando  $k=0$ ,  $m \cdot 0 = 0$

↳  $m \cdot \mathbb{Z}$  e' UN SOTTOGRUPPO DI  $\mathbb{Z}$

• E' una parte chiusa poiché:  $k_1 \cdot m + k_2 \cdot m = (k_1 + k_2) \cdot m \in m \cdot \mathbb{Z}$

• Ha gli inversi poiché: Preso  $k \cdot m$ , anche  $-k \cdot m \in m \cdot \mathbb{Z}$

↳ E' SEMPRE UN MULTIPLO DI  $\mathbb{Z}$

Alcuni esempi di sottogruppi di  $\mathbb{Z}$  sono:

$$\cdot \{0\} = 0 \cdot \mathbb{Z} \rightarrow \text{TUTTI I MUL. DI ZERO}$$

$$\cdot \mathbb{Z} = 1 \cdot \mathbb{Z} \rightarrow \text{TUTTI I MUL. DI 1}$$

$$\cdot 2 \cdot \mathbb{Z} \rightarrow \text{I NUMERI PARI}$$

• Si puo' dimostrare che i sottogruppi di  $(\mathbb{Z}, +)$  sono tutti e solo i multipli di  $\mathbb{Z}$

## OMOMORFISMI TRA STRUTTURE ALGEBRICHE

↳ E' una operazione binaria.

OMOMORFISMO  $\rightarrow$  Stesse forme, o simili.

In matematica abbiamo tante cose diverse che sono praticamente le stesse cose (o simili).  $\rightarrow$  Tanti tipi di strutture algebriche che sono, bene o male, le stesse cose.

ESEMPIO:

• Consideriamo il gruppo fatto dalla parola vuota e il gruppo formato dallo 0.

↳ Questi due gruppi sono bene o male gli stessi poiché hanno un solo elemento e la stessa operazione.

↳ E' un isomorfismo tra i due

gruppi  
perché  
sono  
simili,  
ma non  
e' univoco  
e' comune

# DEFINIZIONE DI OMOMORFISMO

Premendo  $(S, *)$  e  $(\bar{S}, \bar{*})$  l'OPERAZIONE  $*$  è  
SOMMARE A  $*$

- Una funzione  $\varphi: S \rightarrow \bar{S}$  si dice omomorfismo se

$$(\forall x, y \in S) (\varphi(x * y) = \varphi(x) \bar{*} \varphi(y))$$

Tra  $x \in S$   
Può starci  
Solo  $*$

POSSANO PASSARE  
DA UNA STRUTTURA  
ALL'ALTRA TRAMITE  
QUESTA FUNZIONE  
CHE RISPETTA  
L'OPERAZIONE  $*$

## ESEMPIO:

- EXP:  $x \in \mathbb{R} \mapsto e^x \in \mathbb{R}$

C'è un omomorfismo fra la somma e il prodotto perché  $e^{x+y} = e^x \cdot e^y$

$(\mathbb{R}, +)$  e  $(\mathbb{R} \setminus \{0\}, \cdot)$  sono le strutture dell'omomorfismo

→ E' UN OMOMORFISMO PERCHE  
STA PORTANDO LA SOMMA  
IN UN PRODOTTO, TRA LE  
IMMAGINI  $e^x$  E  $e^y$

## MONOMORFISMO

- Omomorfismo iniettivo si dice monomorfismo

## EPIMORFISMO

- Omomorfismo suriettivo si dice epimorfismo

## ISOMORFISMO

- Omomorfismo biiettivo si dice isomorfismo

## ESEMPIO:

d'applicazione identità è un isomorfismo  
perché conserva le strutture e le sue caratteristiche

• Anche la funzione logaritmica è un isomorfismo perché  
è l'inverso delle funzioni esponenziali

# 2) L'INVERSA DI UN ISOMORFISMO È UN ISOMORFISMO?

Consideriamo  $(S, *)$  e  $(\bar{S}, \bar{*})$  e l'isomorfismo  $\varphi$  tra le due strutture.

Essendo  $\varphi$  biiettiva, esiste  $\varphi^{-1}$  e poi anche essa un omomorfismo.

DIM Prendo  $x, y \in \bar{S}$  e considero:

$$\varphi(\varphi^{-1}(x) * \varphi^{-1}(y)) = \varphi(\varphi^{-1}(x)) \bar{*} \varphi(\varphi^{-1}(y)) = x \bar{*} y$$

da cui PROPRIETÀ  
DELL'ISOMORFISMO

Applico  $\varphi^{-1}$  l'omologo i lati e otto:

$$\varphi^{-1}(x) * \varphi^{-1}(y) = \varphi^{-1}(x \bar{*} y)$$

Quindi anche  $\varphi^{-1}$  è un isomorfismo.

## PROPRIETÀ CONSERVATE DEGLI EPIMORFISMI

Gli epimorfismi "conservano":

- La commutatività

- L'associatività

- Gli elementi neutri

- Gli inversi

QUELLI A DESTRA LI MANDA  
A DESTRA, QUELLI A SINISTRA  
LI MANDA A SINISTRA

ASSORBE L'ELEMENTO  
NEUTRO DI UN GRUPPO  
ALL'ELEMENTO NEUTRO L'ELIMINA

DIM (CONSERVAZIONE DEGLI ELEMENTI NEUTRI)

- Consideriamo  $\varphi: S \xrightarrow{\text{EPI}} \bar{S}$  e  $1_S \in S$

- Sia  $y \in \bar{S}$ ,  $y = y \bar{*} \varphi(1_S) = \varphi(x) \bar{*} \varphi(1_S)$  perciò,

dato che  $\varphi$  è suriettiva,  $(\exists x \in S)(\varphi(x) = y)$  → DEFINIZIONE DI SURIETTIVITÀ

- Ma  $\varphi$  è un omomorfismo, quindi avrò che:

$$(\varphi(x)) \bar{*} \varphi(1_S) = \varphi(x \bar{*} 1_S) = \varphi(x) = y \rightarrow$$

di conservazione perché  
l'elemento neutro  $\varphi(1_S)$  è l'unica di 5

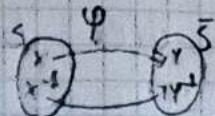
$\varphi$  conservava

l'elemento neutro

## DIM (CONSERVAZIONE DEGLI ELEMENTI INVERSI)

Per dimostrare che l'elemento inverso di  $x$  viene mappato all'elemento inverso dell'elemento associato a  $x$  nell'altro gruppo dobbiamo dimostrare che:

$$(\forall x \in S)(\varphi(x^{-1}) = (\varphi(x))^{-1})$$



Per far vedere che una cosa è l'inversa di un'altra, allora li moltiplico e dimostra di essere l'identità.

In  $\bar{S}$  abbiamo che, visto che  $\varphi$  è un omomorfismo,  $\varphi(x^{-1}) * \varphi(x) = \varphi(x^{-1} * x) = \varphi(1_S) = 1_{\bar{S}}$  SAPPIANO CHE L'IDENTITÀ SI TRASPORTA

Inoltre,  $(\varphi(x))^{-1} * \varphi(x) = 1_{\bar{S}}$ , quindi  $\varphi(x^{-1}) = (\varphi(x))^{-1}$  e sono le stesse inverse sinistra di  $\varphi(x)$ .

Ripetendo lo stesso procedimento considerando  $\varphi(x^{-1})$  e  $(\varphi(x))^{-1}$  le inverse destra otterremmo lo stesso risultato, quindi  $\varphi(x^{-1}) = (\varphi(x))^{-1}$  e sono le stesse inverse.

## DIM (CONSERVAZIONE DELLA COMMUTATIVITÀ)

Prendo  $x, y \in \bar{S}$  e considero  $(\bar{S}, *)$  commutativo.

Dato che  $\varphi$  è suriettiva,  $\exists w, z \in S$  |  $\varphi(w) = x \wedge \varphi(z) = y$

Prendo in  $\bar{S}$ ,  $x * y$

$$\hookrightarrow x * y = \varphi(w) * \varphi(z)$$

Dato che  $\varphi$  è un omomorfismo

$$\hookrightarrow \varphi(w) * \varphi(z) = \varphi(w * z)$$

LA COMMUTATIVITÀ SI CONSERVA

Ma  $(\bar{S}, *)$  è commutativo, quindi:

$$\hookrightarrow \varphi(w * z) = \varphi(z * w) = \varphi(z) * \varphi(w) = y * x$$

# PERCHE' GLI AUTOMORFISMI SONO IMPORTANTI?

→ Il fatto che ci siano degli automorfismi ci dice delle cose molto importanti su  $S$

↳ A volte puo' succedere che  $\bar{S}$  sia un insieme molto intricato e difficile da capire.

↳ Possiamo così trovare un insieme  $S$  più semplice da descrivere e, visto che c'è l'automorfismo, ci aiuta a descrivere più facilmente  $\bar{S}$  grazie alle proprietà conservate.

## ESEMPI:

• Consideriamo  $S \neq \emptyset$  e definiamo la funzione  $f$ :

$$f: x \in P(S) \mapsto S \setminus x \in P(S)$$

Sappiamo che la funzione  $f$  è biettiva.

LEGGI DI  
DE MORGAN

Sappiamo che  $\forall x, y \in P(S), S \setminus (x \cup y) = (S \setminus x) \cap (S \setminus y)$

Questo mostra ci indica che  $f$  è un isomorfismo tra  $(P(S), \cup)$  e  $(P(S), \cap)$ .

SE MI DEDICO PER E' L'ELEMENTO NEUTRO DI  $\cup = \emptyset$   
NEUTRO DI UNO, BASTA CHE MI E' L'ELEMENTO NEUTRO DI  $\cap = f(\emptyset) =$   
RICORDO QUELLO DELL'ALTO C'È NC → STESSA COSA PER  $= S \setminus \emptyset = S$   
FACCIO L'IMMAGINE TRAMITE  $f$  INVERSI CEC...

→ Anche se  $\cup$  e  $\cap$  sono due operazioni diverse, il fatto che esista un isomorfismo, ci dice che in realtà  $(P(S), \cup)$  e  $(P(S), \cap)$  sono le stesse strutture, quindi qualunque cosa dimostri per una vale anche per l'altra.

↳ Risparmio del lavoro

↓ SONO DUE STRUTTURE  
DIVERSE MA POSSO  
PASSARE DALL'UNA  
ALL'ALTRA

## ANELLI

Gli anelli sono delle strutture algebriche e due operazioni.

### DEFINIZIONE DI ANELLO

Sia  $a$  un insieme non vuoto ( $a \neq \emptyset$ ) e siano  $+, \cdot$  due operazioni binarie interne di  $a$ .

Se le treuple  $(a, +, \cdot)$  si dice anello se:

- $(a, +)$  è un gruppo abeliano
- $(a, \cdot)$  è un semigruppo
- Vale la distributività di  $\cdot$  rispetto a  $+$   
 $\hookrightarrow (\forall x, y, z \in a)(x \cdot (y + z) = xy + xz)$

### ESEMPIO:

- $(\mathbb{Z}, +, \cdot)$  è un anello

## ANELLO COMMUTATIVO

- $(a, +, \cdot)$  è un anello commutativo se - anche  $(a, \cdot)$  è commutativo  $\rightarrow (a, +)$  lo è già per definizione.

## ANELLO UNITARIO

- $(a, +, \cdot)$  si dice anello unitario se  $(a, \cdot)$  è un monoido  $\rightarrow$  DEVE ESSERE L'UNITÀ MOLTIPLICATIVA

## CONVENTIONI

- " $0_a$ " o " $0$ " è l'elemento neutro di  $(a, +)$
- " $1_a$ " o " $1$ " è l'elemento neutro di  $(a, \cdot)$  (se c'è)

## SOTTO ANELLO

SONO GRANDE I MONTE

Se  $(S, +, \cdot)$  è un anello e  $S \subseteq a$  chiuso,

$\hookrightarrow S$  è una parte chiusa di  $a$

$\hookrightarrow S$  è detto sottanello di  $a$

### ESEMPIO:

- $\forall x, y, z \in P(S)$  con  $S \neq \emptyset$ , vale  $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$

DISTRIBUTIVITÀ  
DI  $\cap$  RISPETTO A  $\cup$

Quindi  $(P(S), \cup, \cap)$  è un anello commutativo unitario

$\downarrow$

• È commutativo perché l'intersezione è commutativa

• È unitario perché c'è l'unità rispetto l'intersezione

## DEFINIZIONI E PROPRIETÀ

- Definisco  $x - y := x + (-y)$  dove  $-y$  è l'opposto di  $y$  in  $(a, +)$   $\hookrightarrow$  E' ABELIANO PER DEFINIZIONE

$$\bullet (\forall m \in \mathbb{N} \setminus \{0\})(mx = \underbrace{x + x + \dots + x}_m \text{ volte}) \rightarrow \forall x \in a$$

$$\bullet (\forall m \in \mathbb{Z} \setminus \mathbb{N})(mx = \underbrace{-x - x - \dots - x}_m \text{ volte}) \rightarrow \forall x \in a$$

- $0 \cdot X = O_a$   $\rightarrow$  Sono due zeri diversi

$\hookrightarrow$  LO ZERO IN  $\mathbb{Z}$   
LO ZERO IN  $a$

$$\text{DIM } 0 \cdot X = (1 - 1)X = 1X + ((-1)X) = X - X = O_a$$

$\hookrightarrow$  E' LO ZERO DI  $a$  PERCHÉ  
E' LA SOMMA DI UN ELEMENTO PIÙ L'OPPOSTO

- $(\forall X \in a)(X \cdot O_a = O_a) \rightarrow$  NON E' UNA COSA OMIA

$\downarrow$

$$\text{DIM } X \cdot O_a = X(X - X) = X \cdot X - X \cdot X = O_a$$

$\hookrightarrow$  DISTRIBUTIVITÀ

- $(\forall m \in \mathbb{N} \setminus \{0\})(x^m = \underbrace{x \cdot x \cdot \dots \cdot x}_{m \text{ volte}}) \rightarrow \forall x \in \mathcal{Q}$

- $(\forall m \in \mathbb{Z} \setminus \mathbb{N})(x^m = \underbrace{x^{-1} \cdot x^{-1} \cdot \dots \cdot x^{-1}}_{m \text{ volte}}) \rightarrow \forall x \in \mathcal{Q}$

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

$\downarrow$   
DIM

Per dimostrare che  $x(-y) = -xy = (-x)y$ , dimostro che queste sono le inverse dello stesso elemento e dato che l'inverso di un elemento è unico, allora queste sono la stessa cosa.

$$1) x(-y) + xy = x(-y + y) = x(0) = 0 \cdot x = 0 \xrightarrow[\text{DISTRIBUZIONE AL CONTRARIO}]{} \text{ELEMENTO NEUTRO DI } (0, +)$$

$$2) -xy + xy = 0$$

$$3) (-x)y + xy = y(-x + x) = y(0) = 0 \cdot y = 0$$

Quindi  $x(-y) = -xy = (-x)y$

- è distributiva rispetto a  $\cdot$

- Se  $(\mathcal{Q}, +, \cdot)$  è unitario, vale che:

$$(\forall x \in \mathcal{Q})(\forall m \in \mathbb{Z})((m \cdot 1_{\mathcal{Q}}) \cdot x = m \cdot x)$$

Correzione esercizi 05/11/2021 (LEZIONE 18)

1.  $f: \alpha \rightarrow \alpha$   $S = \{f^4, f, f^2, f^3\}$

$f(x) = x$   $\leftarrow f \in \text{Sym}(\alpha)$   
 $\epsilon \text{ BIETTIVA}$

$f(x) = y$

$f(y) = z$

$f(z) = w$

PER VEDERE  
CHE S E'  
UNA PARTE  
CHIUSA

• Dimostrare che  $(S, \circ)$  è un gruppo abeliano

↳ Prendo uno qualunque degli  $f$  di  $S$  e voglio far vedere  
che composti danno ancora uno di quegli  $f$  in  $S$ .

↓  
Chi è  $f^4$ ?  $f^4(x) = f \circ f \circ f \circ f(x) = f \circ f \circ f(x) = f \circ f(y) = f(z) = w$

↳ Se lo moltipico con tutti gli elementi, metterò che  
 $f^4$  non è altro che  $\text{Id}_\alpha \rightarrow f^4 = \text{Id}_\alpha$

↓

$S = \{\text{Id}_\alpha, f, f^2, f^3\}$

Se prendo un ente  $i \in \mathbb{Z}$  tali che:  $1 \leq i, j \leq 3$ ,

$$f^i \circ f^j = f^{i+j}$$
 per le proprietà delle potenze.

↳ Nota che se faccio qualsiasi potenza, il risultato  
sarà sempre in  $S \rightarrow f^3 = f^6 = f^{4+2} = f^2$  perché  $f^4$  è l'identità

↳  $f$  è una funzione periodica

↓  
S è una parte chiusa.

$(S, \circ)$  ha le inverse?

Sì perché  $f \circ f^3 = f^4 = \text{Id}_\alpha$ ,  $f^3 \circ f^4 = \text{Id}_\alpha$ ,  $f^2 \circ f^2 = f^4 = \text{Id}_\alpha$  ecc..

↳  $(S, \circ)$  è un gruppo.

Inoltre,  $(S, \circ)$  è abeliano perché le potenze commutano  
tra di loro  $\rightarrow$  bba la proprietà commutativa

Facciamo la tavola di Cayley:

|       |       |       |       |       |
|-------|-------|-------|-------|-------|
| $0$   | $1_s$ | $g$   | $g^2$ | $g^3$ |
| $1_s$ | $1_s$ | $g$   | $g^2$ | $g^3$ |
| $g$   | $g$   | $g^2$ | $g^3$ | $1_s$ |
| $g^2$ | $g^2$ | $g^3$ | $1_s$ | $g$   |
| $g^3$ | $g^3$ | $1_s$ | $g$   | $g^2$ |

Comportiamoci

con la tavola  $\rightarrow$

di Cayley

dell'esercizio

1a lezione +

\*  $u \times v \times z$

$u \times u \times v \times z$

$x \times v \times z \times u$

$v \times v \times z \times u \times x$

$z \times z \times u \times v$

Notiamo che hanno la stessa tavola solo con nomi (distanza)

$\hookrightarrow$  Sono omomorfismi  $\rightarrow$  conservano le operazioni

$\hookrightarrow$  chi è  $\varphi$ ?

$$\varphi: 1_s \rightarrow u$$

$$g \rightarrow x$$

$$g^2 \rightarrow y$$

$$g^3 \rightarrow z$$

Inoltre,  $(S, \circ)$  è un gruppo ciclico perché  $S$  è generato da  $g$ .

$\hookrightarrow S = \langle g \rangle$ , cioè  $g^2, g^3 \in g$  TORNA  
INDIETRO

3. Dato  $i: G \hookrightarrow S$ , l'immersione, da  $G$  ad  $S$  è:

$$i: x \in G \mapsto x \in S$$

$\hookrightarrow$  Questo è un monomorfismo (omomorfismo iniettivo)

Esempio l'operazione in  $S$  la stessa  
di quella di  $G$ ,

$$\hookrightarrow i(x * y) = x * y = i(x) * i(y) \rightarrow \text{E CHIARAMENTE UN OMOMORFISMO}$$

E' iniettivo perché  $i$  è una funzione suriettiva

NON E' DETTO CHE E'  
UN ISOMORFISMO  
PERCHE' POTREBBERE NON  
ESSERE SURIESSIVA

6.  $f: x \in \mathbb{P}(\omega) \mapsto c \cap x \in \mathbb{P}(\omega)$  è un automorfismo di  $(\mathbb{P}(\omega), \cup)$ ? È di  $(\mathcal{P}(\omega), \cap)$ ?

↳ In realtà  $f$  è la funzione identità perché  $c \cap x = x$

$\downarrow$

$f: x \in \mathbb{P}(\omega) \mapsto x \in \mathbb{P}(\omega) \rightarrow f$  è un isomorfismo

7-5.  $\alpha: (x, y) \in \mathbb{Z} \times \mathbb{Z} \mapsto x+y+1 \in \mathbb{Z}$        $f: m \in \mathbb{Z} \mapsto m+1 \in \mathbb{Z}$

$\gamma: (x, y) \in \mathbb{Q} \times \mathbb{Q} \mapsto \frac{x+y}{z} \in \mathbb{Q}$        $f: a \in \mathbb{Q} \mapsto 2a \in \mathbb{Q}$

4. Voglio far vedere come  $f$  si comporta rispetto a  $(\mathbb{Z}, +)$  e  $(\mathbb{Z}, \alpha)$ . Sono isomorfi?

↳ Prendo due elementi  $m, n \in \mathbb{Z}$

$$f(m+n) = m+n+1 = f(m) + f(n)$$

Se le due strutture sono state omomorfi con  $f$  omomorfismo, ci saremmo dovuti trovare che:

$$f(m+n) - (m+n+1) = f(m) - f(n) \rightarrow \text{DEFINIZIONE DI OMOMORFISMO}$$

↓  
CONTROESEMPIO:

$$\left. \begin{array}{l} f(1+1) = f(2) = 3 = 1 + 1 \\ f(1) \alpha f(1) = 2 \alpha 2 = 5 \end{array} \right\} \text{Non omomorfismi}$$

5. Anche la funzione  $f$  non è un omomorfismo. Infatti,  $x, y \in \mathbb{Q}$ :

$$f(x+y) = 2(x+y) = 2x+2y$$

$$f(x) \gamma f(y) = \underline{\underline{f(x) + f(y)}} = \underline{\underline{2x+2y}} - x+y \left\} \text{Non omomorfismi} \right.$$

↳ E' possibile fare un controsenso più avanti con  $x=1$  e  $y=1$

## AUTOMORFISMO

Se  $f: \alpha \rightarrow \alpha$  è un isomorfismo,

$f$  si dice automorfismo  $\rightarrow$  UN ISOMORFISMO  $\alpha$  IN  $\alpha$  STESSO

## OMONORFISMO DI ANELLI

Se ho due anelli  $(S, +, \cdot)$  e  $(\bar{S}, \bar{+}, \bar{\cdot})$ ,

$f: S \rightarrow \bar{S}$  si dice omonorfismo di anelli se:

$$(\forall x, y \in S) ((f(x+y) = f(x) \bar{+} f(y)) \wedge (f(x \cdot y) = f(x) \bar{\cdot} f(y)))$$

↳

Inoltre, se  $S$  ha l'elemento neutro,  $f(1_S) = 1_{\bar{S}}$

L'ELEMENTO  
NEUTRO LO  
MANOA  
NELL'ALTRIO  
L'ELEMENTO  
NEUTRO

## ESEMPIO:

Sappiamo che tra  $(P(S), \cup)$  e  $(P(S), \cap)$  ci è un isomorfismo  $\varphi: (P(S), \cup) \xrightarrow{\cong} (P(S), \cap)$

$$\varphi: x \in P(S) \mapsto S \setminus x \in P(S)$$

Perché vale che  $\forall x, y \in P(S)$ ,  $S \setminus (x \cap y) = S \setminus x \cup S \setminus y$

• In particolare,  $\varphi$  è un isomorfismo anche tra gli anelli  $(P(S), \cup, \cap)$  e  $(P(S), \cap, \cup)$

↳  $\varphi$  manda  $\cup$  in  $\cap$  e viceversa.  $\rightarrow S \setminus (x \cap y) = S \setminus x \cup S \setminus y$

↳  $\varphi$  manda l'elemento neutro nell'elemento neutro

↳ Si parla dell'elemento neutro riguardo alla seconda operazione dato che la prima è sempre l'unione.

I due anelli  $(P(S), \cup, \cap)$  e  $(P(S), \cap, \cup)$  sono unitari dato

che  $1_{P(S)} = S$  mentre  $1_{P(S)} = \emptyset \rightarrow$  se è unione

IL PRIMO  
ANELLO

UNIONE

IL SECONDO  
ANELLO

Infatti,  $\varphi(S) = S \setminus S = \emptyset$

↳ Quindi  $\varphi$  è un isomorfismo di anelli

## LEGGE DI ANNULLAMENTO DEL PRODOTTO

Se ho l'anello  $(\mathcal{S}, +, \cdot)$ , se  $\mathcal{S}$  non ha la legge di annullamento del prodotto (lo indico con "LAP") ne:

$$(\forall x, y \in \mathcal{S})(xy = 0_{\mathcal{S}} \rightarrow x = 0_{\mathcal{S}} \vee y = 0_{\mathcal{S}})$$

NON PUÒ ESSERE CHE  
IL PRODOTTO DI DUE ELEMENTI  
NON NULLI FACCIA 0

Ci sono alcuni esempi dove non vale la LAP.

### ESEMPIO:

• Consideriamo  $(P(S), \cup, \cap)$ . Voglio dimostrare che qui non vale la legge di annullamento del prodotto, cioè:

$$(\exists x, y \in P(S))(x \cap y = \emptyset \wedge (x \neq \emptyset \wedge y \neq \emptyset)) \rightarrow \text{LAP}$$

↓ Se  $S = \{a, b\}$ , in  $P(S)$  c'è  $\{a\}$  e  $\{b\}$ .  
RISTRAZIONE  
ALMENO DUE ELEMENTI → Sono sottoinsiemi

↳ L'intersezione tra questi due singleton è uguale a  $\emptyset$ ,  
ma questi due insiemi non sono nulli.

↓

Non vale la legge di annullamento del prodotto

## ANELLO INTEGRO

Se ho l'anello  $(\mathcal{S}, +, \cdot)$ , se  $\mathcal{S}$  non ha la legge di annullamento del prodotto,  $\mathcal{S}$  si dice anello integro.

## DOMINIO DI INTEGRITÀ

Se ho l'anello  $(\mathcal{S}, +, \cdot)$ , se  $\mathcal{S}$  è un anello commutativo unitario integro,  $\mathcal{S}$  si dirà dominio di integrità.

HA l'ELEMENTO  
NEUTRO

VALE LA  
LAP

## DIVISORE SINISTRO DELLO ZERO

Un  $x \in a \setminus \{0\}$  si dice divisore sinistro dello 0 se:

$$(\exists y \in a \setminus \{0\})(xy = 0) \quad \text{SE 'y' E UN ELEMENTO NON NULLO E IL PRODOTTO CON UN 'x' DIVERSO DA 0 DA LO 0, X LO DIVISO SINISTRO DELLO 0}$$

ESEMPIO:  $\{a\} \cap \{b\} = \emptyset \rightarrow \{a\}$  è un divisore sinistro dello 0.

## DIVISORE DESTRO DELLO ZERO

Un  $x \in a \setminus \{0\}$  si dice divisore destro

$$(\exists y \in a \setminus \{0\})(yx = 0)$$

## DIVISORE DELLO ZERO

Un  $x \in a \setminus \{0\}$  si dice divisore dello 0 se è un divisore sinistro e un divisore destro  $\rightarrow$  DEVONO ESSERE DUE Y DIVERSI

## TEOREMA

$a \neq 0$  è un ANELLO

Un  $x \in a$  è un divisore sinistro dello 0 se e solo se  $x$  non è cancellabile a sinistra

### DIM

( $\rightarrow$ ) Supponiamo che  $x$  è un divisore sinistro dello 0.

Per definizione,  $(\exists y \in a \setminus \{0\})(xy = 0)$

Per esurdo, se fosse che  $x$  è cancellabile a sinistra,

$y = 0$  perché  $xy = 0 = x0$ . Ma ciò è un esurdo.  $\clubsuit$

( $\leftarrow$ ) Supponiamo che  $x$  non è cancellabile a sinistra.

Per definizione,  $(\exists y, z \in a)(y \neq z \wedge xy = xz) \rightarrow$  NON CANCELLABILITÀ A SINISTRA

Visto che vale  $xy = xz$ , e fanno fare le operazioni che fanno fare negli anelli, fanno fare che:  $\rightarrow$

Potrei sentire che:

$$x(y-z) = xy - xz \text{ per la distributività, ma } xy = x^2$$

quindi  $x^2 - x^2 = 0$

Ma  $y-z$  non è uguale a 0 perché  $y \neq z$ , quindi

- $x$  è un divisore sinistro dello 0 → HO TROVATO UN ELEMENTO CHE NON È ZERO MA CHE MOLTIPLICATO PER X MI DA 0  
Stesso ragionamento se  $x$  è un divisore destro.

## ANELLI BOOLEANI

Un anello  $(\sigma, +, \cdot)$  si dice **booleano** se:

$$(\forall x \in \sigma)(x^2 = x)$$

cioè  $x \cdot x$

ESEMPIO: In  $(P(S), \cup, \cap)$ , abbiamo che  $x \cap x = x$ , quindi questo anello è un anello booleano

## PROPRIETÀ

- Se  $\sigma$  è booleano,  $\sigma$  è commutativo

DIM

VOGLIO DIMOSTRARE  
CHE  $x \cdot y = y \cdot x$

Siamo  $x, y \in \sigma$

$$x+y = (x+y)^2 \text{ perché } \sigma \text{ è un anello booleano}$$

$$\text{ma } (x+y)^2 = x^2 + xy + yx + y^2 = x+y + xy + yx$$

NON POSSO SERVIRE

2xy perché non sappiamo → NON SAPPIANO SE  
SE  $xy = yx$  VALE LA COMMUTATIVITÀ

Quindi  $x+y = x+y+xy+yx$  che, per la cancellatività

di  $x+y$ , sarei:  $xy+yx=0$ , quindi  $xy=-yx$

↳ Visto che  $\sigma$  è un anello booleano, vale che  $xy=-yx=yx$

↳ Quindi  $xy=yx$  e abbiamo dimostrato la commutatività

- Se  $\sigma$  è booleano,  $x = -x$

DIM  $(x+x)^2 = x^2 + x \cdot x + x \cdot x + x^2 = x^2 + 2x^2 + x^2 = x+2x+x$

ma  $(x+x)^2 = x+x$ , quindi per la cancellatività di  $x+x$ ,  $2x=0$

↳  $2x=0$  equivale a dire che  $x+x=0$ , quindi vale che  $x=-x$

## TEOREMA

- Se  $(\mathcal{O}, +, \cdot)$  è un anello commutativo unitario,  $\mathcal{O}$  è un dominio di integrità se e solo se è privo di divisori dello 0.

DIM SUPPONIAMO CHE  $(\mathcal{O}, +, \cdot)$  SIA UN DOMINIO DI INTEGRITÀ

$\rightarrow$  Consideriamo, per secondo, che esista  $X$   
↓ che è un divisore dello zero. Cioè:

$(\exists Y \in \mathcal{O} \setminus \{0\})(XY = 0)$ . Visto che  $(\mathcal{O}, +, \cdot)$  è un dominio  
di integrità, vale la legge di annullamento del prodotto,  
quindi  $X=0 \vee Y=0$ , ma dato che, per definizione

di divisore dello 0, nessuno dei due è zero, si ha un assurdo.

$\leftarrow \rightarrow$  SUPPONIAMO CHE  $(\mathcal{O}, +, \cdot)$  SIA PRIVO DI DIVISORI DELLO ZERO

PER IL TEOREMA DI PRIMA Se finiscono di divisori dello zero, vuol dire che tutti gli elementi sono cancellabili. Allora, se  $X \cdot Y = 0$  con  $X \neq 0$ ,

$X$  è cancellabile, quindi  $Y = 0 \rightarrow$  Vale la LAP

$Y$  COTRA E CHE  
NON È ZERO

$YX = X0$

## TEOREMA

- Se  $(\mathcal{O}, +, \cdot)$  è un anello e  $\mathcal{O}$  ha almeno due elementi, allora 0 non è cancellabile.

In particolare 0 non è invertibile.

DIM

L'ANELLO NE HA ALMENO DUE PER IPOTESI

Premetto due elementi, lo 0 (che c'è sempre) e  $X$ .

$\hookrightarrow 0 \neq X \in \mathcal{O}$

Sappiamo che  $0 \cdot X = 0$ , ma zero non è cancellabile perché è così forte estremo che  $X = 0$ . Ma ciò è falso. In particolare, visto che 0 non è cancellabile, allora non è invertibile perché tutti gli invertibili sono cancellabili.

## CORPO

Se un insieme  $(\mathbb{Z}, +, \cdot)$  si dice **corpo** se  $(\mathbb{Z}, +)$  e  $(\mathbb{Z} \setminus \{0\}, \cdot)$  sono gruppi e tale ha proprietà distributiva.

Y RISPETTO ALL'ANELLO,  $(\mathbb{Z} \setminus \{0\}, \cdot)$   
HA SICURAMENTE L'UNITÀ E  
GLI INVERSI

## CAMPO

Si si riferisce a  $(\mathbb{Z} \setminus \{0\}, \cdot)$

Un corpo commutativo si dice **campo**.

Inoltre, ogni campo è dominio di integrità.

↳ Non è vero che ogni dominio di integrità è un campo

↓ Ogni campo è un dominio di integrità perché ogni campo ha gli inversi. Di conseguenza tutti gli elementi sono cancellabili. Se sono tutti cancellabili, allora non ci sono divisori dello zero. Di conseguenza, per il teorema di prima, è un dominio di integrità.

Un campo non è detto che sia un dominio di integrità perché deve essere commutativo.

## ESEMPIO:

- $(\mathbb{Z}, +, \cdot)$  è un dominio di integrità dato che non lo LAP ma non è un campo perché  $(\mathbb{Z}, \cdot)$  non è un gruppo

RELAZIONI BINARIE  $\rightarrow$  POSSONO ESSERE TUTTE SCRITTE A PARTIRE DA diag S E RELAZIONE OPPosta

Sia  $a$  un insieme non vuoto ( $a \neq \emptyset$ ) e  $p$  una relazione binaria:  $p(a \times a, g)$  con  $g \subseteq a \times a$

1.  $p$  si dice riflessiva se:  $(\forall x \in a)(x p x) \rightarrow (\exists x \in a)(x, x) \in g$

2.  $p$  si dice simmetrica se:  $(\forall x, y \in a)(x p y \rightarrow y p x)$

3.  $p$  si dice antiriflessiva se:  $(\forall x \in a)(\neg(x p x))$

ESEMPIO:

Diverso da "non riflessivo" perché  
non c'è una manca qualche coppia  
( $x, x$ ) in  $g$ , ma non ce ne sono proprio

b) la coppia  
 $(x, x) \in g$

• Ad esempio, la relazione " $<$ " è antiriflessiva

$1, 2 < 2$  è sempre falso

4.  $p$  si dice asimmetrica se:

$(\forall x, y \in a)(x p y \wedge y p x \rightarrow x = y)$

ESEMPIO:

• Ad esempio, la relazione " $\leq$ " è asimmetrica  $\rightarrow$  ALLORA  $x = y$

SE  $x \leq y$  C  $y \leq x$

5.  $p$  si dice relazione duale se:  $(\forall x, y \in a)(x \bar{p} y \rightarrow y p x)$

6.  $p$  si dice transitiva se:

$(\forall x, y, z \dots \in a)(x p y \wedge y p z \rightarrow x p z)$

b) NON SONO PER FORZA  
TUTTI ELEMENTI DISTINTI

## RELAZIONE DI EQUIVALENZA

Se  $p$  è riflessiva, simmetrica e transitiva,  
 $p$  si dice relazione di equivalenza

## RELAZIONE D'ORDINE

Se  $p$  è asimmetrica e transitiva,  
 $p$  si dice relazione d'ordine

## RELAZIONE D'ORDINE LARGO

Se  $P$  è riflessiva, asimmetrica e transitiva,  
 $P$  si dice relazione d'ordine largo

ESEMPPIO:  
↳ QUALEcosa E IN  
RELAZIONE CON  $\rightarrow$  SE STESSO  
 $\rightarrow 2 \leq 2$

## RELAZIONE D'ORDINE STRETTO

Se  $P$  è antiriflessiva, asimmetrica e transitiva,  
 $P$  si dice relazione d'ordine stretto

ESSEMPIO:  
↳ NON IN  
RELAZIONE  $\rightarrow 2 < 2$   
CON SE STESSO

↓  
Se ho  $P$  come relazione  
d'ordine stretto, l'asimmetria  
diventa inutile

↳ L'implicazione dell'asimmetria è sempre vera  
poiché  $xPy \wedge yPx$  è sempre falsa

↓  
Se fasse vero che  $xPy \wedge yPx$ , Nota che per la  
transitività avremmo che  $xPx \rightarrow$  è un assurdo ↗

UATO CHE UNA RELAZIONE  
D'ORDINE STRETTO DEVE  
ESSERE ANTIRIFLESSIVA

## ESEMPPIO:

• Verificare la transitività della relazione.

↳ Per verificarla dovrò sempre considerare più  
di due elementi distinti

↓

Se lo faccio con due o meno entra che:

$(\forall x, y, z)(xPx \wedge yPy \rightarrow xPz)$  → SE  $xPx$  È VERA,  
TUTTO È SEMPRE VERO

2.  $(\mathbb{Z} \times \mathbb{Z}, +, \circ) \rightarrow$  E' NON COMMUTATIVO?

$(a, b) + (c, d) := (a+c, b+d)$  → L'elemento neutro è la coppia  $(0, 0)$  in  $(\mathbb{Z} \times \mathbb{Z}, +)$

$$(a, b) \circ (c, d) := (ac, bd)$$

↪ Notiamo che  $(\forall d \in \mathbb{Z})(\forall a, b \in \mathbb{Z})((a, b) \circ (1, d) = (a, b))$

↪ Ci sono infiniti elementi neutri a destra

↪ Esistono elementi neutri a sinistra?

ESEMPIO:

$$(1, 1) \circ (c, d) = (c, c)$$

NON E' UN  
ELEMENTO  
NEUTRA A  
SINISTRA

Per il teorema che se c'è un elemento neutro a destra e un elemento neutro a sinistra, questi coincidono si  $a=1=d$  è l'unico elemento neutro

↪ Visto che abbiamo infiniti 1, si può dire che non esistono elementi neutri a sinistra.

Infatti,  $(ae, be) = (a, b) \circ (e, d)$ : togliamo che sia

uguale a  $(e, d)$ . Quindi  $(ae, be) = (e, d)$ .

iff anche ciò sia vero, allora avremo che:

PER ESSERE  
UGUALI,  
DUE COPIE  
DERONO AVER  
LE COORDINATE  
ORDINATAMENTE  
UGUALI

$$\cdot a \cdot e = e$$

$$\cdot be = d$$

Questo deve valere sempre, quindi deve valere anche quando  $e \neq 0$

↪ Quindi  $e$  è cancellabile a destra,

$$\text{quindi } ad = d \rightarrow \cdot a = 1$$

•  $b$  completa  $-d$  somma di  $c$  e  $d$  → Non c'è un unico elemento neutro a sinistra

• Tutte le coppie  $(0, d)$  sono divisori destra dello 0 ( $a \neq 0$ )

↪ Infatti, qualsiasi coppia  $(a, b)$  moltiplicata con  $(0, d)$  dà come risultato nulla →  $(a, b) \circ (0, d) = (0, 0)$

• Ma qualsiasi elemento  $(a, b)$  è divisore sinistro dello 0 se  $c=0$

$$(\forall (a, b) \in \mathbb{Z} \times \mathbb{Z})((a, b) \neq (0, 0) \rightarrow \text{c'è divisore sinistro dello 0})$$

↪ ESISTE UN ELEMENTO CHE NON PUO'ESSERE  
A DESTRA MA DA SINISTRA

# DIAGONALE DI $S$ E RELAZIONI BINARIE

$P = (S \times S, g)$ ,  $g \subseteq S \times S$   $x \bar{P} y \Leftrightarrow y P x$

RELAZIONE  
ESPOSTA

$\text{diag } S = \{(x, y) \in S \times S \mid x = y\} \rightarrow \text{Diagonale di } S$

TUTTE LE COPPIE  
CHE HANNO UGUALI  
LE DUE COORDINATE

ESEMPIO: • In  $\mathbb{Z} \times \mathbb{Z}$  sono:

$$(2, 2), (2, 2), (3, 3), (-2, -2)$$

• In  $S = \{a, b\}$

$$\text{diag } S = \{(a, a), (b, b)\}$$

NON SONO DEFINIZIONI  
MA MOLTI PER VEDERLO

•  $P$  è riflessiva se e solo se  $\text{diag } S \subseteq g$

$$(\forall x \in S)(x, x) \in g$$

•  $P$  è simmetrica se e solo se  $P = \bar{P}$

$$(\forall x, y \in S)(x, y) \in g \rightarrow (y, x) \in g$$

ESEMPIO: • Se  $g = \{(a, b)\}$ ,  $\bar{g} = \{(b, a)\} \rightarrow$  NON VALE LA SIMMETRIA PERCHÉ  $g \neq \bar{g}$

Immag, se  $g = \{(a, b), (b, a)\}$ ,  $\bar{g} = \{(b, a), (a, b)\}$

VALE LA SIMMETRIA  
PERCHÉ  
 $g = \bar{g}$

•  $P$  è antiriflessiva se e solo se  $\text{diag } S \cap g = \emptyset$

$$(\forall x \in S)(x, x) \notin g$$

ESEMPIO: • Se ho  $g = \{(a, b)\}$ , l'intersezione con  $\text{diag } S$  è sempre uguale a  $\emptyset$  perché non ci sono elementi uguali ( $a, a$ ) o ( $b, b$ ) in  $g \rightarrow (S \times S, g)$  è antiriflessivo

•  $P$  è antisimmetrica se e solo se  $g \cap \bar{g} \subseteq \text{diag } S$

$$(\forall x, y \in S)(x \bar{P} y \wedge y P x \rightarrow x = y)$$

ESEMPIO: • Se ho  $a \neq b$ , e dico che  $g = \{(a, b), (b, a)\}$

NON ANTISIMMETRICA  
PERCHÉ NON PUÒ ESSERE CHE  $a \neq b \in Q$   
 $(a, b) \neq (b, a) \neq (a, a)$   
 $\neq (b, b)$   
 $(a, a) \neq (b, b) \in Q$

• Immagine,  $g = \{(a, b), (a, c), (b, b)\}$  è antisimmetrica.  
 $\bar{g} = \{(b, a), (c, a), (b, b)\} \cap \bar{g} = \{(a, a), (b, b)\} \subseteq \text{diag } S$

# RELAZIONI DI EQUIVALENZA IMPORTANTI

## DEFINIZIONE DI RELAZIONE DI EQUIVALENZA

Però  $P = (S \times S, g)$  con  $g \subseteq S \times S$

$P$  è una relazione di equivalenza se  $P$  è riflessiva, simmetrica e transitiva.

## RELAZIONE UNIVERSALE

$P$  si dice relazione universale se:

$$g = S \times S$$

o RELAZIONE TOTALE

→ E' SIMMETRICA PERCHE'  
 $P = \bar{P}$  ATTO CHE  $P = S \times S$   
→ E' RIFLESSIVA PERCHE'  
 $\forall x \in S \subseteq g$   
→ E' TRANSITIVA SE CCC  
 $x \in g \in g \in x$  ALLORA  
 $\exists y \in g \in g \in x$  E' STAVO  
SEMPRE PENSARE CI SONO TUTTI

## CONGRUENZA MODULO m

Sia  $m \in \mathbb{Z}$ ,  $\equiv_m$  si dice congruenza modulo m

la definisco così:  $\frac{\text{è la}}{\text{definizione delle classi di equivalenza}}$

$$\equiv_m = (\mathbb{Z} \times \mathbb{Z}, g) \xrightarrow{\text{modulo } m}$$

$$(\forall a, b \in \mathbb{Z})((a, b) \in g \iff ((\exists k \in \mathbb{Z})(a - b = km)))$$

ESEMPIO: 2 è congruente a

$$\cdot 2 \equiv_2 2 ? \xrightarrow{2 \text{ MODULO } 2}$$

↳ Cioè, 2-2 deve essere un multiplo di 2 → Si perché le

$$((2, 2) \in g \iff (\exists k \in \mathbb{Z})(2 - 2 = k \cdot 2))$$

La congruenza modulo m è una relazione di equivalenza

1) E' RIFLESSIVA? Cioè, è vero che  $(\forall x \in \mathbb{Z})(x \equiv_m x)$  Nole?

↳ Si perché  $(\forall x \in \mathbb{Z})(x - x = 0)$  ma  $0 = 0 \cdot m \xrightarrow{\text{o } 0 \text{ È UN MULTIPLO DI } m}$

2) E' SIMMETRICA? Cioè,  $(x \equiv_m y \rightarrow y \equiv_m x)$

↳ Si perché se prendo  $x \equiv_m y$  allora  $(\exists k \in \mathbb{Z})(x - y = k \cdot m)$

Ma a Nole che  $(x - y = k \cdot m)$  allora  $(y - x = (-k) \cdot m)$ ,

quindi altrettanto che Nole  $y \equiv_m x$

↳ Se  $k$  è proprio l'inverso  
di quello di  $x \equiv_m y$

3) E' transitiva? Cioè,  $(X \equiv_m Y \wedge Y \equiv_m Z \rightarrow X \equiv_m Z)$

↪ Si perché  $(X \equiv_m Y \wedge Y \equiv_m Z)$  significa che:

$(\exists k_1, k_2 \in \mathbb{Z})(X - Y = k_1 \cdot m \wedge Y - Z = k_2 \cdot m)$ .

Allora  $(X - Y) + (Y - Z) = k_1 \cdot m + k_2 \cdot m = (k_1 + k_2) \cdot m$  ma

$(X - Y) + (Y - Z) = X - Z \rightarrow X - Z = (k_1 + k_2) \cdot m$

Ho quindi trovato un altro  $k$  affinché valga che  $X \equiv_m Z$

## RELAZIONE DI UGUALIANZA

$\equiv$  è la relazione di ugualanza

LA DIFFERENZA DI DUE NUMERI È UN MULTIPLO DI 0 QUANDO SONO LO STESSO NUMERO

↪  $a - b = k \cdot 0 \leftrightarrow a = b$

$\hookrightarrow a - b = 0 \hookrightarrow$  E' LA DIAGONALE

## RELAZIONE UNIVERSALE

$\equiv_1$  è la relazione universale

↪  $a - b = k \cdot 1 \rightarrow$  Tutti i numeri sono multipli di 1,  
quindi tutti i numeri sono in  
relazione con tutto

## NUCLEO DI EQUIVALENZA DI $f$ (DAL TEDESCO "KERNEL" CHE SIGNIFICA "NUCLEO")

Bando una funzione  $f: a \rightarrow b$

$\text{KER } f = (a \times a, g)$  si dice nucleo di equivalenza  
di  $X$ , e lo si può indicare anche con  $\sim_f$  se:

$(\forall x, y \in a)(x \in \text{KER } f \wedge y \leftrightarrow f(x) = f(y))$

DUE ELEMENTI SONO IN  
RELAZIONE KER  $f$  SE E  
SOLO SE HANNO LE  
IMMAGINI UGUALI

## CLASSE DI EQUIVALENZA DI $X$ (MODULO $p$ )

• Sia  $P = (S \times S, g)$  con  $g \subseteq S \times S$ , preso  $x \in S$ ,

$[x]_P$  si dice classe di equivalenza di  $x$  (modulo  $p$ )

$[x]_P := \{y \in S \mid x \sim_p y\}$

SONO TUTTI GLI "CHE  
SONO IN RELAZIONE DI  
EQUIVALENZA CON X"

$y$  SI CHIAMA RAPPRESENTANTE  
DELLA CLASSE

• Per brevità, se ho che  $P = \equiv_m$ , allora  $[x]_{\equiv_m}$  lo indico  $[x]_m$

$\hookrightarrow [x]_{\equiv_m} := [x]_m$

## ESEMPIO:

- $[2]_2 \rightarrow$  Sono tutti quanti i numeri tali che 2 - quel numero è un multiplo di 2.

$$[2]_2 = \{ y \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(2-y=2k) \} \rightarrow \text{? c'è? si perché } 2-y \text{ È UN MULTIPLO DI 2}$$

↳ Questi sono tutti i numeri pari

↳ Infatti  $2-y=2k$  solo se  $y$  è un numero pari

- $[5]_2 = \{ y \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(5-y=2k) \}$

↳ Affinché si abbia che  $5-y=2k$ ,  $y$  deve essere

dispari  $\rightarrow$  SE SOTTRAGGO A 5 UN NUMERO PARI, OTTENGO UN NUMERO DISPARI CHE NON È UN NUMERO MULTIPLO DI 2

↳ INVECE SE SOTTRAGGO UN NUMERO DISPARI OTTENGO UN NUMERO PARI

$[5]_2 \rightarrow$  Sono tutti i numeri dispari.

Inoltre,  $[5]_2 = [1]_2$  perché anche  $[1]_2$  sono tutti i numeri dispari

## INSIEME QUOTIENTE

$S/p$  si dice insieme quoziente di  $S$  rispetto a  $p$  se:

$$S/p := \{ [x]_p \mid x \in S \} \rightarrow \text{E' L'INSIEME DI TUTTE LE CLASSI DI EQUIVALENZA DI MODULO } p \text{ PER UN QUALCHE ELEMENTO DI } S$$

P E SEMPRE UNA RELAZIONE DI EQUIVALENZA

COME FORMULA

BEN FORMATA E':  $S/p = \{ y \in P(S) \mid (\exists x \in S)(y = [x]_p) \}$

# PROPRIETA' FONDAMENTALI DELLE CLASSE DI EQUIVALENZA

1) Ogni classe di equivalenza è non vuota. Cioè:

$$(\forall y \in S/p)(y \neq \emptyset)$$

DIM

DI S/p

TH: Prendo un certo  $y \in S/p$ ,  $y$  sarà una classe di  $p$  per la definizione.

Quindi ci sarà un  $x$  tale che  $y = [x]_p$

↳ Per la riflessività di  $p$ , ho sicuramente  $xpx$ .

Quindi  $x \in [x]_p$ , quindi  $x$  sta nella classe di equivalenza di  $x$  stesso e quindi  $[x]_p$  non sarà mai vuota.

2) Le classi di equivalenza sono a due a due

disgiunte  $\rightarrow$  SE HO DUE CLASSI DI EQUIVALENZA DIVERSE,  
LA LORO INTERSEZIONE E' IL VUOTO

↳ Se due classi di equivalenza condividono anche un solo elemento, allora sono le stesse classi di equivalenza (LA NEGAZIONE)

$$(\forall y, z \in S/p)(y \neq z \rightarrow y \cap z = \emptyset)$$

DIM

Uso la tautologia della negazione di  $\rightarrow$ . Voglio dimostrare che, supposto  $y \cap z \neq \emptyset$ , allora  $y = z$

Suppongo  $y \cap z \neq \emptyset$ . Prendo  $x \in y \cap z$

Serivo  $y$  e  $z$  come classi di equivalenza:

$$\hookrightarrow y = [\bar{y}]_p \quad e \quad z = [\bar{z}]_p$$

↳ PER LA DEFINIZIONE DI INSIEME QUOTIENTE

Visto che  $x$  sta sia in  $[\bar{y}]_p$  che in  $[\bar{z}]_p$ ,  
per definizione vale  $\bar{y}px$  e  $\bar{z}px$

Per la simmetria di  $p$  vale anche  $x\bar{p}\bar{y}$  e  $x\bar{p}\bar{z}$ .

Per la transitività di  $p$ , se ho  $\bar{y}px$  e  $x\bar{p}\bar{z}$  allora  
vale  $\bar{y}p\bar{z}$ . Ma vale anche  $\bar{z}p\bar{y}$  da  $\bar{z}px$  e  $x\bar{p}\bar{y}$

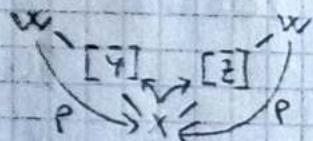
Di conseguenza, per definizione di classe di equivalenza:

$$\begin{aligned} \cdot \bar{y}p\bar{z} &\rightarrow \bar{z} \in [\bar{y}]_p \\ \cdot \bar{z}p\bar{y} &\rightarrow \bar{y} \in [\bar{z}]_p \end{aligned}$$

Se prendo un certo elemento  $w \in [\bar{y}]_p$ :

$$w \in [\bar{y}]_p \leftrightarrow \bar{y}p w \leftrightarrow \bar{z}p w \leftrightarrow w \in [\bar{z}]_p$$

Quindi  $[\bar{y}]_p = [\bar{z}]_p$  perché ho appena dimostrato che  
ogni elemento di  $[\bar{y}]_p$  appartiene a  $[\bar{z}]_p$  e viceversa.



3) d' unione dell' insieme quoziente è  $S$

$$\hookrightarrow \bigcup S_p = S \rightarrow \text{STO PRENDENDO TUTTI GLI ELEMENTI DELLE CLASSI DI EQUIVALENZA}$$

DIM

( $\subseteq$ ) Se  $y \in \bigcup S_p$  allora  $(\exists [x]_p)(y \in [x]_p)$   
allora, visto che  $[x]_p \in P(S)$ ,  $y \in S$

ESISTE UN ELEMENTO DEGLI ELEMENTI TALE CHE GLI APPARTIENE

( $\supseteq$ ) Se prendo  $x \in S$ , allora  $[x]_p \in S_p$

Quindi  $x \in \bigcup S_p$

X APPARTIENE ALLA PROPRIA CLASSE DI EQUIVALENZA PER LA PROPRIETÀ 1

Quindi i due insiemi sono uguali perché gli elementi di uno sono gli elementi dell' altro.

E' EQUIVALENTE DIRE CHE:

$$x \rho y \leftrightarrow y \rho x \leftrightarrow x \in [y]_\rho \leftrightarrow y \in [x]_\rho \leftrightarrow [x]_\rho = [y]_\rho \leftrightarrow [x]_\rho \cap [y]_\rho \neq \emptyset$$

~~~~~

Correzione esercizi 30/11/2021 (LEZIONE 20)

3. 1) $f: m \in \mathbb{Z} \mapsto m+1 \in \mathbb{Z}$ ($\mathbb{Z} \times \mathbb{Z}, f$)

Notiamo che f è iniettiva, quindi:

$$x \in \text{KER } f \leftrightarrow f(x) = f(y) \leftrightarrow x = y$$

Quindi $\text{KER } f$ è proprio l'uguaglianza, coincide con la relazione " $=$ "

ESEMPIO: Se ho $[0]_{\text{KER } f}$, questi sono tutti quanti gli elementi di \mathbb{Z} che hanno per immagine l'immagine di 0

$$\hookrightarrow [0]_{\text{KER } f} = \{0\} \rightarrow \text{CI SONO TANTI SINGLETON QUANTI GLI ELEMENTI DI } \mathbb{Z}$$

$$\mathbb{Z}_{/\text{KER } f} = \{\{m\} \mid m \in \mathbb{Z}\}$$

CON LA RELAZIONE DI UGUALANZA SOLO DA UN LIVELLO, METTI LE PARENTESI GIAFFE ALL'ELEMENTO

NOTAZIONE ALTERNATIVA PER DIRE CHE SONO I SINGLETON DEGLI ELEMENTI DI \mathbb{Z} . DOVREI SCRIVERE:

$$\mathbb{Z}_{/\text{KER } f} = \{y \in \mathcal{P}(\mathbb{Z}) \mid y = \{m\}\}$$

$\mathbb{Z}_{/\text{KER } f} \cap \mathbb{Z} = \emptyset$ perché \mathbb{Z} ha i numeri, non i singleton dei numeri

$\mathbb{Z}_{/\text{KER } f}$ e \mathbb{Z} sono legati da una relazione isomorfa

↪ ESEMPIO: $\{m\} + \{m\} = \{m+m\}$ ecc...

$$7. f: m \in \mathbb{Z} \mapsto (-1)^m \in \mathbb{Z} - (\mathbb{Z} \times \mathbb{Z}, g)$$

Trovare $\text{KER } f$. $x \in \text{KER } f \iff f(x) = f(y)$

\hookrightarrow Per vedere come è fatto $\text{KER } f$, devo vedere come sono le immagini $f(x) \in f(y)$

Quando $(-1)^x = (-1)^y$? Quando $x \in y$ sono entrambi pari o entrambi dispari

$$(-1)^x = (-1)^y \Leftrightarrow \begin{cases} x \text{ e } y \text{ sono pari} \\ x \text{ e } y \text{ sono dispari} \end{cases} \xrightarrow{\text{stesso grafico}} x \equiv_2 y \rightarrow \begin{cases} \text{DUE ELEMENTI} \\ \text{SONO IN RELAZIONE} \\ \text{PER } \text{KER } f \text{ SE ESSO} \\ \text{SE SONO IN} \\ \text{RELAZIONE } \equiv_2 \end{cases}$$

Quindi $\text{KER } f$ coincide con la relazione \equiv_2

\hookrightarrow Stesso dominio, codominio e grafico

Chi è $\mathbb{Z}/\text{KER } f$? l'insieme delle classi di equivalenza modulo $\text{KER } f$

$$\mathbb{Z}/\text{KER } f = \left\{ [0]_{\text{KER } f}, [1]_{\text{KER } f} \right\} \rightarrow \begin{array}{l} \text{Perché una classe di} \\ \text{equivalenza prende tutte le} \\ \text{relazioni "essere pari" e} \\ \text{l'altra "essere dispari"} \end{array}$$

\downarrow
Non ci sono elementi di \mathbb{Z} lasciati fuori, tutti rientrano in una classe di equivalenza.

OMOOMORFISMO TRA GRUPPI

Prendiamo $f: g_1 \rightarrow g_2$ con g_1 e g_2 gruppi e f come omomorfismo tra gruppi.

Sappiamo per definizione che $X \text{ KER } f \Leftrightarrow f(x) = f(y)$

Essendo g_1 e g_2 gruppi, tutti i loro elementi sono invertibili quindi avremo che in g_2 :

$$f(x) = f(y) \Leftrightarrow f(x) \cdot (f(y))^{-1} = 1_{g_2} \xrightarrow{\substack{\text{COME SE FOSSE } f(x) \cdot (f(x))^{-1} = 1 \\ \text{DI INVERSA}}} \quad \text{DEFINIZIONE}$$

Per le proprietà di conservazione degli omomorfismi sappiamo che $(f(y))^{-1} = f(y^{-1})$, di conseguenza:

$$f(x) \cdot (f(y))^{-1} = 1_{g_2} \Leftrightarrow f(x) \cdot f(y^{-1}) = 1_{g_2}$$

Per definizione di omomorfismo, però:

$$f(x) \cdot f(y^{-1}) = 1_{g_2} \Leftrightarrow f(x \cdot y^{-1}) = 1_{g_2}$$

RELAZIONE
KER φ PER
GLI OMOOMORFISMI
DI GRUPPI

Quindi abbiamo che $\boxed{X \text{ KER } f \Leftrightarrow f(x \cdot y^{-1}) = 1_{g_2}}$

Se f è iniettiva (è un monomorfismo) allora avremo che x l'immagine è un'identità allora anche l'antimmagine lo è: $f(x \cdot y^{-1}) = 1_{g_2} \Leftrightarrow x \cdot y^{-1} = 1_{g_1} \xrightarrow{\substack{\text{QUINDI } x=y}}$

ESEMPIO:

• Se ho $f: X \in G \mapsto x^{-1} \in G$ con G abeliano, f è un omomorfismo

↪ Prendo $x \cdot y \in G$, la sua inversa $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$, ma

dato che G è abeliano allora $y^{-1} \cdot x^{-1} = x^{-1} \cdot y^{-1} \xrightarrow{\substack{\text{MOLTIPLICATO } xy \\ \text{DA } ? \text{ IDENTITÀ}}} \Rightarrow f$ è un omomorfismo

$$\boxed{x \in \text{KER } f \Leftrightarrow f(x) = f(y) \Leftrightarrow x^{-1} = y^{-1} \Leftrightarrow x = y \xrightarrow{\substack{\text{L'INVERSO E' UNICO}}}}$$

Se $\text{KER } f$ è l'inversione (nei gruppi) allora è la funzione identità

TEOREMA FONDAMENTALE DI OMOMORFISMO PER INSIEMI (PREHESSE)

- Presi due insiemi a e b ,

Considero una funzione

$$f: a \rightarrow b$$

- Esistono una cosa immagine

di f che è un sottoinsieme di b

$$\hookrightarrow \text{Im } f \subseteq b$$

Esistono quindi la funzione immersione:

$$x \in \text{Im } f \rightarrow x \in b \rightarrow \text{funzione immersiva} \rightarrow \begin{array}{l} \text{E PRATICAMENTE} \\ \text{L'IDENTITÀ MA NON} \\ \text{SURGETTIVA} \end{array}$$

- Anziemo anche un insieme quoziente di a su $\text{Ker } f$

\hookrightarrow Poco prendere una funzione π che associa ad ogni elemento $x \in a$, la classe di equivalenza di x .

$$\pi: x \in a \mapsto [x] \in a/\sim \rightarrow \text{Queste funzioni si chiamano proiezione canonica di } a \text{ su } a/\sim$$

Questa è una funzione ovviamente surgettiva

\rightarrow OGNI ELEMENTO x HA UNA CLASSE DI EQUIVALENZA
STUTTE LE CLASSI DI EQUIVALENZA SONO PRESE IN a/\sim

- Vogliamo chiudere il diagramma in maniera commutativa. Prendo una funzione \tilde{f} , tale che:

$$\tilde{f}: [x]_{\sim} \in a/\sim \mapsto f(x) \in \text{Im } f$$

Ma \tilde{f} è ben posta? Potrebbe succedere che, per x e y diversi, ma con la stessa classe di equivalenza, potrebbe succedere che l'immagine di una stessa classe di equivalenza è sia $f(x)$ che $f(y)$ che sono diversi

\hookrightarrow Controlliamo se \tilde{f} è ben posta.

$$\begin{array}{ccc} a & \xrightarrow{f} & b \\ \pi \downarrow & & \uparrow \iota \\ a/\sim & \xrightarrow{\tilde{f}} & \text{Im } f \end{array}$$

\tilde{f} è ben posta?

Prendo $(x, y \in a) / [x]_{\sim_f} = [y]_{\sim_f}$. Dobbiamo dimostrare che i elementi uguali sono le immagini uguali.

$$\tilde{f}([x]_{\sim_f}) = f(x) \text{ per definizione.}$$

Dalle proprietà fondamentali delle classi di equivalenza soffiamo che $[x]_{\sim_f} = [y]_{\sim_f}$ significa dire che $x \sim_f y$. Ma la relazione \sim_f è quella di "essere le stesse immagine". Di conseguenza:

DEFINIZIONE
DI KER f

$$\tilde{f}([x]_{\sim_f}) = f(x) = f(y) = \tilde{f}([y]_{\sim_f})$$

Ottiamo fatto vedere che per ogni elemento di a/\sim_f , ce n'è uno solo nel grafico che ha come prima coordinate l'elemento di a/\sim_f e cioè quando come seconde coordinate ottiamo $f(x)$.

$\hookrightarrow f(x)$ non cambia a variazione del rappresentante della classe $\rightarrow f(x)$ non dipende dal rappresentante

Quindi \tilde{f} è ben posta

TEOREMA FONDAMENTALE DI OMOMORFISMO

PER INSIEMI

Vale che:

- 1) \tilde{f} è biettiva
- 2) $f = i \circ \tilde{f} \circ \pi$

$$\begin{array}{ccc} a & \xrightarrow{\tilde{f}} & b \\ \pi \downarrow & \uparrow i & \\ a/\sim_f & \xrightarrow{f} & \text{Im } f \end{array}$$

PER DEFINIZIONE:

$[x]_{\sim_f} = \{\tilde{f}(f(x))\}$ Perché con $[x]_{\sim_f}$ sto prendendo tutti gli elementi di a che sono in relazione \sim_f con x . $\rightarrow x \sim_f y \Leftrightarrow f(x) = f(y)$

\hookrightarrow Hanno tutta la stessa immagine, cioè $f(x) \in \text{IMMAGINE di } x$

DIM

1) Definisco α :

$$\alpha: f(x) \in \text{Im } f \mapsto [x]_{\sim_f} \in \alpha/\sim_f \rightarrow$$

ASSOCIA AD OGNI IMMAGINE
DI x , LA CLASSE DEGLI
ELEMENTI CHE VANNO
IN $f(x)$

↪ α è una funzione perché ad ogni elemento associa una classe

• α è suriettiva?

Sia $y \in \alpha/\sim_f$, cioè $(\exists z \in \alpha)(y = [z]_{\sim_f})$.

Per dunque, $\alpha(f(y)) = [y]_{\sim_f} = y$ quindi α è suriettiva

↪ Cioè, preso una classe di equivalenti con rappresentante y , troverò sempre l'elemento associato: proprio $f(y)$

• α è iniettiva?

Se ho che $[x]_{\sim_f} = [y]_{\sim_f}$, dalla definizione di \sim_f , $f(x) = f(y)$. Di conseguenza α è iniettiva.

↪ Ho preso due immagini di α uguali e ho visto che $f(x) = f(y)$, quindi se $[x]_{\sim_f} \neq [y]_{\sim_f}$ anche $f(x) \neq f(y)$

$$[x]_{\sim_f} = [y]_{\sim_f} \Leftrightarrow f(x) = f(y)$$

• Quindi α è biettiva. → C'è l'inverso

Definisco $\tilde{f}: = \alpha^{-1} \rightarrow$ Quindi \tilde{f} è biettiva perché ha l'inverso

Si tratta di una
FUNZIONE CHE
VOLEVANO PER
COME L'ABBANDONARO
DEFINITA

↪ Il punto 1 è verificato

2) Per vedere che $\tilde{f} = \text{co}\tilde{f} \circ \pi$ dobbiamo vedere che le due funzioni hanno dominio, codominio e grafico uguali.

- Il dominio di f è a .
Il dominio di $i \circ \tilde{f} \circ \pi$ è a dato che è quello di π .
- Il codominio di f è b .
Il codominio di $i \circ \tilde{f} \circ \pi$ è b perché è quello di i .
- Per vedere che f e $i \circ \tilde{f} \circ \pi$ hanno lo stesso grafico dobbiamo vedere che le immagini degli elementi sono le stesse.
 - ↳ L'immagine di f è $f(x)$
 - ↳ Chi è $(i \circ \tilde{f} \circ \pi)(x)$?
 - ↳ $(i \circ \tilde{f} \circ \pi)(x) = i(\tilde{f}(\pi(x))) = i(f([x]_{\sim_f})) = i(f(x)) = f(x)$

Dato che queste due funzioni hanno lo stesso dominio, lo stesso codominio e lo stesso grafico, allora $f = i \circ \tilde{f} \circ \pi \rightarrow$ il punto 2 è verificato

COROLLARIO

Ogni funzione si può scrivere come la composizione di una funzione iniettiva e una suriettiva.

↳ L'ordine è importante, la prima funzione deve essere iniettiva e la seconda suriettiva.

Per ogni $f: a \rightarrow b$, con a e b due insiemi, esiste un insieme c tale che:

$\exists g$ iniettiva da $c \rightarrow b$

$\exists h$ suriettiva da $a \rightarrow c$

Tale che $f = g \circ h$

INFATTI, IN $f = i \circ \tilde{f} \circ \pi$, $\tilde{f} \circ \pi$ è la h , MENTRE i è la g

ESEMPIO:

- Come posso scrivere $f: m \in \mathbb{Z} \mapsto (-1)^m \in \mathbb{Z}$ come composizione di una funzione iniettiva e una suriettiva?

Trovò l'insieme quoziante, in modo tale da scrivere π (la proiezione canonica), quindi la funzione \tilde{f} e l'immersione da funzione $\tilde{f} \circ \pi$ sarà la mia funzione suriettiva e i (immersione) è la funzione iniettiva.

$$\mathbb{Z}_{\text{fg}} = \{[0]_2, [1]_2\}$$

$$\pi: m \in \mathbb{Z} \xrightarrow{\begin{array}{l} \text{PARI} \\ \text{DISPARI} \end{array}} \in \mathbb{Z}_{\text{fg}} \xrightarrow{\begin{array}{l} \text{MANDA I PARI NEI PARI} \\ \text{E I DISPARI NEI DISPARI} \end{array}}$$

$$i: m \in \text{Im } f \mapsto m \in \mathbb{Z}$$

$$\tilde{f}: \begin{array}{l} [0]_{\text{fg}} \mapsto f(0) = 1 \\ [1]_{\text{fg}} \mapsto f(1) = -1 \end{array} \in \{-1, 1\}$$

$$i \circ \tilde{f}: \begin{array}{l} [0]_{\text{fg}} \in \mathbb{Z}_{\text{fg}} \mapsto 1 \in \mathbb{Z} \\ [1]_{\text{fg}} \end{array}$$

$i \circ \tilde{f}$ è iniettiva perché i due elementi di \mathbb{Z}_{fg} si manda in due immagini separate.

π è suriettiva perché manda tutti gli \mathbb{Z} o nei pari o nei dispari, in \mathbb{Z}_{fg} non c'è altro oltre i pari o i dispari.

$$f = (i \circ \tilde{f}) \circ \pi$$

$$f: m \in \mathbb{Z} \mapsto m+1 \in \mathbb{Z}$$

~~Notiamo che f è suriettiva perché per ogni $n \in \mathbb{Z}$ esiste $m \in \mathbb{Z}$ tale che $f(m) = n$.~~

~~Quindi f è suriettiva.~~

Notiamo che f è già di per sé iniettiva, quindi basta fare la composizione con l'identità (che è suriettiva)

↳ E' BANALE

- $f: m \in \mathbb{Z} \mapsto (-1)^m \in \mathbb{Z}$

Prendo la funzione $\tilde{g}: [n]_{\mathbb{Z}} \in \mathbb{Z} \mapsto m+1 \in \mathbb{Z}$

La funzione \tilde{g} non è ben posta, infatti:

$$\tilde{g}([0]_{\mathbb{Z}}) = 1$$

$$\tilde{g}([2]_{\mathbb{Z}}) = 3$$

Ma $[0]_{\mathbb{Z}}$ e $[2]_{\mathbb{Z}}$ sono lo stesso elemento nell'insieme quoziente, quindi nel grafico della funzione ci sono le cosidd $([0]_{\mathbb{Z}}, 1)$ e $([0]_{\mathbb{Z}}, 3)$. Di conseguenza \tilde{g} non è una funzione perché a uno stesso x sono associate due immagini diverse

↳ Non è ben posta.

PARTIZIONI DI α

Sia α un insieme. Un insieme β sottinsieme delle parti di α ($\beta \subseteq P(\alpha)$) si dice partizione di α :

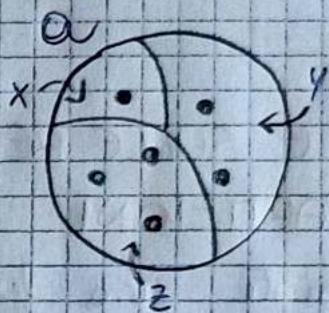
CONCETTO
SIMILE A
QUELLO DI
CLASSI DI
EQUIVALENZA

$$1) (\forall x \in \beta)(x \neq \emptyset)$$

$$2) (\forall x, y \in \beta)(x \neq y \rightarrow x \cap y = \emptyset)$$

$$3) \bigcup \beta = \alpha$$

ESEMPIO:



$$\beta = \{x, y, z\}$$

↳ E' una partizione

- Se prendano $x, y \circ z$ tutti allora β non era una partizione
- Se c'era anche un solo elemento in comune tra $x, y \circ z$ non c'era la partizione
- Se lasciato anche un solo elemento fuori, β non era più una partizione

PARTIZIONI BANALI DI α

Sono partizioni:

$$\bullet \beta = \{\alpha\}$$

$$\bullet \beta = \{\{x\} \mid x \in \alpha\}$$

→ LA PARTIZIONE DEI SINGOLI ELEMENTI

RELAZIONE TRA PARTIZIONI E RELAZIONI DI EQUIVALENZA

d'insieme quoziente, rispetto a una relazione di equivalenza, è una partizione \rightarrow c'è un'affezione biunivoca tra i due concetti

Questa applicazione diretta ci viene data dal teorema fondamentale sulle relazioni di equivalenza e le partizioni

↳ INFORMAZIONI PRELIMINARI

- Definisco $\text{EQ}(\alpha)$ come l'insieme di tutte le relazioni di equivalenza su α
 - Definisco $\text{PART}(\alpha)$ come l'insieme di tutte le partizioni di α
- PER L'ASSIOMA DI SEPARAZIONE

TEOREMA FONDAMENTALE SULLE RELAZIONI DI EQUIVALENZA E LE PARTIZIONI

Per ogni insieme α , esiste una funzione diretta f che ad una certa relazione di equivalenza $\sim \in \text{EQ}(\alpha)$ associa $\% \in \text{PART}(\alpha)$

$$\hookrightarrow f: \sim \in \text{EQ}(\alpha) \longmapsto \% \in \text{PART}(\alpha)$$

OGNI PARTIZIONE POSSO SCRIVERLA COME RELAZIONE DI EQUIVALENZA

STESO CONCETTO VISTO SOTTOFORMA DI ELEMENTI IN RELAZIONE E DI SOTTO INSIEMI DI QU

DIM

- f è iniettiva?
- SE LE IMMAGINI SONO UGUALI ALLORA PIRE CHE GLI ELEMENTI DA CUI VENGONO SONE UGUALI

Premolo: $\sim_1, \sim_2 \in \text{EQ}(\alpha)$

Suffrago che $f(\sim_1) = f(\sim_2)$, cioè che $\%_{\sim_1} = \%_{\sim_2}$

Quindi per definizione, $\%_{\sim_1} = \%_{\sim_2}$ significa che

$$\{[X]_{\sim_1} \mid X \in \alpha\} = \{[X]_{\sim_2} \mid X \in \alpha\} \quad \begin{matrix} \downarrow \\ \text{DOBBIANO FAR VEDERE CHE OGNI COPPIA DI ELEMENTI IN RELAZIONE } \sim_1, \text{ SONO ANCHE IN RELAZIONE } \sim_2 \end{matrix}$$

$$\forall x, y \in \alpha, x \sim_1 y \leftrightarrow [x]_{\sim_1} = [y]_{\sim_1} \leftrightarrow (\exists z \in \alpha)([x]_{\sim_1} = [z]_{\sim_2})$$

$$\text{e } (\exists w \in \alpha)([y]_{\sim_1} = [w]_{\sim_2}) \leftrightarrow w \sim_2 z \leftrightarrow x \sim_2 y$$

x E y SONO NELLA STESSA CLASSE DI EQUIVALENZA QUINDI ANCHE w E z SONO IN RELAZIONE \sim_2

Infatti, $x, y \in [z]_r$, e quindi le classi sono equivalenti

Quindi, visto che assunto $f(z_1) = f(z_2)$ abbiamo che $x \sim y$, f è iniettiva.

- f è suriettiva? ~ Dobbiamo far vedere che esiste una relazione di equivalenza che abbia come immagine una partizione
Sia $\{f\} \in \text{PART}(a)$

Definisco:

$$(\forall x, y \in a)(x \sim y : \leftrightarrow ((\exists z \in \{f\})(x \in z \wedge y \in z))$$

x e y appartengono ad uno stesso elemento della partizione

\sim è una relazione di equivalenza?

- 1) È riflessiva? Sì, perché x e x appartengono a uno stesso elemento della partizione. \rightarrow Per me sarà sempre uno che li contiene
 \downarrow
 $(\forall x \in a)(\exists z \in \{f\}(x \in z))$ perché $U_f = a$

- 2) È simmetrica? Se x, y appartengono alla stessa parte, anche y, x appartengono alla stessa parte

- 3) È transitiva? Prendo $x \sim y \wedge y \sim z$. Per definizione:

$$(\exists w_1, w_2 \in \{f\})(x \in w_1 \wedge y \in w_1 \wedge y \in w_2 \wedge z \in w_2)$$

Ma ciò significa che $w_1 \cap w_2 \neq \emptyset$ (c'è y)

- ↳ Dalla definizione di partizione, se l'intersezione tra i due mondi vuote, $w_1 = w_2$

\downarrow
Quindi $x \sim z$, quindi vale la transitività.

Quando è vero che $f(z) = \emptyset$?

Sì, $f(z)$ è proprio \emptyset

→ MOTIVAZIONE
PROSSIMA PAGINA

Infatti, essendo $f(\sim)$ l'insieme quoziente, è l'insieme di tutti gli elementi che stanno nella parte della partizione $\{ \}$

↪ Ogni singolo elemento di $\{ \}$ sta in $f(\sim)$ e ogni singola classe di equivalenza è una parte della partizione $\rightarrow f(\sim)$ e $\{ \}$ coincidono
↪ PER CIOE' E' STATA DEFINITA

PERCHÉ IL TEOREMA FONDAMENTALE SULLE RELAZIONI DI EQUIVALENZA E LE PARTIZIONI È UTILE?

Il teorema fondamentale delle relazioni di equivalenza e le partizioni è utile perché, per un certo insieme, posso definire la relazione di equivalenza semplicemente facendo delle partizioni a caso dell'insieme

↪ One posso, ad esempio, elencare tutte le relazioni di equivalenza di un insieme con tre elementi

↪ MI BASTA FARLE DELLE PARTIZIONI DELL'INSIEME CON TRE ELEMENTI

$$1. f: m \in \mathbb{Z} \mapsto m^2 \in \mathbb{Z}$$

Servirebbe la funzione f come composizione di una funzione iniettiva e una suriettiva

↪ Usiamo il teorema fondamentale per l'omomorfismo tra gli insiemi

1. Bisogna trovare il $\text{KER } f$
per trovare la funzione π



UN MODO PER SCRIVERE
LA RELAZIONE
 $\text{ker } f = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid f(m) = f(n)\}$ → TUTTE LE COPIE
DI ELEMENTI CHE
HANNO LA STESSA
IMMAGINE

UN ALTRO
MODO DI
SCRIVERE IL
 $\text{ker } f$



$$\text{ker } f = \{m \in \mathbb{Z} \mid f(m) = f(m)\} = \{m \in \mathbb{Z} \mid m^2 = m\}$$

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & \mathbb{Z} \\ \pi \downarrow & & \uparrow i \\ \mathbb{Z}_{\text{ng}} & \xrightarrow{\sim} & \text{Im } f \end{array}$$

Se due numeri elevati al quadrato sono uguali
e solo se sono uguali oppure uno è l'opposto
dell'altro → PROPRIETÀ ARITMETICA IN \mathbb{Z} DICE $\sqrt{m^2} = \pm m$

$$\hookrightarrow m^2 = m^2 \leftrightarrow m = m \vee m = -m$$



↳ piatta PER
SCONTRARE ALCUNE
PROPRIETÀ ARITMETICHE
IN \mathbb{Z}

Quindi stiamo dicendo che due elementi sono in
relazione tra di loro quando o uno è uguale all'altro
o uno è l'opposto dell'altro → $m \in \text{ker } f \iff m = m \vee m = -m$

$$\hookrightarrow [\text{ker } f] = \{m, -m\} \rightarrow f(m) = m^2 \quad f(-m) = m^2$$

Quindi, \mathbb{Z}_{ng} , che è per definizione l'insieme di
tutte le classi di equivalenza di modulo \sim_f è
proprio l'insieme delle copie $\{m, -m\} \forall m \in \mathbb{Z}$

SURIEDETTA

Quindi, $\pi: m \in \mathbb{Z} \mapsto [m]_{\text{ng}} \in \mathbb{Z}_{\text{ng}}$

↪ ANCHE $\{0, -0\}$ CHE
IN REALTA' È $\{0\}$

cioè, $\pi: m \in \mathbb{Z} \mapsto \{m, -m\} \in \mathbb{Z}_{\text{ng}} \rightarrow$ PER ESSERE PIÙ ESPLICATIVA

\tilde{f} è quella relazione che a qualunque classe di equivalenza associa f di un qualunque rappresentante della classe

$$\hookrightarrow \tilde{f}: [m]_{\sim_f} \in \mathbb{Z}_{\sim_f} \mapsto f(m) \in \text{Im } f$$

Ma $\text{Im } f$ è proprio \mathbb{N} dato che m^2 è un numero sempre positivo

$$\hookrightarrow \tilde{f}: \{m, -m\} \in \mathbb{Z}_{\sim_f} \mapsto m^2 \in \mathbb{N}$$

SURROGAZIONE

$$\underbrace{i \circ \tilde{f}}_{\text{INIEZIONE}}: \{m, -m\} \in \mathbb{Z}_{\sim_f} \mapsto m^2 \in \mathbb{Z}$$

INIEZIONE

Ho trovato le due funzioni tali che $f = (i \circ \tilde{f}) \circ \pi$

$$8. \quad \alpha = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

$\xrightarrow{\text{RELAZIONE DI EQUIVALENZA}}$
 $P = (\alpha \times \alpha, g)$

$$\text{Vb: } 0 \sim 6 \quad 0 \sim 7 \quad (1, 4) \in g \quad \{3, 4, 5, 7\} \subseteq [2]_P$$

Visto che abbiamo che $\{3, 4, 5, 7\} \subseteq [2]_P$, allora in selezione con 2 sono:

- 2 perché P è riflessiva essendo una relazione di equivalenza
- 3, 4, 5, 7 perché $\{3, 4, 5, 7\} \subseteq [2]_P$
- 0 perché, per la transitività 0 è in relazione con 7 e 7 è in relazione con 2
- 6 per simmetria e transitività tra 0 e 7
- 1 perché $(1, 4) \in g$ (cioè 1 è in relazione con 4) e si ha la transitività

$$\text{Quindi } [2]_P = \alpha \rightsquigarrow \alpha / P = \{\alpha\}$$

\hookrightarrow C'è una sola classe di equivalenza, quindi la relazione di equivalenza è univocamente determinata

Quindi g è quella dove tutti sono in relazione con tutti

\hookrightarrow da relazione universale $\rightarrow g = \alpha \times \alpha \rightarrow \text{RELAZIONE BANALE}$

RELAZIONE D'ORDINE

Una relazione d'ordine è una relazione asimmetrica e transitiva. Inoltre, si vede anche la:

- Riflessività si parla di relazione d'ordine largo
- Antiriflessività si parla di relazione d'ordine stretto

INSIEME DELLE RELAZIONI DI ORDINE LARGO

Sia $a \neq \emptyset$, definisco l'insieme di tutte le relazioni di ordine largo:

$$[OL(a) = \{ p \in P(P(P(\{a \times a\})) \mid \underbrace{\text{RIFL} \wedge \text{ASIMM} \wedge \text{TRANS}}_{(x \in a)(x \neq x) \wedge \dots \wedge \dots} \}]$$

PERCHE?

Verifichiamo a chi appartiene p .

$$\hookrightarrow p = (a \times a, g)$$

Per definizione delle copie ordinate, $p = \{\{a \times a\}, \{a \times a, g\}$

\downarrow $\{a \times a\}$ di chi è sottoinsieme?

$$\hookrightarrow a \times a \subseteq a \times a \quad (\text{e' ovvio})$$

Quindi il singleton di $a \times a$ è un sottoinsieme delle parti di $a \times a$

$$\hookrightarrow \{a \times a\} \subseteq P(a \times a)$$

Visto che $\{a \times a\} \subseteq P(a \times a)$ e $g \subseteq a \times a$, allora.

$$\{a \times a, g\} \subseteq P(a \times a)$$

Noi vogliamo scoprire p di chi è elemento. Essendo $\{a \times a\}$ e $\{a \times a, g\}$ delle parti di $a \times a$, allora questi saranno elementi delle parti delle parti di $a \times a$

$$\hookrightarrow \{a \times a\} \in P(P(a \times a)) \quad \text{e} \quad \{a \times a, g\} \in P(P(a \times a))$$

Per avere un altro livello di parentesi e tenere
 $\{\{x\}, \{x, y\}\}$ dentro nelle $P(P(P(x)))$
 ↳ Quindi, $\{\{x\}, \{x, y\}\} \in P(P(P(x)))$

Per questo: $p = (x, y) = \{\{x\}, \{x, y\}\} \in P(P(P(x)))$

INSIEME DELLE RELAZIONI DI ORDINE STRETTO

Sia $\omega \neq \emptyset$, definisco l'insieme di tutte le relazioni di ordine stretto:

$$OS(\omega) = \{ p \in P(P(P(\omega))) \mid \text{ANTIRIFL} \wedge \text{ASIMM} \wedge \text{TRANS} \}$$

RELAZIONE TRA OL(ω) E OS(ω)

E' possibile definire un'applicazione biettiva tra i due insiemi. → E' O' CI PERMETTE DI STUDIARE UN SOLO TIPO DI RELAZIONE E TROVARE LE PROPRIETÀ ANCHE NELL'ALTRO

Sia $p \in OL(\omega)$, definisco:

$$p^*: (\forall x, y \in \omega)(x p^* y : \leftrightarrow (x p y \wedge x \neq y))$$

Sia $p \in OS(\omega)$, definisco:

$$p': (\forall x, y \in \omega)(x p' y : \leftrightarrow (x p y \vee x = y))$$

Si puo' dimostrare che l'applicazione f :

$$f: p \in OL(\omega) \mapsto p^* \in OS(\omega) \text{ è biettiva.}$$

La sua inversa sarà:

$$f^{-1}: p \in OS(\omega) \mapsto p' \in OL(\omega)$$

LA DEMOSTRAZIONE SI FA FACENDO VEDERE CHE SE p È DI ORDINE LARGO, ALLORA p^* È DI ORDINE STRETTO, E IDEVA VALE LA ANTIRIFLESSIVITÀ E LA TRANSITIVITÀ, VICEVERSA CON f^{-1}

ESEMPI DI RELAZIONI D'ORDINE:

- \leq in $\mathbb{R}, \mathbb{Z}, \mathbb{N} \dots$
- \subseteq in $P(S)$ con S insieme
- La divisibilità in \mathbb{N}

$\hookrightarrow m | m \leftrightarrow (\exists k \in \mathbb{N})(m = mk) \rightarrow$ M DIVIDE m SE
ESISTE UN K IN N TALE
CHE m · k E' PROPRIO m

PERCHE' LA DIVISIBILITA' E'
UNA RELAZIONE D'ORDINE?

\hookrightarrow 1) m divide se stesso

2) Se $m | m$ e $p | m$ allora: $p | m$:

$$hm = mk \wedge m = h \cdot p \rightarrow m = h \cdot k \cdot p \rightarrow \text{TRANSITIVITA'}$$

3) Se $m | m$ e $m | m$ allora $m = m$:

$$m = mk \wedge m = m \cdot h \rightarrow m = m \cdot h \cdot k \rightarrow \text{ASIMMETRIA}$$

\downarrow

VALE L'ASIMMETRIA a) Se $m = 0$ allora anche $m = 0$ perché $m = m \cdot h$

b) Se $m \neq 0$, visto che in \mathbb{N} tutti gli elementi sono cancellabili, m è cancellabile.
Di conseguenza $m = m \cdot hk \rightarrow h \cdot k = 1$.
In \mathbb{N} , l'unico elemento invertibile è solo 1.
Quindi $h = k = 1$, quindi $m = m$.

Quindi la divisibilità in \mathbb{N} è una relazione di ordine largo

Se invece definisco la divisibilità in \mathbb{Z} , cioè:

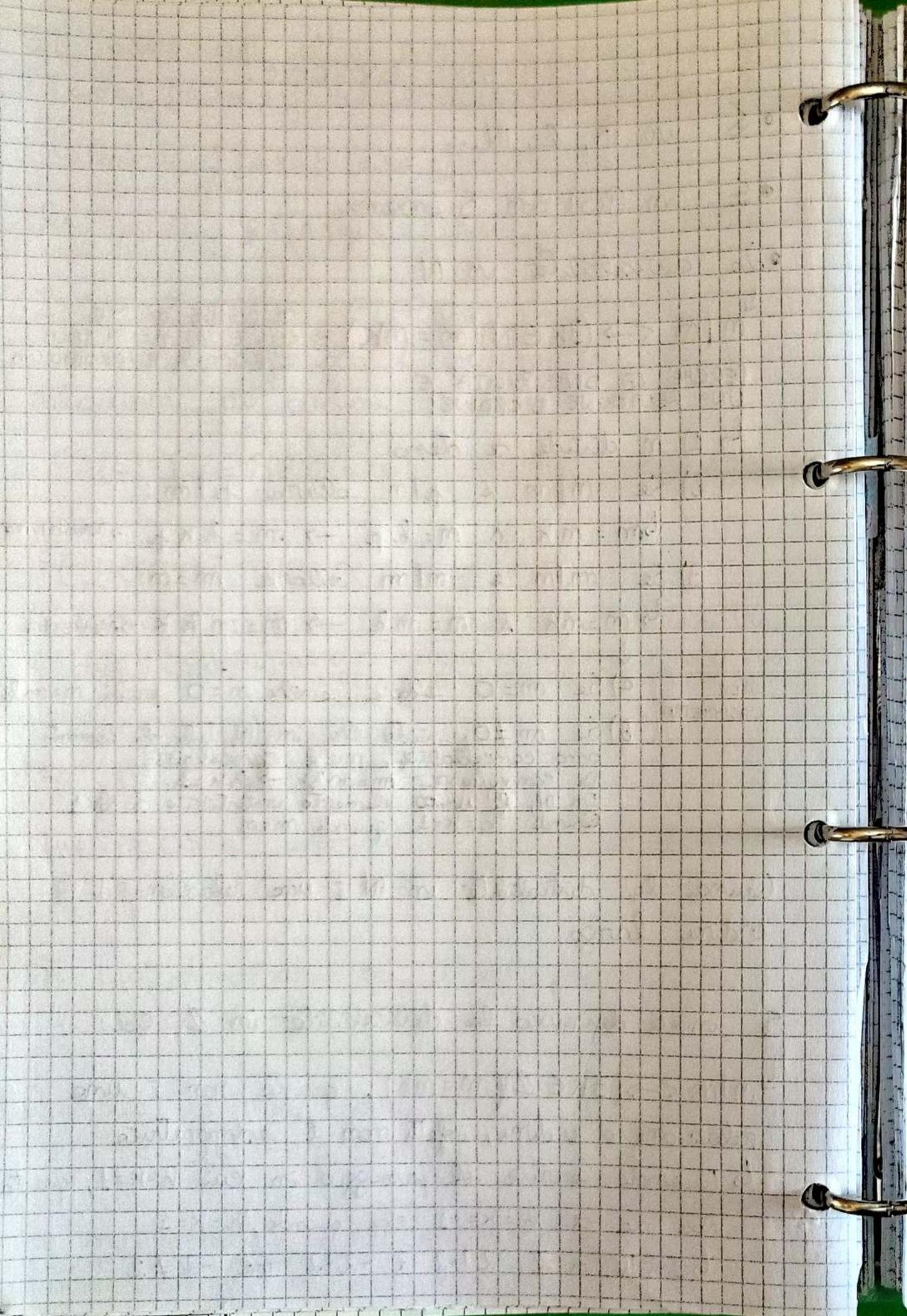
$\hookrightarrow m | m \leftrightarrow (\exists k \in \mathbb{Z})(m = mk)$, questa non è una relazione d'ordine, infatti non è antisimmetrica

\hookrightarrow Quando arrivo al passaggio in cui $h \cdot k = 1$, questo

UNO
DEVE ESSERE
L'INVERSO
DELL'ALTRO

dalle sic se $h = k = -1$ che quando $h = k = 1$

\hookrightarrow Infatti, in \mathbb{Z} , $2 | -2$ e $-2 | 2$ ma $-2 \neq 2$



INSIEMI ORDINATI

Sia $S \neq \emptyset$ e $p = (S \times S, g)$. Sia p una relazione d'ordine su S .

La coppia (S, p) si dice insieme ordinato
RELAZIONE D'ORDINE

↪ SI DICEVA ORDINATO
QUANDO ORDINO
GLI ELEMENTI CON
UNA RELAZIONE
D'ORDINE

RELAZIONE D'ORDINE INDOTTO

Se $t \in P(S) \setminus \{\emptyset\}$, la relazione
 \subseteq_S

$P_t = (t \times t, g \cap (t \times t))$ si dice relazione d'ordine
ESEMPPIO:
indotto da (S, p) su t

PRENDO L'ORDINE DI N E
NE LO RITROVO ANCHE IN
UN SUO SOTTOINSIEME

SOTTOINSIEME ORDINATO

(t, P_t) lo chiamo sottoinsieme ordinato di (S, p)

ESEMPPIO:

Se ho (\mathbb{Z}, \leq) , dovrà indicare il sottoinsieme ordinato su \mathbb{N} con:

$(\mathbb{N}, \leq_{|\mathbb{N}}) \rightarrow$ Per brevità scriverò: (\mathbb{N}, \leq)

↪ LA STESSA DI PRIMA
MA RISTRETTA AD \mathbb{N}

CONFRONTABILI IN (S, p)

Due elementi $x, y \in S$ si dicono confrontabili se vale $x \mathrel{p} y \vee y \mathrel{p} x$, per (S, p) insieme ordinato

ESEMPPIO:

- In (\mathbb{N}, \leq) tutti gli elementi sono sempre confrontabili;
- In $(\mathbb{N}/1)$ non tutti gli elementi sono confrontabili perché non ha né che 2/3 né che 3/2

ORDINE TOTALE

Se tutti gli elementi di S sono confrontabili rispetto a p , p si dice ordine totale su S

MINIMO \rightarrow SI HA SOLO SE P(E) (S)

Un elemento $m \in S$ si dice minimo di (S, p)

$\exists: (\forall x \in S)(m p x) \rightarrow \begin{array}{l} m \in X \text{ SONO} \\ \text{NELLO STESSO} \\ \text{INSIEME} \end{array}$ y \rightarrow lo indico con $\min(t)$
 \hookrightarrow IL MINIMO STA PRIMA

MASSIMO \rightarrow SI HA SOLO SE P(E) (S)

Un elemento $m \in S$ si dice massimo di (S, p)

$\exists: (\forall x \in S)(x p m) \rightarrow \begin{array}{l} m \in X \text{ SONO} \\ \text{NELLO STESSO} \\ \text{INSIEME} \end{array}$ y \rightarrow lo indico con $\max(t)$
 \hookrightarrow IL MASSIMO STA DOPPIO

INSIEME BEN ORDINATO

(S, p) si dice ben ordinato se ogni parte

d'intero del \emptyset ha minimo \rightarrow IL MINIMO DELLA PARTE RISPETTO LA RELAZIONE INDUTTA \rightarrow SI $\{x\}$ E' X, CHE E' ANCHE IL MASSIMO
 \hookrightarrow P DEVE ESSERE PER FORZA DI ORDINE
(PAGO, cioè per $x \in S$ vale $x p x$)

UNICITA' DEL MINIMO (O DEL MASSIMO)

Se esiste il minimo, questo è unico

DIM

Siamo m_1, m_2 minimi di (S, p) .

Per definizione vale $m_1 p m_2 \wedge m_2 p m_1$

Essendo p una relazione d'ordine, per assimmetria $m_1 = m_2$. Stesso ragionamento per il massimo

ESEMPI:

- (\mathbb{N}, \leq) è ben ordinato perché ogni parte non vuota ha il minimo \rightarrow Anche tutto \mathbb{N} ce l'ha

• (\mathbb{Z}, \leq) non è insiem ordinato perché l'insieme "tutto \mathbb{Z} " non ha minimo

- Se ho l'insieme $Q = \mathbb{Z} \cup \{-\infty\}$, dove $-\infty$ è un elemento che è sempre più piccolo di tutti gli interi, e $p = (\alpha \times \epsilon, g)$ allora:

$(\forall m, m \in \mathbb{Z})(m \leq m \Leftrightarrow m \leq m)$ e ho anche che $(\forall m \in \mathbb{Z})(-\infty \leq m)$ e, per la riflessività, anche $-\infty \leq -\infty$.
Anche se l'insieme Q ha minimo, c'è la forte di α (cioè \mathbb{Z}) che non ha minimo, di conseguenza $(\mathbb{Z} \cup \{-\infty\}, p)$ non è insiem ordinato

- L'insieme $Q = \mathbb{N} \cup \{-\infty\}$ con $p = (\alpha \times \epsilon, g)$ è con definito così:
 - $(\forall m, m \in \mathbb{N})(m \leq m \Leftrightarrow m \leq m)$
 - $(\forall m \in \mathbb{N})(-\infty \leq m)$
 - $-\infty \leq -\infty$

E' insiem ordinato perché ogni forte di Q ha minimo $\rightarrow \mathbb{N} \cup \{-\infty\}$ È UN INSIEME IMPORTANTE PER I POLINOMI

INSIEME TOTALMENTE ORDINATO

Se (S, p) è insiem ordinato allora (S, p) è anche totalmente ordinato

DIM Supponiamo che (S, p) sia insiem ordinato
Preso $x, y \in S$, $\{x, y\} \subset S \setminus \{\emptyset\}$

Dato che (S, p) è insiem ordinato, per definizione:

$$(\exists m \in S)(m = \min(\{x, y\})). \quad \begin{cases} \text{Se } m = x \text{ allora } x \leq y \\ \text{Se } m = y \text{ allora } y \leq x \end{cases}$$

RELAZIONE DI COPERTURA

Dato l'insieme ordinato (S, \leq)

$$y \text{ COPRE } x \text{ se } x \leq y \wedge (\forall z \in S)(z \leq x \Rightarrow z \leq y)$$

↳ Cioè y sta sotto
dato x e tra x e y
non c'è nient'altro
in mezzo

UNA RELAZIONE
di COPERTURA ROSSO
PERCAMPARE CLARINA
DELL'INSIEME

NON STA IN MEZZO
A x E y

d'unica cosa che manca affinché "COPRE" sia una
relazione di ordine è la transitività:

↳ In (N, \leq)

• 2 COPRE 1

• 3 COPRE 2

• Ma 3 NON COPRE 1 → Transitività

C'E IL
2 IN MEZZO

y si dice immediato successore di x

DIAGRAMMI DI HASSE

Il diagramma di Hasse di (S, \leq) è la coppia

$(S \times S, g)$ con $(x, y) \in g \Leftrightarrow y \text{ COPRE } x$

RAPPRESENTAZIONE DEI DIAGRAMMI DI HASSE

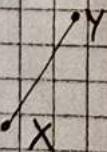
- Tutti gli elementi di S hanno dei puntini
- I puntini sono collegati da linee non orizzontali se e solo se y copre x

ESEMPIO:

Se ho due elementi di S

Tali che y copre x , li →

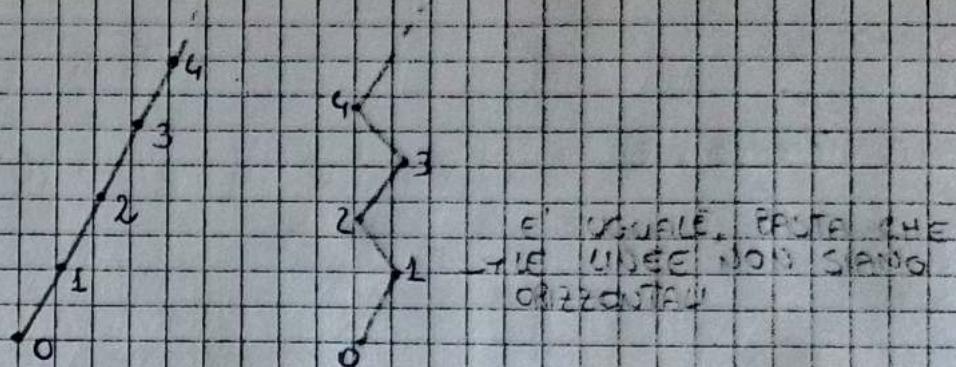
rappresento così:



Scorre se AVESSE
IL < E NON IL >
X NON COPRE X PERCHE
CI STAREBBERE L'ELEMENTO
GESSO X CHE STA IN
MEZZO

ESEMPIO:

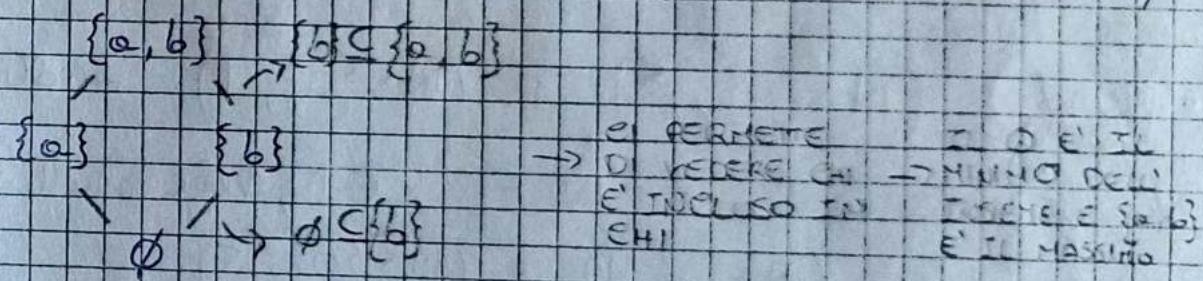
- In N , cerchiamo una rappresentazione del tipo:



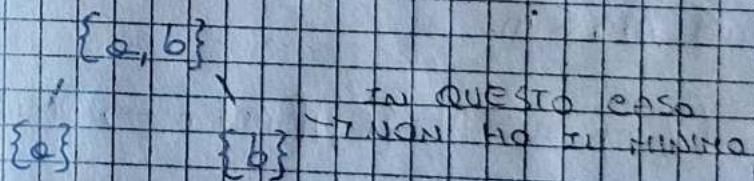
- Prendo $S = \{a, b\}$ e ordino le parti di S con l'inclusione

$$\hookrightarrow (\mathcal{P}(S), \subseteq)$$

Chi è $(\mathcal{P}(S), \subseteq)$? $(\mathcal{P}(S), \subseteq) = (\{\emptyset, \{a\}, \{b\}, \{a, b\}\}, \subseteq)$



- Se ho $S = \{a, b\}$ e $(\mathcal{P}(S) \setminus \{\emptyset\}, \subseteq)$ è così:



NOTIAMO CHE...

- Se S è totalmente ordinato e c'è la relazione di copertura (S è finito), il diagramma di Hasse è una linea.

Un esempio, \mathbb{N} è totalmente ordinato ma non possiamo rappresentarlo come linea perché non c'è la relazione

CRESCENTE

Siamo (S, p) e (\bar{S}, \bar{p}) insiemmi ordinati e la funzione:

$$f: S \rightarrow \bar{S}$$

f si dice crescente se: $(\forall x, y \in S)(x p y \rightarrow f(x) \bar{p} f(y))$

x, y potrebbe essere falsa,
ma non diventa vera
l'interpretazione → perdo informazioni

SEMbra la definizione di
crescenza ma non lo è

ISOMORFISMO TRA STRUTTURE ORDINATE

Siamo (S, p) e (\bar{S}, \bar{p}) insiemmi ordinati e la funzione:

$$f: S \rightarrow \bar{S}$$

f si dice isomorfismo se:

deve essere biettiva

$$(\forall x, y \in S)(x p y \leftrightarrow f(x) \bar{p} f(y))$$

e c'è il
se e solo

ESEMPIO:

- Premendo $(\mathbb{N} \setminus \{0\}, \leq)$ e $(\mathbb{N} \setminus \{0\}, |)$. Insomma, prendo la funzione $f: x \in \mathbb{N} \rightarrow x \in \mathbb{N}$, che è biiettiva e crescente tra $(\mathbb{N} \setminus \{0\}, |)$ e $(\mathbb{N} \setminus \{0\}, \leq)$.

Premendo $m, n \in \mathbb{N} \setminus \{0\}: m|n$

Siamo in \mathbb{N} , quindi $m \leq n$.

↳ Vual dire che: $(\forall m, n \in \mathbb{N} \setminus \{0\})(m|n \rightarrow f(m) \leq f(n))$

Notiamo che f è un isomorfismo solo se
abbiamo $x \neq x$. Infatti, se x è zero che
 $x \neq 1$ allora $1 \leq 1$, il contrario non è sempre
vero.

↳ Anche se $3 \leq 4$, non è vero che $3|4$

INSIEMI ISOMORFI E DIAGRAMMI DI HASSE

Siamo (S, ρ) e $(\bar{S}, \bar{\rho})$ insiemi ordinati finiti.

- (S, ρ) e $(\bar{S}, \bar{\rho})$ sono isomorfi se e solo se puoi rappresentare con lo stesso diagramma di Hasse. \hookrightarrow SE SONO ISOMORFI, LA RELAZIONE DI COPERTURA È LA STESSA

DIM

\rightarrow Sia f un isomorfismo tra $(S, \rho) \hookrightarrow (\bar{S}, \bar{\rho})$

\hookrightarrow Voglio dimostrare che $(\forall x, y \in S)(y \text{ copre } x \Leftrightarrow f(y) \text{ copre } f(x))$

Presi due $x, y \in S$, considereremo un altro z :

$\exists z \in S (x \rho z \wedge z \rho y) \rightarrow z \text{ sta in mezzo}$

\hookrightarrow Queste cose c'è solo se è solo se

$\exists z \in S (f(x) \bar{\rho} z \wedge z \bar{\rho} f(y)) \rightarrow$ Dico che f è un
ISOMORFISMO

\hookrightarrow Ma z è minimo $f(z)$, quindi

$\exists z \in S (x \rho z \wedge z \rho y) \Leftrightarrow \exists f(z) \in S (f(x) \bar{\rho} f(z) \wedge f(z) \bar{\rho} f(y))$

Ho quindi fatto vedere che c'è uno z in mezzo a x e solo a x c'è un $f(z)$ in mezzo

\hookrightarrow Ho così dimostrato che $(\forall x, y \in S)(y \text{ copre } x \Leftrightarrow f(y) \text{ copre } f(x))$
Meglio la relazione di copertura, cioè
usando la Tautologia $(p \Leftrightarrow q) \Leftrightarrow (\neg p \Leftrightarrow \neg q)$

\leftarrow PER LA DEMOSTRAZIONE DELL'ALTRO VERSO SERVE
LA DEFINIZIONE DI "ESSERE UN INSIENE FINITO", QUINDI
LA FARANNO PIÙ AVANTI

\hookrightarrow SI TROVA DOPO LA CORREZIONE ESERCIZI 23/11/2021

Correzione esercizi 16/11/2021 (LEZIONE 22)

- Prendo $a = \{x, y\}$ con $x \neq y$. che tutti gli elementi sono confrontabili

↓
 $P(a)$ è totalmente ordinato rispetto a \subseteq .

No, $(P(a), \subseteq)$ non è totalmente ordinato perché abbiamo che $\{x\} \subseteq \{y\}$ e che $\{y\} \subseteq \{x\}$

Basta che ci siano almeno due elementi
in $P(a)$, che le parti non sono totalmente ordinate.

↓
Infatti, prego $b = \{x\}$

$(P(b), \subseteq)$ sono totalmente ordinate. Infatti il diagramma di Hasse è:

↓
Solo x in b ha un solo elemento (o zero) allora

è totalmente ordinato \rightarrow le parti di \emptyset

MASSINALE

Dato l'insieme ordinato (S, ρ) e un elemento $m \in S$, m si dice massimale di S se:

$$(\forall x \in S) ((x \rho m \vee m \rho x) \rightarrow x \rho m)$$

ESSERE CONFRONTABILE

SE PER OGNI ELEMENTO DI S CONFRONTABILE CON m , m STA SOPRA, ALLORA m E' UN MASSINALE

MINIMALE

Dato l'insieme ordinato (S, ρ) e un elemento $m \in S$, m si dice minimale di S se:

$$(\forall x \in S) ((x \rho m \vee m \rho x) \rightarrow m \rho x)$$

ESSERE CONFRONTABILE

MAGGIORANTE DI t IN S

Dato l'insieme ordinato (S, ρ) , una parte t di S , cioè $t \subseteq S$, e un elemento $m \in S$, m si dice maggiorante di t in S se:

$$(\forall x \in t)(x \rho m)$$

LA DIFFERENZA E' CHE
IL MASSIMO E' CHE
X E' INVECE DI S → X STA IN
UN SOTTO-INSIEME E
M STA FUORI

SONO GLI ELEMENTI DI S CHE SONO PIÙ
GRANDI DI TUTTI GLI ELEMENTI DI t

MINORANTE DI t IN S

Dato l'insieme ordinato (S, ρ) , una parte $t \subseteq S$ e un elemento $m \in S$, m si dice minorante di t in S se:

$$(\forall x \in t)(m \rho x)$$

RISPETTO AL MINIMALE, NON
MI INTERESSA LA CONFRONTABILITÀ

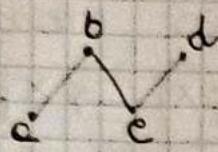
INSIENE DI TUTTI I MAGGIORANTI / MINORANTI

L'insieme dei maggioranti di t in S lo indico con $\text{MAGGIOR}_{(S, \rho)}(t)$

L'insieme dei minoranti di t in S lo indico con $\text{MINOR}_{(S, \rho)}(t)$

ESEMPIO:

Consideriamo l'insieme ordinato (S, p) con questo diagramma di Hasse:



Consideriamo $T = \{a, c\}$

- t non ha minimo
- t non ha massimo
- $\text{MAGGIOR}_{(S,p)}(t) = \{b\}$ PERCHÉ È CONFRONTABILE CON a, c
- $\text{MINOR}_{(S,p)}(t) = \text{Non esiste} \rightarrow \text{Il MINOR}_{(S,p)}(\{b\}) = \{a, c\}$

Consideriamo (S, p) , quindi con $S = \{a, b, c, d\}$,
 $p = (S \times S, g)$ e $g = \{(a, b), (c, b), (c, d)\}$

- b è massimale perché:
 - è confrontabile con a e c
 - è confrontabile con d , quindi l'implicazione è vera perché la prima parte è falsa

↳ p potrebbe anche essere riflessiva e contenere le coppie $(a, a), (b, b), (c, c), (d, d)$

«Ere massimale è come dire "è massimo rispetto agli elementi confrontabili"»

↳ Anche d è un massimale

- Stesso ragionamento anche per i minimali
 - a e c sono minimali di S

Correzione esercizi 17/11/2021 PLESSIONE 23)

2) $S = \{x \in \wp(\mathbb{N}) \mid x \text{ è SINGETON}\} \quad (S, \subseteq)$

In questo insieme nessuna coppia di elementi è confrontabile

↪ se $x \neq y$ con $x, y \in S$, non c'è né zero che $x \subseteq y$ né che $y \subseteq x \rightarrow$ IL DIAGRAMMA DI HASSE È TUTTO SCANNESO

Visto che nessuno è confrontabile allora sono tutti sia massimale che minimale \rightarrow

L'ANTECEDENTE
DEL \rightarrow È
FALSO QUINDI
LA FRASE È VERA
NELLA DEFINIZIO
DI MASSIMALE
E MINIMALE

c) $(\mathbb{Z}, |)$

Non è una relazione d'ordine perché non è simmetrica

↪ Non possiamo cercare massimo e minimo né massimali e minimali perché non sono definiti

Possiamo, però, trovare un numero che è divisibile da tutti gli altri numeri

↪ $x|y \Leftrightarrow (\exists k \in \mathbb{Z})(x \cdot k = y) \xrightarrow{\Delta(x,y)}$ cioè 0, che sta sempre a destra, cioè è un "massimo"

$$\min = -1$$

$$\max = 0$$

↪ invece, è il "minimo"

Dato che c'è il minimo, questo coincide con l'elemento minimale \rightarrow TUTTI GLI ELEMENTI MINIMALI COINCIDONO CON IL MINIMO

Gli elementi massimali non ci sono perché non c'è un numero che è multiplo di tutti gli altri numeri, oltre 0

- $(\mathbb{N} \setminus \{1\}, |)$

In questo caso i minimi sono quei numeri i cui divisori sono soltanto loro stessi

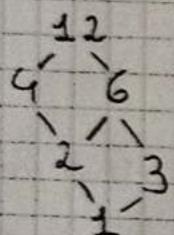
$$\hookrightarrow m \text{ è MINIMALE} \Leftrightarrow (\forall x \in \mathbb{N} \setminus \{1\}) (x \in m \text{ CONFRONT} \rightarrow m|x)$$

Ad esempio i minimi sono i numeri primi

- Prendo S uguale ai divisori di 12 in \mathbb{N}

$$S = \{1, 2, 3, 4, 6, 12\} \text{ con } (S, |)$$

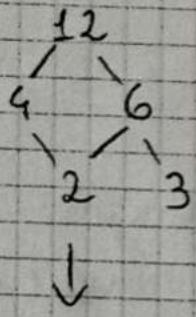
Se facciamo il diagramma di Hasse vediamo:



- 12 è il massimo
- 1 è il minimo
- massimale e minimale sono il minimo e il massimo

- Consideriamo $(S \setminus \{1\}, |)$

$S = \{2, 3, 4, 6, 12\}$. Il diagramma di Hasse sarà:



- Qui non c'è il minimo
- Il massimo è 12
- Gli elementi minimi sono 2 e 3
 - ↳ DUE ELEMENTI CHE SONO NON HANNO NULLA

Tutto \mathbb{N} è un grafico del genere con solo tutti i numeri primi

\hookrightarrow Possono esserci infiniti elementi minimi se non c'è il minimo

INSIEME LIMITATO SUPERIORMENTE

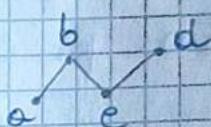
Dato $t \subseteq S$, e (S, p) insieme ordinato,
 t si dice limitato superiormente in S se:
 $\text{MAGGIOR}_{(S,p)}(t) \neq \emptyset$

INSIEME LIMITATO INFERIORMENTE

Dato $t \subseteq S$ e (S, p) insieme ordinato,
 t si dice limitato inferiormente in S se:
 $\text{MINOR}_{(S,p)}(t) \neq \emptyset$

ESEMPIO:

Considerando (S, p) e $t = \{a, e\} \subseteq S$ con diagramma
di Hasse del tipo:



- Possiamo dire che t è limitato superiormente perché $\text{MAGGIOR}_{(S,p)}(t) = \{b\}$

NON È NECESSARIO CHE SI ABbia UN INSIEME INFINTO PER ESSERE ILLIMITATI

- Se invece abbiamo $N = \{d\}$, N è illimitato superiormente perché non c'è massimo al di sopra di d , anche se S è un insieme finito

INSIEME NATURALMENTE ORDINATO

L'insieme ordinato (S, p) si dice naturalmente ordinato se è ben ordinato e ogni parte non vuota superiormente limitata ha massimo. \rightarrow essendo ben ordinato, vuol dire che ci troviamo su una relazione d'ordine LARGO

In questo caso si riferisce all'esempio di PRIMA, VALE XPX, QUINDI DALL'PARTE E' UNITATA ANCHE I SINGOLI ELEMENTI HANNO IL MASSIMO

ESISTENZA DI N

Notiamo che di ciò che abbiamo studiato, non c'è nulla che giustifichi l'esistenza di $N \rightarrow$ bisogna INTRODURRE L'ASSIOMA DELL'INFINITO MA LO FAREMO PIÙ AVANTI DOPO TEOREMA FONDAMENTALE ARITMETICA

do considero come enigma:
Esiste un insieme naturalmente ordinato e non superiormente limitato. Questo insieme lo chiamo N \rightarrow EQUIVALENTE ALL'ASSIOMA DELL'INFINITO

INDUZIONE

Ora che abbiamo degli insiemi infiniti, vogliamo dimostrare una certa proprietà per tutti i numeri di questo insieme.

↳ L'induzione mi permette di dimostrare una certa proprietà per tutti i numeri naturali o, comunque, da un certo numero in poi.

CONTROESEMPIO MINIMO

Se voglio far vedere una proprietà dei numeri naturali posso procedere ragionando per assurdo che quella cosa non sia vero.

↳ Se non è vero che quella cosa non vale per tutti i numeri naturali, c'è qualcuno per cui non vale.

↓
Prendo il minimo dell'insieme per cui questa proprietà non vale \rightarrow Posso farlo perché \mathbb{N} è ben ordinato.

↳ Da qui entro un assurdo.

ESEMPIO:

- Voglio dimostrare che non tutti i numeri sono pari.
DIM

Per Assurdo, considero che Tutti i numeri siano pari.

Prendo il più piccolo dei numeri pari.

Se prendo l' $n+1$ elemento, sarà un numero dispari, ma ciò è un assurdo. ↴

↓
CONTROESEMPIO MINIMO

$\text{IN}_{\min X}$

Considero una parte di \mathbb{N} non vuota
↳ Sia $x \in P(\mathbb{N}) \setminus \{\emptyset\}$, definisco $\text{IN}_{\min X}$:

$$\text{IN}_{\min X} = \{m \in \mathbb{N} \mid \min X \leq m\} \quad \begin{array}{l} \text{TUTTI GLI } m \text{ APPARTIENENTI} \\ \text{AD } X \text{ TALI CHE TUTTI} \\ \text{SONO PIÙ GRANDI DEL} \\ \text{MINIMO DELLA PARTE } X \end{array}$$

PRINCIPIO DI INDUZIONE DI I FORMA

$$(\forall x \in P(\mathbb{N}) \setminus \{\emptyset\}) ((\forall m \in \mathbb{N})(m \in x \rightarrow m+1 \in x)) \rightarrow x = \text{IN}_{\min X}$$

↳ Cioè, per ogni x , sottoinsieme di \mathbb{N} non vuoto, questo parte di \mathbb{N} è proprio quella parte che contiene il minimo di x .

ESEMPPIO:

Se il minimo di x è 3, la parte x coincide proprio con $\{3, 4, 5, 6, 7, 8, \dots\}$

L'ipotesi su x è che, per ogni m naturale,
 $m \in x$ allora anche $m+1 \in x \rightarrow$ SE m STA IN X ,
ANCHE IL SUCCESSIVO STA IN X

ESEMPPIO:

Se il minimo di x è 10, allora in x ci sta anche 11. Se ci sta 11 ci sta 12. Se ci sta 12 ci sta 13 ecc...

Nel principio di induzione di prima forma ci si basa sul fatto che uno prende il minimo, poi il successivo ecc...

DIM PRINCIPIO DI INDUZIONE DI PRIMA FORMA

Sic $m := \min X$

L'INDIENE CHE
VI UN MINIMO IN X

Per Assurdo, sic $x \neq \min X$

TUTTI I NUMERI
DI X SONO
MAGGIORI DEL
MINIMO DI X

Certamente, $m \in N_{\min X}$, quindi $X \subset N_{\min X}$

Visto che $x \neq \min X$, definisco $Y := N_{\min X} \setminus X$

$\hookrightarrow Y \neq \emptyset$ per ipotesi dell'assurdo

Visto che Y non è vuoto e visto che N è ben ordinato, possiamo prendere il minimo di Y

$\hookrightarrow m := \min Y$

Visto che i numeri di Y sono tutti i numeri che non stanno in X , certamente $m \neq m$.

Inoltre, $m < m$ perché m l'ha preso da Y che sono tutti i numeri naturali più grandi di m meno l'insieme $X \rightarrow$ Sono comunque numeri più grandi di m

Da qui segue che $m \leq m-1$, e certamente $m-1 < m$

$\hookrightarrow m \leq m-1 < m$

Cio' significa che $m-1 \in X$ perché $m-1$ è maggiore del minimo di X ma è minore strettamente del minimo dei numeri che non appartengono ad X .

Se $m-1 \in X$, allora anche $(m-1)+1 \in X$, cioè $m \in X$, per ipotesi del principio di induzione

Ma ciò è un assurdo \hookrightarrow

\downarrow
E' UNA DEMOSTRAZIONE
PER CONTROESEMPIO MINIMO \rightarrow

* PRENDO IL PIÙ PICCOLO DI
QUELLI CHE NON C'E'

* PRENDO QUELLO DI PRIMA CHE C'E'

* PER I PARSI PRENDO QUELLO DI
COSÌ MA QUELLO DOPO DI QUELLO
DI PRIMA E' UN STESSO \hookrightarrow

CHI E' $m-1$?

Nella dimostrazione del principio di induzione di prima forma abbiamo detto che, preso $Y = \min_{x \in X} Y$, $Y \neq \emptyset$ quindi possiamo prendere il min Y .
Abbiamo chiamato $m = \min Y$ e abbiamo visto che se $\underbrace{m-1}_{\in X} \rightarrow m \in X \subseteq Y$

$m-1$ è il massimo degli elementi minori di m
 \hookrightarrow è il massimo dei numeri naturali che sono strettamente minori di m

$m-1$ è il massimo perché \mathbb{N} è naturalmente ordinata
 \hookrightarrow Se prendo $S = \{m \in \mathbb{N} \mid m < m\}$, questa parte di \mathbb{N} è sicuramente non vuota perché, visto che $\min Y \neq \min X$ allora in S c'è almeno il $\min X \rightarrow S \neq \emptyset$

$\hookrightarrow S$ è superiormente limitata perché esiste M che è il maggiorente di S

Quindi, esiste il $\max S$ che chiamo $m-1$.

PRINCIPIO DI INDUZIONE DI II FORMA

$$(\forall x \in P(N) \setminus \{\emptyset\}) ((\forall m \in N) ((\forall k \in N) (\min x \leq k < m \rightarrow k \in x)) \rightarrow \exists x \in x \rightarrow x = N_{\min x})$$

QUESTA È LA PARTE
CHE CAMBIA RISPETTO
ALLA PRIMA FORMA

Con il principio di induzione di seconda forma

non andiamo di successo in successo ma

consideriamo tutti i numeri che stanno prima di m

↳ Se tutti i precedenti di m stanno in x ,
anche m sta in x

Il principio di induzione di seconda forma è più forte del primo perché ci permette di prendere tutti gli elementi che stanno prima

↳ A volte potremmo non avere un buon ordinamento con $m, m+1$ ecc...

AD ESEMPIO
NELLA DIM
DEL TEOREMA
FONDAMENTALE
DELL'ARITMETICA

Quella parte del principio di induzione di prima forma: $m \in x$, viene riempierata con: $(\forall k \in N) (\min x \leq k < m \rightarrow k \in x)$

TUTTI QUELLI
PRIMA DI m E
MAGGIORI DEL
MINIMO STANNO IN x

DIM PRINCIPIO DI INDUZIONE DI SECONDA FORMA

Sia $m := \min x$

Per Assurdo, sia $x \neq N_{\min x}$, quindi $x \subset N_{\min x}$.

Possò definire $y := N_{\min x} \setminus x$, quindi $y \neq \emptyset$ per ipotesi dell'assurdo. Possò quindi avere un minimo di y per le stesse motivazioni della dimostrazione del principio di induzione di prima forma.

$m := \min y$

Per poter continuare la dimostrazione, dobbiamo vedere che $(\forall k \in \mathbb{N})(m \leq k < m \rightarrow k \notin X)$ è vero così da ottenere che l'implicazione è vera e che $m \in X$.

↪ Sia $k \in \mathbb{N}$ tale che $m \leq k < m$

Così, prendo un certo k che sta tra il minimo di X e il massimo di Y .

↪ Ma $k \notin X$ perché, per lo stesso discorso di prima, k è maggiore di m ed è più piccolo dell'elemento più piccolo di tutti gli elementi che non stanno in X . Di conseguenza,

$$(\forall k \in \mathbb{N})(m \leq k < m \rightarrow k \notin X)$$

Bmo che usare l'ipotesi del Teorema dato che è verificata

↪ Segue che $m \in X$

I PRIMI NON DEVONO ESSERE INVERTIBILI,
INFATTI IN \mathbb{R} NON CI SONO NUMERI PRIMI
PERCHE' TUTTO E' DIVISIBILE PER TUTTO

NUMERO PRIMO

$p \in \mathbb{Z}$ si dice primo se $p \neq 1 \wedge p \neq -1$

\hookrightarrow = PRIMI SEMPRE \hookleftarrow

$(\forall a, b \in \mathbb{Z})(p | ab \rightarrow (p | a \vee p | b))$

DEFINIZIONE EQUIVALENTE
AL FATTO DI AVERE
SOLI DIVISORI "NON
BANALI"

ESEMPIO:

• 216? Allora è vero che 213 oppure 212

DECOMPOSIZIONE DI p

La definizione di primo, non ha nulla a che vedere con la decomposizione di p stesso.

↪ Vogliamo dimostrare che p ha solo divisori banali.

LEMMA 1

Se $p \in \mathbb{Z}$ è un numero primo, allora ha come divisori soltanto i divisori banali

$\hookrightarrow \underbrace{\{m \in \mathbb{Z} \mid m \mid p\}}_{\text{INSIEME DEI DIVISORI DI } p} = \underbrace{\{-p, -1, 1, p\}}_{\text{INSIEME DEI DIVISORI OVV. (O DIVISORI BANALI)}}$

DIM

Prendo un qualunque divisore di p che chiamo m

\hookrightarrow Sia $m \in \mathbb{Z}$ tale che $m \mid p$, cioè $(\exists k \in \mathbb{Z})(mk = p)$

Visto che p è primo ed è evidente che p divide $m \cdot k$, allora per la definizione di primo, p divide o m o k

\hookrightarrow Per definizione di primo, $p \mid m \vee p \mid k$ DEVE SUCCEDERE UNA DELLE DUE COSE

1. Suppongo che $p \mid m$, cioè che $(\exists h \in \mathbb{Z})(p \cdot h = m)$

Sostituisco " $p \cdot h = m$ " in " $mk = p$ " e entro che.

$p \cdot h \cdot k = p \rightarrow$ Di conseguenza $h \cdot k = 1$

Visto che ci troviamo in \mathbb{Z} , allora vale che:

$$h = k = 1 \vee h = k = -1$$

\hookrightarrow Di conseguenza $m = p \vee m = -p$

2. Suppongo che $p \mid k$, cioè che $(\exists l \in \mathbb{Z})(p \cdot l = k)$

Sostituisco " $p \cdot l = k$ " in " $mk = p$ ", quindi entro che

$p \cdot m \cdot l = p \rightarrow$ Di conseguenza $m \cdot l = 1$

Di conseguenza $m = l = 1 \vee m = l = -1$

\hookrightarrow Segue che $m = 1 \vee m = -1$

Allora abbiamo quindi dimostrato che i divisori di un numero primo sono ± 1 o $\pm p$

LEMMA 2

L'INSIEME DI TUTTI I NUMERI NATURALI
TAI CHE M DIVIDA $m \cdot b$

Siamo $m, b \in \mathbb{N} \setminus \{0\}$, sia $X = \{m \in \mathbb{N} \setminus \{0\} \mid m \mid m \cdot b\}$,
sia $S = \min X$.

↪ S divide tutti gli elementi di X

↪ Cioè, $(\forall y \in X)(S \mid y)$

$\rightarrow X$ È SEMPRE DIVERSO
DAL VUOTO PERCHÉ
 $m \cdot b$ PUÒ ANCHE
ESSERE PROPRIO m

IL MINIMO
DELL'INSIEME X
DIVIDE TUTTI GLI ELEMENTI

DIM → E' UNA DIMOSTRAZIONE
PER CONTROESEMPIO MINIMO

Per Assurdo, dico che S non divide tutti gli elementi di $X \rightarrow$ l'insieme degli elementi di X che non sono divisibili da S non è vuoto.

↪ Cioè, per assurdo, non è vuoto l'insieme degli $y \in X$ tali che $S \nmid y$

↓ \nwarrow NON DIVIDE

Visto che \mathbb{N} è ben ordinato, posso prendere il minimo dell'insieme degli $y \in X$ tali che $S \nmid y$, e chiamarlo questo elemento z .

Visto che ci trattiamo ancora nell'insieme X , per definizione di X ho che $m \mid z \cdot b$ e $m \nmid S \cdot b$.

↪ Cioè significa che vale che $mh = zb$ e $mk \neq Sb$, quindi $(z - S)b = zb - Sb = mh - mk = m(h - k)$

↓

Di conseguenza vale che $m \mid (z - S) \cdot b$

↪ Di conseguenza anche $(z - S) \in X$ perché verifica la condizione di appartenenza a X

Visto che z è il minimo dell'insieme degli $y \in X$ tali che $S \nmid y$ e visto che $S \neq 0$ dato che $S \in X$ e X sono numeri naturali diversi de 0, allora $[z - S < z]$ perché sestraissimo e z una quantità non nulla.

Visto che $z-s < z$, cioè è più piccolo del minimo per cui vale che $s \leq y$, allora per $z-s$ vale che non è diverso da s

↪ Quindi $S \mid (z-s)$, cioè $(\exists l \in \mathbb{N})(Sl = z-s)$

Visto che vale che $Sl = z-s$, allora posso ridurlo come $S(l+1) = z$. Ma ciò significa che $S \mid z$, che è un assurdo ↴

TEOREMA FONDAMENTALE DELL'ARITMETICA

a. Sia $m \in \mathbb{Z} \setminus \{-1, 0, 1\}$.

Allora, $\exists p_1, p_2, \dots, p_r$ numeri primi di \mathbb{Z} tali che $m = p_1 \cdot p_2 \cdots p_r$

↪ Cioè, m è un numero primo o prodotto di numeri primi

b. Inoltre, se $m = q_1 \cdot q_2 \cdots q_s$ allora $r = s$ ed esiste una funzione biettiva $f: \{1, \dots, r\} \rightarrow \{1, \dots, r\}$ tale che $(\forall i \in \{1, \dots, r\})(p_i = \pm q_{f(i)})$

E' QUASI LA STESSA
DECOMPOSIZIONE IL NUMERO DI
FACTORI E' LO STESSO

↪ ESEMPIO: $6 = 2 \cdot 3$ MA
ANCHE $6 = 3 \cdot 2$

DIM → USEREMO ENTRAMBI I PRINCIPI DI INDUZIONE → PER APPLICARLI ABBIAMO BISOGNO DI UN INSIEME NATURALMENTE ORDINATO

c. Dato che il principio di induzione è riferito a \mathbb{N} e \mathbb{Z} non è ben ordinato, dobbiamo ridurci ad \mathbb{N}

I PROBLEMI
CHE
M'HA
MESSO → Sia $m \in \mathbb{N}$

↪ Voglio procedere per induzione di seconda forma

HO BISOGNO
DELLA BASE
DI INDUZIONE

↪ Voglio dimostrare che tutti i numeri naturali

PRINCIPIO
DI INDUZIONE
SU \mathbb{N} Maggiori o uguali a due si possono scrivere come prodotto di primi → Il passo base è che 2 verifica la tesi

Voglio dimostrare che 2 è primo. DEVO FAR VEDERE CHE 2 È PRIMO

↪ Scrivo $2 \mid ab$ e suppongo che $2 \nmid a$

Visto che $2 \mid ab$, allora vale che $2k = ab$ per la definizione di divisibilità.

Dato che $2 \nmid a$ allora a è un numero dispari, quindi $a = 2h + 1$.

Possò sostituire " $2h+1$ " in " $2k = ab$ ", quindi entra che $2k = 2hb + b$

↪ Di conseguenza $b = 2(k - hb)$, quindi $2 \mid b$. Cioè significa che 2 è primo per la definizione di numero primo.

Possò usare il principio di induzione di seconde forme

1. Suppongo vere le tesi per tutti gli m tali che:
SUPPOGNO CHE TUTTI GLI m SIANO DIVISIBILI PER PRIMI O SIANO PRODOTTO DI PRIMI

$2 \leq m < m \rightarrow$ SE LA PROPRIETÀ VALE PER GLI m (ogni precedente di m) ALLORA VALE ANCHE PER $m \rightarrow$ CA' CHE APPLICO IL PRINCIPIO DI INDUZIONE

↪ Se m è primo, la tesi è ovvia perché è proprio x stesso. \rightarrow ^{perché m è prodotto di primi} _{è l'unico fattore}

2. Suppongo m non primo (Ricordo che $m \in \mathbb{N}$)

↪ Se m non è primo allora posso trovare una decomposizione non banale \rightarrow ^{perché} DIMOSTRARLO

• Dato che m non è primo allora:

$(\exists h, k \in \mathbb{N})(m \mid h \cdot k \wedge (m \nmid h \wedge m \nmid k)) \rightarrow$ NEGAZIONE DELLA DEFINIZIONE DI PRIMO

↪ Dato che m non può comportarsi come primo, dovrà avere altri divisori oltre 1 e m (QUELLI BANALI)

Per Assurdo dico che l'insieme: $\{m \in \mathbb{N} : m \mid m\} = \{1, m\}$ \hookrightarrow SI SONO SICURI? DIMOSTRIANNOLO

Definisco l'insieme X :

$X := \{m \in \mathbb{N} \setminus \{0\} : m \mid m\}$ è un insieme $S = \min X$

Noto che: $h, m \in X \rightarrow$ PERCHÉ?

- $h \in X$ perché per ipotesi $m \nmid h \cdot k$, mentre $m \in X$
perché $m \mid m \cdot k$

Dunque, per il lemma 2 abbiamo che:

$$S \mid h \wedge S \mid m \rightarrow \begin{array}{l} S \text{ È UN DIVISORE} \\ \text{DI } m \end{array}$$

Dato che abbiamo supposto che $\{m \in \mathbb{N} : m \mid m\} = \{1, m\}$,

abbiamo che $S=1 \vee S=m$

- ↪ Se $S=1$, allora, dato che $S \in X$, $m \mid 1 \cdot k$, cioè
 $\{m \mid k \rightarrow$ Queste cose non puo' essere dalla definizione
di non primo
- ↪ Se $S=m$, allora dal fatto che $S \mid h$ si ha
 $\{m \mid h \rightarrow$ Anche questo è falso dalla definizione

Quindi non è vero che ci sono soltanto divisori
bassi $\rightarrow S$ può essere anche altre cose oltre 1 e m

↪ Ciò significa che:

$$(\exists a, b \in \mathbb{N} \setminus \{0, 1\})(m = a \cdot b) \rightarrow \begin{array}{l} a \text{ NON PUO' ESSERE NE 1 NE } m \\ \text{PERCHE' ALTRIMENTI } b \text{ DOVREBBE} \\ \text{ESSERE } 0 \text{ O } 1 \end{array}$$

↪ Se $m=12$, posso prendere
 $a=3 \in b=4$, BASTA CHE
ESISTANO I DUE VALORI

• Se a e b sono diversi da 1 e m , allora
 $1 < a, b < m$

• Anello, inoltre, supposto che l'anello solesse per
tutti gli m : $2 \leq m \leq m$

Ciò significa che esistono $p_1, p_2, \dots, p_t, p_{t+1}, \dots, p_u$
primi tali che:

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_t \quad e \quad b = p_{t+1} \cdot p_{t+2} \cdot \dots \cdot p_u$$

Se queste cose è vero, allora significa che
vale anche per m , infatti:

$$m = a \cdot b = p_1 \cdot p_2 \cdot \dots \cdot p_t \cdot p_{t+1} \cdot p_{t+2} \cdot \dots \cdot p_u$$

Quindi per induzione di II forma, tutti i numeri naturali in $\mathbb{N} \setminus \{0, 1\}$ verificano l'assunto

SE VERIFICAMO CHE SE LA COSA VALE PER I NUMERI PRIMA DI UN ALLORA VALE ANCHE PER UN ALGORITMO VALE PER TUTTI I NUMERI NATURALI MAGGIORI DI UN

↓

Dobbiamo ora dimostrare il caso generale con $m \in \mathbb{Z}$. Avendolo già dimostrato per $m \in \mathbb{N}$, considero $m \in \mathbb{Z} \setminus \mathbb{N}$.

↪ Allora $-m \in \mathbb{N}$, ma per i numeri naturali abbiamo già dimostrato questa cosa, quindi $\exists p_1, p_2, \dots, p_r$ numeri primi tali che $-m = p_1 \cdot p_2 \cdot \dots \cdot p_r$. Ma ciò significa che $m = (-p_1) \cdot p_2 \cdot \dots \cdot p_r \rightarrow -p_1$ è ancora primo perché la definizione resta uguale

b. Vogliamo dimostrare che se ci sono due decomposizioni di m , allora sono uniche a meno dell'ordine e del segno

↪ Se $p_1 \cdot \dots \cdot p_r = m = q_1 \cdot \dots \cdot q_s$, allora $r = s$ ed $\exists f : \{1, \dots, r\} \rightarrow \{1, \dots, s\}$ biiettiva tale che

$$f(\forall i \in \{1, \dots, r\})(p_i = \pm q_{f(i)})$$

$$\text{ESEMPIO: } 12 = 2 \cdot 2 \cdot 3 = 2 \cdot (-2) \cdot (-3) = 3 \cdot 2 \cdot 2$$

Usiamo l'induzione di prime forme su r

• BASE DI INDUZIONE:

Se $r=1$, $p_1 = m = q_1 \cdot \dots \cdot q_s$

Visto che $q_1 \cdot \dots \cdot q_s$ sono divisori di p_1 , per il lemma 1 questi divisori sono tutti quelli stessi

↪ $s=r=1$ e $q_1 = p_1$ perché in $q_1 \cdot \dots \cdot q_s$ possono esserci solo un p_1 e poi tutti +1 o -1

Suppongo l'assesso vero per $n-1$
 p_1 è primo per definizione e, dato che
 $p_1 = m = q_1 \cdot \dots \cdot q_s$, $p_1 \mid q_1 \cdot \dots \cdot q_s$
 \hookrightarrow Dalla definizione di primo, p_1 deve dividere
 uno tra q_1, q_2, \dots, q_s (almeno)
 $\hookrightarrow (p_1 \mid q_1 \vee p_1 \mid q_2 \dots q_s) \xrightarrow{\text{PER INDUZIONE}} (p_1 \mid q_1 \vee \dots \vee p_1 \mid q_s)$

Dato che $(p_1 \mid q_1 \vee \dots \vee p_1 \mid q_s)$ pensiamo supporre,
 senza perdere la generalità (WLOG) che $p_1 \mid q_1$

\downarrow
 Poiché q_1 è primo e non può essere ± 1 ,
 allora $p_1 = \pm q_1$ per il lemma 1.

Di conseguenza ho che $p_1 \cdot p_2 \cdot \dots \cdot p_r = m = \pm p_1 \cdot q_2 \cdot \dots \cdot q_s$

\hookrightarrow Ciò significa p_1 è cancellabile, quindi ho
 che $p_2 \cdot \dots \cdot p_r = q_2 \cdot \dots \cdot q_s \xrightarrow{\substack{\text{LA DECOMPOSIZIONE CON } n-1 \text{ FATTORI} \\ \text{È UGUALE A QUELLA CON } s-1 \text{ FATTORI}}$

Per l'ipotesi di induzione ho che $n-1 = s-1$,
 cioè $n=5$

Inoltre, $\exists \sigma: \{2, \dots, n\} \rightarrow \{2, \dots, n\}$ biiettiva

tele che $(\forall i \in \{2, \dots, n\})(p_i = \pm q_{\sigma(i)}) \xrightarrow{\substack{\text{SI HA UNA} \\ \text{PERMUTAZIONE} \\ \text{DEGLI INDIPI}}$

Dobbiamo forse vedere che abbiamo un funzione
 $f: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ tale che $(\forall i \in \{1, \dots, n\})(f_i = \pm q_{f(i)})$

\hookrightarrow Definisco $f: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ tale che:

\downarrow
 F CONTINUA AD
 ESSERE
 BIETTIVA

$f(1) = 1$ e $(\forall i \in \{2, \dots, n\})(f(i) = \sigma(i))$

CALCOLO COMBINATORIO

DEFINIZIONI

- Un insieme X si dice finito se esiste una biettione tra X e l'insieme $\{1, \dots, m\} \subseteq \mathbb{N}$.
 m si dice ordine o cardinalità di X e si indica con $|X| := m \rightarrow |\{1, 2, 3\}| = 3$.
- Un insieme X si dice infinito se esiste una biettione tra X e una parte propria di X .
- X e Y si dicono equipotenti se esiste $f: X \rightarrow Y$ dove f è biettiva.

ASSIOMA DELL' INFINITO

Esiste un insieme infinito

DA QUI SI HA L'ESISTENZA EQUIVALENTE DI UN INSIEME NATURALMENTE ORDINATO NON SUPERIORMENTE LIMITATO, E' C'È IN, E VICEVERSA

↳ Ciò esiste un insieme equipotente ad una parte propria

ESEMPIO: (\leftarrow)

- $f: m \in \mathbb{N} \mapsto 2m \in 2\mathbb{N}$
(\rightarrow) È DIFFICILE E NON LO FAZZIAMO

E' UNA FUNZIONE BIETTIVA
TRA \mathbb{N} E UNA PARTE PROPRIA
DATO CHE $2\mathbb{N} \subset \mathbb{N}$

TEOREMA

$(\forall m \in \mathbb{N} \setminus \{0\}) (\{1, 2, \dots, m\} \text{ non è infinito})$

↳ Sarete per dire che un insieme finito è non infinito

NO DIM

TEOREMA \rightarrow DIM NEGLI ESERCIZI
DEL 19/11/2022

Se S è un insieme finito, allora ho che

$$|\mathcal{P}(S)| = 2^{|S|}$$

L'ORDINE DELLE PARTI DI S

3) TEOREMA

Se S è un insieme finito - allora ho che se $|S| = m$ allora $|\mathcal{P}(S)| = 2^m$

DIM → per induzione di prima forma.

Th: $(\forall m \in \mathbb{N})(|S|=m \rightarrow |\mathcal{P}(S)|=2^m)$

BASE DI INDUZIONE Per $m=0$ ho che $|S|=0$.

Ma $|S|=0$ vuol dire che esiste un'applicazione biettiva $f: S \rightarrow \{m \in \mathbb{N} \mid 1 \leq m \leq |S|\}$.

Visto che l'ordine di S è 0, nell'insieme $\{m \in \mathbb{N} \mid 1 \leq m \leq |S|\}$ non ci sono elementi, quindi è uguale all' \emptyset

↳ NON ci sono numeri TRA 1 E 0

↳ Per essere un'applicazione biettiva nel senso, dobbiamo avere $S = \emptyset$. → DALLA DEFINIZIONE

Infatti, la definizione di funzione è che

$(\forall x)(x \in S \rightarrow (\exists y \in \emptyset)(f(x)=y))$, ma dato che la

seconda parte dell' " \rightarrow " è falsa, ma la frase

dove deve essere vera per definizione, - allora

" $(\forall x)(x \in S)$ " è falsa, cioè $S = \emptyset$

Nei sopraffatti che $\mathcal{P}(\emptyset) = \{\{\emptyset\}\}$. Quindi sappiamo che esiste un'applicazione biettiva $\varphi: \{\{\emptyset\}\} \rightarrow \{1\}$

Quindi per definizione $|\mathcal{P}(S)| = 1 = 2^0$

Quindi se $S = \emptyset$, la formula è verificata con $m=0$

PASSO INDUTTIVO: Suppongo vero l'enunciato per tutti gli insiemi di ordine $m > 0 \rightarrow$ DEVO FAR VEDERE CHE VALE PER $m+1$

Prendo S di ordine $|S|=m+1$

Visto che $m \geq 0$, allora $S \neq \emptyset$ perché esiste

f biettiva che $f: S \rightarrow \{1, 2, \dots, m, m+1\}$

• Premuto un certo $x \in S$ e definisco $t = S \setminus \{x\}$

Visto che f è biettiva, posso dire che

l'immagine di x è compresa tra 1 e $m+1$

↳ Se $f(x) = m$, $1 \leq m \leq m+1$

• Possiamo costruire $f_{|t}$, che sarà ancora biettiva e
sarà del tipo:

$f_{|t}: t \rightarrow \text{Im } f_{|t} = \{1, 2, \dots, m-1, m+1, \dots, m, m+1\}$

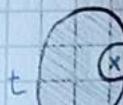
Dato che abbiamo tolto m, $|t|=m$, quindi è

un'applicazione biettiva che:

$f_{|t}: t \xrightarrow{B_1} \{1, 2, \dots, m-1, m+1, \dots, m, m+1\} \xrightarrow{B_2} \{1, \dots, m\}$

• Dall'ipotesi induttiva, abbiamo che $|P(t)| = 2^m$

• Posto graficamente ho che:

 $S = t \cup \{x\}$

$\left. \begin{array}{l} m \in S \\ t = P(S) \cup \{x\} \\ |t| = m \end{array} \right\}$ {Ogni parte di S è uguale a una parte di t unite
e una parte di x.

Le parti di x sono 2, cioè $P(x) = \{\emptyset, \{x\}\}$

↳ Ciò significa che $|P(S)| = 2^m \cdot 2 = 2^{m+1}$

• Possiamo ora dire che per induzione di I forme
segue la tesi, cioè che l'esito $\forall m \in \mathbb{N}$

PRINCIPIO DI INCLUSIONE-ESCLUSIONE

Se Q_1, Q_2, \dots, Q_m sono insiemi, scrivo:

$$\bigcup_{i=1}^m Q_i := Q_1 \cup Q_2 \cup \dots \cup Q_m$$

TEOREMA DEL PRINCIPIO DI INCLUSIONE-ESCLUSIONE

$$\left| \bigcup_{i=1}^m Q_i \right| = \sum_{i=1}^m |Q_i| - \sum_{1 \leq i < j \leq m} |Q_i \cap Q_j| + \sum_{1 \leq i < j < k \leq m} |Q_i \cap Q_j \cap Q_k| - \dots + (-1)^{m-1} \cdot |Q_1 \cap Q_2 \cap \dots \cap Q_m|$$

I SEGNI SONO ALTERNI

Il concetto di questo teorema è che:

Se ho m insiemi, prendo l'unione di tutti questi insiemi. Poi, mi accorgo che ho preso degli elementi in più che stanno nelle intersezioni e che non ri-contavo facendo la cardinalità dell'insieme unione. Quindi il principio di inclusione-esclusione ci permette di calcolare la corretta cardinalità dell'unione di più insiemi.

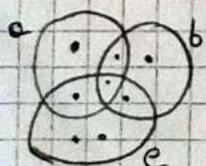
ESEMPI:

CON DUE INSIEMI

$$|a|=3 \quad \begin{matrix} \bullet \\ \bullet \\ \bullet \end{matrix} \quad |b|=4 \quad \begin{matrix} \bullet \\ \bullet \\ \bullet \\ \bullet \end{matrix} \quad \rightarrow a \cup b = (a \Delta b) \cup (a \cap b)$$

$|a \cup b| = 6$ perché dobbiamo fare $3+4-1=6$, altrimenti considereremmo due volte l'elemento nell'intersezione.

CON TRE INSIEMI



Vogliamo trovare $|a \cup b \cup c|$

$$\left. \begin{array}{l} |a|=4 \\ |b|=4 \\ |c|=5 \end{array} \right\} \text{PRINCIPIO DI INCLUSIONE-ESCLUSIONE} \rightarrow 4+4+5-2-2-2+1 = 8 = |a \cup b \cup c|$$

$$|\varnothing \cup b \cup c| = 8 \quad \text{perché:}$$

- Sommiamo prima tutte le cardinalità $|a| + |b| + |c|$
- Sottraiamo le intersezioni a due a due:
 $|a| + |b| + |c| - |a \cap b| - |b \cap c| - |a \cap c|$
- Ma così facendo abbiamo fatto l'intersezione di tutti e tre, quindi dobbiamo sottrarre:
 $|a| + |b| + |c| - |a \cap b| - |a \cap c| - |b \cap c| + |a \cap b \cap c|$

ESEMPI:

$$\begin{aligned} &|a|=5 & |a \cup b|? \\ &|b|=9 \\ &|a \cap b|=3 \end{aligned}$$

$$|a \cup b| = |a| + |b| - |a \cap b| = 11$$

$$\begin{aligned} &|a|=5 & |a \cap b|? \\ &|b|=3 \end{aligned}$$

$|a \cup b| = 2k \rightarrow$ cioè, se l'unione è un multiplo di 2, quanto può valere l'intersezione?

$$2k = |a| + |b| - |a \cap b| \Leftrightarrow$$

$$2k = 14 - |a \cap b| \rightarrow |a \cap b| = 2(7-k)$$

d'intersezione non puoi essere più grande di a e non puoi essere minore di 0, quindi:

$$0 \leq |a \cap b| = 2(7-k) \leq 14$$

$$|a \cap b| può solo essere 0, 2 o 4 \rightarrow |a \cap b| \in \{0, 2, 4\}$$

FATTORIALE

DEFINISCO:

$$0! = 1$$

$$\text{Se } m > 0, \quad m! = (m-1)! \cdot m$$

ESEMPIO:

$$3! = 2! \cdot 3 = 1! \cdot 2 \cdot 3 = 0! \cdot 1 \cdot 2 \cdot 3 = 1 \cdot 1 \cdot 2 \cdot 3 = 6$$

TEOREMA

Siamo a e b insiemi: $|a| = m$, $|b| = n$, allora:

1) ci sono m^n applicazioni da a a b

DIM (Per induzione di prima ferma su m)

• BASE: $m=0$, cioè $a = \emptyset \rightarrow$ PER ESSERE VERIFICATA, CI SERVANO ESSERE $n=1$ FUNZIONI CHE $\emptyset \rightarrow b$

Ritengo $f: \emptyset \rightarrow b \rightarrow$ è una funzione ($\emptyset \times b, f$)

ma $f \subseteq \emptyset \times b = \emptyset$, quindi f è solo $(\emptyset \times b, \emptyset)$. Abbiamo verificato il passo base perché vi è una sola $f: \emptyset \rightarrow b$.

• PASSO INDUTTIVO: Suppongo vero per $(m) \Rightarrow$

Sia $x \in a$, sia $t = a \setminus \{x\}$. Per ipotesi di induzione ci sono n^m applicazioni da t a b

Da a a b ci sono $m \cdot n^m$ applicazioni, cioè m^{m+1} modi diversi di mandare elementi da a a b .

↳ Per induzione vale la tesi

→ QUESTO PERCHÉ TUTTI GLI ALTRI ELEMENTI DI a (ovvero l'insieme t) SAPPIANO AVERE n^m FUNZIONI. QUELL'UNICO ELEMENTO x PUÒ ANDARE IN OGNI ELEMENTO DI b , cioè ci possono essere m FUNZIONI $\{x\} \rightarrow b$

2) a. Esistono applicazioni iniettive da a in b
 a e solo se $m \leq n$

DIM

(\rightarrow) Sia $a \xrightarrow{f_{in}} b$. Assumiamo che esistano delle applicazioni
bigettive che: $\{1, \dots, m\} \cong a \xrightarrow{f_{in}} b \cong \{1, \dots, m\}$ compatibili
fra loro.

Esiste ψ iniettiva di $\{1, \dots, m\}$ in $\{1, \dots, m\}$

Quindi $m \leq m$

non avere l'elenco infinito. Che
 $\{1, \dots, m\} \subseteq \{1, \dots, m\}$

(\leftarrow) Posso fare le stesse dimostrazioni di
prima ma con un'applicazione che
contrario, cioè:

$m \leq m$, quindi esiste ψ iniettiva $\{1, \dots, m\} \rightarrow \{1, \dots, m\}$
dato che risulterà $\{1, \dots, m\} \subseteq \{1, \dots, m\}$ e avrò che
esistono applicazioni bigettive $a \cong \{1, \dots, m\} \xrightarrow{\varphi} \{1, \dots, m\} \cong b$.

Quindi esiste $\psi: a \rightarrow b$ iniettivo

de a in b
2) b. le applicazioni iniettive in numero sono 0 o $\frac{m!}{(m-n)!}$

DIM

• Se $m < n$ allora le applicazioni iniettive da
 a in b sono 0.

• Se $m \leq n$ per l'induzione di prima faccio "m"
BASE: $m=0 \rightarrow$ cioè c'è una sola applicazione iniettiva.

Infatti: $\frac{m!}{(m-0)!} = 1 \quad \checkmark$

PASSO INDUTTIVO. Suppongo $m > 0$ e suppongo
che l'esatto per $m-1$. \rightarrow Voglio far vedere che
sia anche per m

Prendo $X \in a$ e $t = a \setminus \{x\}$, quindi $|t| = m-1$

Ci sono $\frac{m!}{(m-(m-1))!}$ applicazioni iniettive $t \rightarrow b$ per ipotesi iniettive.

Segue che da a a b ci sono $\frac{m!}{(m-(m-1))!} \cdot m = (m-1)$ applicazioni iniettive.

Ma:

$$\frac{m!}{(m-(m-1))!} \cdot (m-(m-1)) = \frac{m!}{(m-m+1)!} \cdot (m-(m-1)) =$$

$$= \frac{m!}{(m-m+1)(m-m)!} \cdot (m-m+1) = \frac{m!}{(m-m)!}$$

Dal principio di induzione di prima forma vale la tesi.

3) Esistono applicazioni suriettive da a in b se e solo se $a = b = \emptyset \vee 0 < m \leq n$

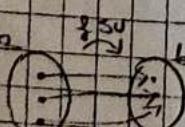
DIM

• da suriettività si ha $x \in a \Rightarrow x \in b$, per definizione, $(\forall y \in b)((\exists x \in a)(f(x) = y)) \rightarrow$ Queste cose in vero $x \in b = \emptyset$, ma affinché $b = \emptyset$ c'è bisogno che anche $a = \emptyset$.

\hookrightarrow da funzione $\emptyset \rightarrow \emptyset$ è suriettiva

• Nel caso in cui $0 < m \leq n$, la dimostrazione è identica a quando f è iniettiva.

$$(\rightarrow) \{1, \dots, m\} \xrightarrow{\text{surj}} b \approx \{1, \dots, m\}$$



Esiste φ suriettiva $\{1, \dots, m\} \xrightarrow{\text{surj}} \{1, \dots, m\}$, quindi il codominio è tutto preso, cioè $m \leq n$

(\leftarrow) UGUALE MA AL CONTRARIO

QUESTO PROBLEMA
RIFERISCE A PIA
INIEZIONI X
PIUTTOSTO
SOLO NEGLI
ELEMENTI DEL
CODOMINIO
PRESI

4) Esistono applicazioni biettive da a in b
 $x \in a \rightarrow x \in b \wedge f(x) = m$

DIM

(\rightarrow) La dimostrazione è un corollario delle due di prima, perché per essere biettiva deve essere:

- SURGETTIVA $\rightarrow m \leq m \wedge m = m$
- INIETTIVA $\rightarrow m \geq m$

(\leftarrow) Esistono, quindi, applicazioni biettive $a \simeq \{1, \dots, m\} \simeq b$

5) $|\text{Sym}(a)| = m!$

DIM Dato che $\text{Sym}(a)$ sono le applicazioni

biettive da a in a , allora queste applicazioni sono anche iniettive. Di conseguenza

$$\frac{m!}{(m-m)!} = \frac{m!}{0!} = m! - m! \text{ dato che } m = m$$

e se hanno lo stesso ordine

6) Sia $m = m' \in f: a \rightarrow b$

f è iniettiva $\Leftrightarrow x \in a \rightarrow f(x) = f(y) \Rightarrow x = y$
se f è surgettiva.

DIM • Se f è biettiva, allora implica che f è anche surgettiva e iniettiva. Inoltre:

• (INIETTIVA \rightarrow BIETTIVA)

In questo caso, le funzioni iniettive sono $\frac{m!}{(m-m)!} = m!$, proprio come quelle biettive.

• (SURGETTIVA \rightarrow BIETTIVA)

Bando $g: b \rightarrow a$ xazione di f , cioè tale che
 $f \circ g = \text{Id}_b$

Dato che Id_b è iniettivo, allora g è iniettiva.

$\hookrightarrow g$ è quindi biettiva + notiamo che $f = g^{-1}$

perché iniettiva e surgettiva

DATO CHE L'INSIEME
di BIETTIVI È UN
SOTTOinsieme DI QUESTI
INIETTIVI E I CERCI INSETTI
HANNO VALORE NUMERO DI ELEMENTI

Infatti, $f = g^{-1}$ perché abbiamo che:

$$f = (\overset{\uparrow}{f \circ g}) \circ g^{-1} = \text{Id}_S \circ g^{-1} = g^{-1}$$

ASSOCIAZIONE

Quindi, avendo l'inverso, f è biettiva.

ATTENZIONE: Queste cose si ha se S e B sono insiemi finiti, ma non se sono infiniti.

ESEMPIO:

- $f: m \in \mathbb{N} \mapsto 2m \in \mathbb{N}$ è iniettiva ma non suriettiva

TEOREMA

S è FINITO

Sia $(S, *)$ un monoido commutativo $\xrightarrow{\text{finito}}$ e sia $x \in S$, allora x è cancellabile $\xrightarrow{x \neq 0}$ se e solo se x è invertibile.

DIM

$$(a, b \in S)(x \cdot a = x \cdot b \rightarrow a = b)$$

(\leftarrow) Il caso in cui invertibile \rightarrow cancellabile
è obiettivo già fatto.

(\rightarrow) 0_x e δ_x sono iniettive \rightarrow allora sono biettevili per il teorema di prima. Essendo 0_x e δ_x biettevili,

essendo che: $(\exists y \in S)(0_x(y) = 1)$, di conseguenza x è invertibile.

\rightarrow A_{0_x} è HA L'ANTIMMAGINE
ESSENDO 0_x BIETTIVA

Quindi $x \cdot y = 1$,

Inoltre, $(\exists z \in S)(\delta_x(z) = 1)$ } Di conseguenza x
è invertibile

Quindi $z \cdot x = 1$

COROLLARIO

TUTTI ELEMENTI
EFFETTUABILI

PERCHE'
TUTTI
INVERTIBILI

- 1) Gli omelli unitari intatti finiti sono corpi.
- 2) I dominii di integrità finiti sono esampi
ESAMI CONSTITUITIVI

FUNZIONE CARATTERISTICA DI t IN S

Sia S un insieme e sia $t \subseteq S$.

Definisco: $\chi_{t,S} : x \in S \mapsto \begin{cases} 0 & \text{se } x \in t \\ 1 & \text{se } x \notin t \end{cases}$
"chi"

La funzione $\chi_{t,S}$ si chiama funzione

caratteristica di t in S MI PERMETTE DI VEDERE CON
L'IMMAGINE CI X SE X STA IN
t O MENO

INSIEME DELLE APPLICAZIONI DA a IN b

Se a e b sono insiemi, l'insieme delle applicazioni da a in b lo scrivo come b^a

ESEMPIO:

Quindi $\chi_{t,S} \in \{0,1\}^S$ perché è una funzione $S \rightarrow \{0,1\}$

TEOREMA

Sia S un insieme.

Allora $\Psi : t \in \wp(S) \mapsto \chi_{t,S} \in \{0,1\}^S$ è biettiva

DIM

1. Sia $f \in \{0,1\}^S$, cioè è una funzione $S \rightarrow \{0,1\}$

↓
Definisco $t = \{x \in S \mid f(x) = 1\}$

↓
Allora, $\Psi(t) = \chi_{t,S}$ e: Quando, $\chi_{t,S} = f$
• Se $x \in t$ $\chi_{t,S}(x) = 1 = f(x)$ e quindi Ψ è suriettiva
• Se $x \notin t$ $\chi_{t,S}(x) = 0 = f(x)$ L^a ogni x CORRISPONDE UNA IMMAGINE $\chi_{t,S}$ PERCHE' HANNO UGUALE

2. Sia $t \in S$ e $N \subseteq S$ con $t \notin N$

↓
INIETTIVA

SENZA

LE DUE LE
GENERALITÀ

WLOG premo $x \in t \setminus N$ \rightarrow UN x CHE STA
SOLI IN t

$$\hookrightarrow \begin{cases} \cdot \chi_{t \setminus N}(x) = 1 \\ \cdot \chi_{N \setminus S}(x) = 0 \end{cases} \quad \left\{ \text{Ma } \chi_{t \setminus N} \neq \chi_{N \setminus S} \right.$$

$$\hookrightarrow \begin{cases} \cdot \chi_{N \setminus S}(x) = 0 \end{cases} \quad \text{cioè } \varphi \text{ è iniettiva.}$$

\hookrightarrow t' diverse \rightarrow p(t) diverse

COROLLARIO

Se S è un insieme finito $|P(S)| = 2^{|S|}$

\hookrightarrow VISTO CHE IL CARAT. DI $\{x_1, x_2, \dots, x_n\}$ È CERTA, IL NUMERO DI ELEMENTI DI $P(S)$ È
UGUALE A C. DELLA P. DI $\{x_1, x_2, \dots, x_n\}$, MA L'ORDINE DI $\{x_1, x_2, \dots, x_n\}$ È $(x_1, x_2, \dots, x_n) = 2^{|S|}$

COEFFICIENTE BINOMIALE

• Se $m \in \mathbb{N} \setminus \{0\}$, definisco $I_m := \{1, \dots, m\}$

• $\forall m, k \in \mathbb{N}$, definito $\binom{m}{k} := |\mathcal{P}_k(I_m)|$ $\begin{matrix} \text{E' l'ORDINE DELLE} \\ \text{k-PARTI DI } I_m \end{matrix}$

COEFFICIENTE
BINOMIALE
 m SU k

$\hookrightarrow \mathcal{P}_k(S)$ si dice "k-parti
di S "

ESEMPIO:

$\cdot \binom{0}{3} = 0 \rightarrow$ E' LA CARDINALITÀ DELLE 3-PARTI DI $I_0 = \emptyset$

$\cdot \binom{4}{4} = 1 \rightarrow$ QUANTE PARTI DI I_4 ESISTONO CON 4 ELEMENTI? 1

• Se $m < k$, $\binom{m}{k} = 0$

\rightarrow PER AVERE UN NUMERO MAGGIORE DI 0
DOVREI METTERE IN UN INSIEME k
ELEMENTI AVENDONE A DISPOSIZIONE
UN NUMERO INFERIORE

TEOREMA

$$(\forall m \in \mathbb{N}) \left(\sum_{k=0}^m \binom{m}{k} = 2^m \right)$$

DI

$$\mathcal{P}(I_m) = \mathcal{P}_0(I_m) \cup \mathcal{P}_1(I_m) \cup \dots \cup \mathcal{P}_m(I_m)$$

Gli ordini di ogni k -parte è, per definizione, $\sum_{k=0}^m \binom{m}{k}$ e
l'ordine di $\mathcal{P}(I_m)$ solitamente essere 2^m

TEOREMA

$$(\forall m, k \in \mathbb{N})(k \leq m \rightarrow \binom{m}{k} = \binom{m}{m-k})$$

PER OGNI PARTE CON
K ELEMENTI EE NE
STA UNA SOLA CON
m-k ELEMENTI, E' LA
DIFERENZA

DIM

$f: X \in P(I_m) \rightarrow I_m \setminus X \in P(I_m)$ vogliamo essere tutt'e

$$\text{Mo } \tilde{f}(P_k(I_m)) = P_{m-k}(I_m) \xrightarrow{\substack{\text{TIFFETTI LE PARTI CON K ELEMENTI} \\ \text{LE MANO NELLE PARTI IN } m-k \text{ ELEMENTI} \\ \text{DATO CHE STO FAENDO LA DIFFERENZA}}} \tilde{f}(P_k(I_m))$$

Se faccio $f|_{P_k(I_m)}: X \in P_k(I_m) \rightarrow I_m \setminus X \in P(I_m)$, posso
poi immagazzinare $P_{m-k}(I_m)$ che è l' I_m RESTRIBUITO AL I_{m-k}

FORMULA RICORSIVA PER I COEFFICIENTI BINOMIALI

$$(\forall m, k \in \mathbb{N})(k \leq m \rightarrow \binom{m+1}{k+1} = \binom{m}{k} + \binom{m}{k+1})$$

DIM

- Prendo le $k+1$ parti di I_{m+1} che non contengono 1 e chiama questo insieme " a ".

- $b = (k+1)$ parti di I_{m+1} che contengono 1 .

$\{a, b\}$ è una partizione di $P_{k+1}(I_{m+1})$

ESSENDO UNA PARTIZIONE

$$\text{Allora: } \binom{m+1}{k+1} = |P_{k+1}(I_{m+1})| = |\{a\}| + |\{b\}| = \binom{m}{k+1} + \binom{m}{k}$$

$|\{a\}| = \binom{m}{k+1}$ perché sono le $k+1$ parti dell'insieme I_{m+1} che, senza un elemento, è isomorfo a I_m

$|\{b\}| = \binom{m}{k}$ perché lo do per niente, devo stare per forza nelle parti, quindi ci saranno essere solo k parti di I_m combinazioni diverse

ESSENDO $\{a, b\}$
UNA PARTIZIONE

$$\binom{m}{k+1} + \binom{m}{k}$$

TARTAGLIA

$$\begin{array}{c} \binom{0}{0} \\ \binom{1}{0} \quad \binom{1}{1} \\ \binom{2}{0} \quad \binom{2}{1} + \binom{2}{2} \\ \binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3} \end{array}$$

$\downarrow m+1$

$$\begin{array}{cccccc} & & 1 & 1 & 1 & \\ & & 1 & 2 & 1 & \\ & & 1 & 3 & 3 & 1 \\ & & 1 & 4 & 6 & 4 & 1 \\ & & 1 & 5 & 10 & 10 & 5 & 1 \end{array}$$

TEOREMA

$$(\forall m, k \in \mathbb{N}) (k \leq m \rightarrow \binom{m}{k} = \frac{m!}{(m-k)! \cdot k!})$$

DIM Usa il principio di induzione di seconda forma
su m → USO LA SECONDA FORMA PERCHÉ NEI COEFFICIENTI BINONIALI AVRO' $m-1$ CHE E' MINORE DI m

BASE: Se $m=0$

$$\binom{0}{k} = \binom{0}{0} = 1 = \frac{0!}{0! \cdot 0!}$$

APPARISCE
2. PASSO
AVANTI

PASSO INDUTTIVO: Sappiamo che la tesi per tutti gli i : $0 \leq i < m$

$$\binom{m}{k} = \binom{m-1}{k-1} + \binom{m-1}{k} = \text{Per l'ipotesi induttiva} =$$

$$= \frac{(m-1)!}{(m-1-(k-1))! \cdot (k-1)!} + \frac{(m-1)!}{(m-1-k)! \cdot k!} = \frac{(m-1)!}{(m-k)!(k-1)!} + \frac{(m-1)!}{(m-k-1)!(k!)!} =$$

Ora ho lo stesso denominatore

MOLTIPLICO
CIVICO PER n

MOLTIPLICO
CIVICO PER $m-k$

$$= \frac{(m-1)! \cdot k}{(m-k)! \cdot k!} + \frac{(m-1)!(m-k)}{(m-k)! \cdot k!} = \frac{(m-1)!(k+m-k)}{(m-k)! \cdot k!} = \frac{(m-1) \cdot m}{(m-k)! \cdot k!} =$$

$$= \frac{m!}{(m-k)! \cdot k!}$$

Correzione esercizi 23/11/2021 (LEZIONE 25)

$$6. \quad \binom{3}{1} = \binom{2}{1} + \binom{2}{2}$$

$$\binom{3}{1} = \binom{2}{1} + \binom{2}{3}$$

$$\binom{3}{1} = \binom{2}{1} + \binom{2}{3}$$

$$\binom{3}{1} = \binom{2}{1} + \binom{2}{3}$$

Vogliamo calcolarlo con il triangolo di T.

Quindi secondo le formule ricavate, il triangolo di Tartaglia sarà:

$$\begin{array}{ccccccc} & & 2 & 1 & & & \\ & & 3 & / & 3 & 1 & \\ & & 4 & / & 6 & 4 & \\ & & 5 & / & 10 & 10 & \\ & & 15 & / & 20 & & \\ & & 35 & / & & & \end{array}$$

QUESTI LI RICAVO FAENDO LA SOMMA DEI DUE DI PIANI, CHE CONOSCO PERCHÉ MI È FACILE CAPIRE $\binom{m}{1} + \binom{m}{2}$

Buu anche calcolare $\binom{7}{3}$ sarà il triangolo di Tartaglia,

$$\frac{7!}{(7-3)!3!} = \frac{7!}{4! \cdot 3!} = \frac{7 \cdot 6 \cdot 5 \cdot 4!}{4! \cdot 6} = 35$$

$$\text{Invece, } \binom{7}{4} = \frac{7!}{(7-4)!4!} = \frac{7!}{3! \cdot 4!} = 35$$

$$7 \in \{ m \in \mathbb{N} \mid m \leq 9 \}$$

NON C'E'
UNA PARTE
DI UN
ELEMENTO
IN UN
INSIEME
DA 10

$$\bullet |P_{11}(e)| = 0$$

$$\bullet |P_{10}(e)| = 1$$

$$\bullet \binom{10}{3} = \frac{10!}{7! \cdot 3!} = \frac{10 \cdot 9 \cdot 8}{6} = 120$$

$$\bullet \binom{10}{7} = \frac{10!}{3! \cdot 7!} = 120$$

$$\cdot |\{t \in P_4(\alpha) \mid 0 \in t\}| = \binom{9}{3} = \frac{9!}{6! \cdot 3!} = \frac{9 \cdot 8 \cdot 7}{6} = 84$$

E' l'insieme delle 4-parti di α che contengono 0 \rightarrow 0 lo do per scontato, quindi quello che puo' combiniare sono tre elementi in $\alpha \setminus \{0\}$

\hookrightarrow le parti sono del

$$\text{tipo: } \{0, x, y, z\} \quad x, y, z \in \alpha \setminus \{0\}$$

INSIEMI ISOMORFI E DIAGRAMMI DI HASSE

$$\rightarrow (S, P) \cong (S', P')$$

Gia' sappiamo che dati due insiemi ordinati finiti, questi sono isomorfi se e solo se sono rappresentati dalla stessa diagramma di Hasse

Abbriamo dimostrato l' implicazione (\rightarrow).

Dimostriamo anche (\leftarrow) \rightarrow PRIMA ci serviva il concetto di FINITTEZZA

DIM (\leftarrow)

Sia γ una relazione di copertura su (S, P) e γ' una relazione di copertura su (S', P') .

Per ipotesi esiste $f: S \rightarrow S'$ biiettivo:

$$(\forall a, b \in S)(a \gamma b \leftrightarrow f(a) \gamma' f(b)) \rightarrow \text{AVERE LO STESSO DIAGRAMMA DI HASSE SIGNIFICA AVERE LA STESSA RELAZIONE DI COPERTURA}$$

\hookrightarrow la relazione di copertura non è una relazione di equivalenza perché non è transitiva

Definisco \hookrightarrow la rendo transitiva

$$(\forall a, b \in S)(a \leq b \leftrightarrow ((\exists m \in \mathbb{N})((\exists e_1, e_2, \dots, e_m \in S) \cdot$$

$$(a = e_1 \wedge e_1 \gamma e_2 \wedge e_2 \gamma e_3 \wedge \dots \wedge e_{m-1} \gamma e_m \wedge e_m = b)))$$

Cioè, così facendo, posso dire che $a \leq b$ se c'è una relazione di copertura a estesa da b fino ad a

\downarrow
 b così ness transittiva
 la copertura, o meglio,
 ho extrapolato una nuova
 relazione che è anche
 transittiva

$\hookrightarrow \begin{cases} b = c, \\ c = e, \\ d = e, \\ a = e, \end{cases}$ In questo caso ho che
 b copre e , e copre d ,
 d copre a , quindi
 $a \leq b$

\hookrightarrow Si verifica facilmente che \leq è una relazione d'ordine su S

Analogamente, definisco la relazione \leq' su S' :

$$(\forall a', b' \in S') (a' \leq b' \leftrightarrow ((\exists m \in \mathbb{N})(\exists e'_1, e'_2, \dots, e'_m \in S') (a' = e'_1 \wedge e'_1 \gamma' e'_2 \wedge e'_2 \gamma' e'_3 \wedge \dots \wedge e'_{m-1} \gamma' e'_m \wedge e'_m = b')))$$

Notiamo che $\leq = p$ e $\leq' = p'$

SE L'INSIEME NON È FINITO,
 LA RELAZIONE DI COBERTURA
 PUÒ ESSERE DIFERENTE DA C'È A B

\hookrightarrow Infatti, se abbiamo una relazione di copertura estesa come quella definita, abbiamo che vale $a \leq b$ allora vale anche $a \leq b'$.

Se, invece, abbiamo $a \neq b$, visto che l'insieme è finito allora abbiamo una relazione di copertura e quindi vale anche $a \leq b$

Inoltre, notiamo che vale che:

$$(\forall a, b \in S) (a \leq b \leftrightarrow f(a) \leq' f(b))$$

$$\begin{matrix} b \\ /e \leftarrow f(e) \\ \backslash c \\ f(a) \end{matrix}$$

\hookrightarrow In base a come abbiamo definito le due relazioni di coperture, se consideriamo $a' = f(a)$, $b' = f(b)$ ecc; se è verificata γ' allora è verificata anche \leq'

Abbiamo così dimostrato la tesi, cioè $(S, p) \cong (S', p')$

*APPROFONDIMENTO SUL TEOREMA DEI COEFFICIENTI BINOMIALI

Nell'ultimo teorema con i coefficienti binomiali, per fare formalmente la dimostrazione con il principio di seconda forma si usa un ordinamento lexicografico

Valevo dimostrare che:

$$\text{K6} \quad \binom{m}{k} = \binom{m-1}{k-1} + \binom{m-1}{k} \rightarrow \begin{array}{l} \text{per usare il principio di induzione} \\ \text{di II forma volevo dimostrare} \\ \text{che valle per tutti i numeri} \\ \text{più piccoli di } k \end{array}$$

Per dare un ordine

si esponenti binomiali
simile all'ordine in \mathbb{N} \rightarrow coppia (m, k) è ordinato
uso un ordine lexicografico le copie in modo
lexicografico

ORDINE LEXICOGRAPHICO

$$(0,0) < (1,0) < (1,1) < (2,0) < (2,1) < (2,2) < (3,0) < \dots$$

\hookrightarrow Primo confronto il valore a sinistra delle copie,
se sono uguali allora confronto il valore a destra

\downarrow
Infatti, noto che $\binom{m-1}{k-1} < \binom{m-1}{k} < \binom{m}{k}$ nell'ordine
lexicografico, quindi posso usare il principio di
induzione di II forma

TEOREMA BINOMIALE O FORMULA DI NEWTON

$$(a+b)^m = \binom{m}{0} a^m b^0 + \binom{m}{1} a^{m-1} b^1 + \dots + \binom{m}{m-1} a^1 b^{m-1} + \binom{m}{m} a^0 b^m$$

DIM \rightarrow sia S un anello unitario, $a, b \in S$ e tali che $ab = ba$

Dimostrazione Tra gli esercizi, si fa con il principio di
induzione di prima forma

PRINCIPIO DI DUALITÀ (PER GLI INSIEMI) ORDINATI

Dato l'insieme ordinato (S, P) , si dice:

MASSIMO: $m = \text{MAX } S \Leftrightarrow (\forall x \in S)(x \leq m)$

MASSIMALE: $(\forall x \in S)(\text{se } x \in m \text{ sono confrontabili} \rightarrow x \leq m)$

MAGGIORANTE: $m \in \text{MAGGIOR}_S(t) \Leftrightarrow (\forall x \in t)(x \leq m)$ con $t \subseteq S$

MINIMO: $m = \text{MIN } S \Leftrightarrow (\forall x \in S)(m \leq x)$

MINIMALE: $(\forall x \in S)(\text{se } x \in m \text{ sono confrontabili} \rightarrow m \leq x)$

MINORANTE: $m \in \text{MINOR}_{(S, P)}(t) \Leftrightarrow (\forall x \in t)(m \leq x)$ con $t \subseteq S$

Notiamo che esiste una corrispondenza tra massimo e minimo, massimale e minimale, maggiorante e minorante.

↳ Possiamo usare un'operazione doppia dei tipi:

Dato (S, P) con $P := (S \times S, g)$, l'operazione opposta sarà $\bar{P} := (S \times S, \bar{g})$ con $(a, b) \in \bar{g} \Leftrightarrow (b, a) \in g$

↓

Da qui possiamo scrivere, ad esempio, che:

$$m = \max(S, P) \Leftrightarrow m = \min(S, \bar{P})$$

COSA SIGNIFICA?

Il concetto dietro il principio di dualità è che è inutile dimostrare uno stesso teorema sia per massimo che minimo, o per massimale e minimale ecc.. perché basta dimostrarlo solo per un tipo di coppia.

↳ ESEMPIO PROSSIMA PAGINA

TEOREMA

Dato l'insieme (S, P) ordinato,

Se $m = \min(S, P)$ allora m è l'unico minimo
in (S, P)

DIM

Premetto m elemento minimo di (S, P) .

Per ipotesi, visto che m è il minimo, vale $m \leq m$

↪ Dunque, m e m sono confrontabili.

Allora per definizione di elemento minimo,
vale $m \leq m$

Ma la relazione è asimmetrica, quindi si ha
che $m = m \rightarrow$ SE ESISTE IL MINIMO, E' L'UNICO MINIMALE

Posso dimostrare questo teorema anche per il massimo

↪ Posso considerare l'insieme (S, \bar{P})

Questo teorema vale anche in (S, \bar{P}) , quindi per il principio di dualità ho che se m è un massimo,
allora è l'unico massimale nell'insieme S

ESEMPI:

- In (\mathbb{N}, \leq) , prendo $t \in \mathbb{N}$

• $\text{minor}_{(\mathbb{N}, \leq)}(t)$? Ad esempio, $\text{minor}_{(\mathbb{N}, \leq)}(2\mathbb{N}) = \{0\}$

- $(\mathbb{N}, |)$ $t \in \mathbb{N}$

SONO I DIVISORI COMUNI DELL'INSIEME \bullet $\text{minor}_{(\mathbb{N}, |)}(t)$? Ad esempio, $\text{minor}_{(\mathbb{N}, |)}(\{2, 3\}) = \{1\}$

$$\text{minor}_{(\mathbb{N}, |)}(2\mathbb{N}) = \{1, 2\}$$

SONO I MULTIPLO COMUNI DELL'INSIEME \bullet $\text{Maggior}_{(\mathbb{N}, |)}(t)$? Ad esempio,

$$\text{maggior}_{(\mathbb{N}, |)}(\{2, 3\}) = 6 \mathbb{N} = \{6\}$$

$$\text{maggior}_{(\mathbb{N}, |)}(2\mathbb{N}) = \{0\}$$

O E' MULTIPLO DI OGNI NUMERO, INFATTI
 $O = n \cdot m$

I MULTIPLO DI 6

• $(P(S), \subseteq)$ $t \subseteq P(S)$

UNIONE UNARIA
DI ϵ

$y \in \text{maggior}_{(P(S), \subseteq)}(t) \leftrightarrow \bigcup t \subseteq y$

↓
SONO TUTTE LE PARTI CHE
CONTENGONO GLI ELEMENTI
DI y

ESEMPIO:

$S = \{1, 2, 3\}$ e prendo $t = \{\{1\}, \{2\}\}$

$\text{maggior}_{(P(S), \subseteq)}(\{\{1\}, \{2\}\})$ = Tutti gli elementi di S che
contengono tutti gli elementi di t

Cioè sono tutti gli elementi y che:

$\{1\} \subseteq y \wedge \{2\} \subseteq y$, cioè, se e solo se $\{1, 2\} = \bigcup t \subseteq y$

$y \in \text{minor}_{(P(S), \subseteq)}(t) \leftrightarrow y \subseteq \bigcap t$

INTERSEZIONE
UNARIA DI ϵ

ESEMPIO:

$\text{minor}_{(P(S), \subseteq)}(\emptyset) = P(S) \rightarrow$ UN ELEMENTO DI $P(S)$ APPARTIENE

DALLA DEFINIZIONE $\leftarrow \forall x \in \emptyset (y \subseteq x)$, MA QUESTA COSA E'
SEMPRE VERA DATO CHE, COME FBF,
SI HA UN " \rightarrow " CHE HA LA PRIMA
PARTE FALSA, QUINDI I MINORANTI
SONO TUTTI GLI ELEMENTI DI $P(S)$

↓

DALL'ASSIOMA DI SEPARAZIONE ABBIAMO
CHE QUESTO E' TUTTO $P(S)$ PERCHE'
SPEREBBE DOVUTO ESSERE L'INSIEME
DI TUTTI GLI INSIEMI

TEOREMA

Sia (S, p) un insieme ordinato finito non vuoto e $p \in \text{OL}(S)$.

Allora (S, p) ha elementi minimi ed elementi massimi.

DIM

Per Assurdo, sia che (S, p) non ha elementi minimi. Considero $x \in S$, che per l'ipotesi di assurdo non è un minimo.

↪ Se $S = \{x\}$, x risulta essere un minimo, quindi necessariamente $(\exists y \in S)(x \neq y) \rightarrow$

S NON PUÒ ESSERE UN SINGLETON

Questo y non è un minimo per ipotesi di assurdo e, inoltre, vale $y \leq x$.

• PERCHÉ VALE $y \leq x$?

NOI SAPPIAMO DALLA DEFINIZIONE CHE:

x è minimo $\Leftrightarrow (\forall y \in S)(x \leq y \vee y \leq x) \rightarrow (x \leq y)$

SE FACCIAMO LA NEGAZIONE DI "ESSERE MINIMO" AVREMO:

x non è minimo $\Leftrightarrow (\exists y \in S)(x \leq y \vee y \leq x) \wedge (\neg(x \leq y)) \Leftrightarrow$
 $\Leftrightarrow (\exists y \in S)((x \leq y \wedge \neg(x \leq y)) \vee (y \leq x \wedge \neg(y \leq x))) \Leftrightarrow$
 $\Leftrightarrow (\exists y \in S)(y \leq x \wedge \neg(x \leq y))$

Di conseguenza ho che y è più piccolo di x , quindi nel diagramma di Hasse ho che:

Visto che y non è minimo, allora ho che
 $(\exists z \in S)(z \neq y \wedge z \leq y)$

↪ Inoltre $z \neq x$ perché se fosse uguale a x , allora potrei avere $x \leq y$, ma abbiamo detto che non è vero.

Poco continuare andando oltre $|S| \leq$

TEOREMA

Se un insieme finito ordinato ha un unico elemento minimo, questo è anche il minimo

Se un insieme finito ordinato ha un unico elemento massimale, questo è anche il massimo

NON

Questo non vale se l'insieme è infinito

ESEMPIO:

- (\mathbb{N}, \leq) e prendo un insieme S .

$$S = \mathbb{N} \cup \{x\}$$

$$\leq = (\mathbb{N} \times \mathbb{N}, G)$$

Considero $p = (S \times S, g)$ con $g = G \cup \{(x, x)\}$

OPZIO? Si $\rightarrow (0, 1) \in g$

OPX? No $\rightarrow (0, x) \notin g$

xpx Si $\rightarrow (x, x) \in g$

DEFINISCO UN'ALTRA RELAZIONE D'ORDINE, UGUALE AL «MA CHE HA ANCHE LA COPPIA (x, x) NEL GRAFICO OLTRE A QUELLE CON I NUMERI NATURALI»

(S, p) Non ha massimo perché non c'è un elemento

c'è un ELEMENTO che è più grande di tutti gli altri, ma non confrontabile

x è l'unico massimale

x è l'unico massimale perché, non essendo confrontabile, la prima parte dell'implicazione è falsa, quindi la frase è vera

\mathbb{N}	0	1	2	3	x
--------------	---	---	---	---	-----

• RELAZIONE D'ORDINE INDOTTA DA ρ SU S
Se $f: S \rightarrow S$ è PEOC (ρ) definisco:

$(\forall x, y \in S)(x \rho y \leftrightarrow f(x) \rho f(y))$ è la chiamo
 ρ_f relazione d'ordine
indotta da f su S .

ESTREMO INFERIORE

(S, ρ) , con $t \in S$, se esiste il massimo di
 $\text{MINOR}_{(S, \rho)}(t)$ lo dico $\inf_{(S, \rho)}(t) \rightarrow$ il MASSIMO DEI MINORANTI

ESTREMO SUPERIORE

(S, ρ) , con $t \in S$, se esiste il minimo di
 $\text{MAGGIOR}_{(S, \rho)}(t)$ lo dico $\sup_{(S, \rho)}(t) \rightarrow$ il MINIMO DEI MAGGIORANTI

ESEMPIO:

$$\bullet (IN, \leq) \quad \sup_{(IN, \leq)}(\{3, 4\}) = 4$$

$$\sup_{(IN, \leq)}(\{1, 2, 3\}) = \nexists \rightarrow \text{IN } 2^{\text{nd}} \text{ non ci sono MAGGIORANTI}$$

$$\inf_{(IN, \leq)}(\{1, 2, 3\}) = \{0\}$$

RETICOLO

(S, ρ) ordinato si dice reticolo se per ogni $x, y \in S$,
 $\{x, y\}$ ha minimo superiore ed estremo inferiore.

OPERAZIONI INF E SUP

Se (S, ρ) è un reticolo, definisco:

- $\wedge: (x, y) \in S \times S \mapsto \inf_{(S, \rho)}(\{x, y\}) \quad \left. \begin{array}{l} (S, \wedge, \vee) \text{ è una} \\ \text{struttura algebrica} \\ \text{a operazioni interne} \end{array} \right\}$
- $\vee: (x, y) \in S \times S \mapsto \sup_{(S, \rho)}(\{x, y\})$

RETIcolo LIMITATO

Un reticolo (S, \leq) si dice limitato se ha massimo e minimo.

RETIcolo COMPLETO

Un reticolo (S, \leq) si dice completo se ogni sua parte diversa dal tutto permette estremo superiore ed estremo inferiore.

DEFINIZIONE FORMALE DI RETIColo

(S, \leq) è un reticolo $\Leftrightarrow (\forall a, b \in S)(\exists \sup(\{a, b\}) \wedge \exists \inf(\{a, b\}))$

Se ho degli elementi non confrontabili, l'implicazione diretta risulta falsa, quindi automaticamente esistono sup e inf, quindi (S, \leq) è un reticolo.

- Correzione esercizi 29/11/2021 (LEZIONE 26)

a) (\mathbb{N}, \leq)

cioè è l'elemento subito dopo
di cioè tale che non ci ne sia
nessuno in mezzo

0 è coprto da 1

1 è coprto da 2

2 è coprto da 3

b) $(\mathbb{N}, 1) \rightarrow x \text{ copre } 0 \Leftrightarrow \exists i x \in \text{NON c'è nessun altro elemento in mezzo}$

$\forall x 0 < x \Leftrightarrow x \neq 0 \rightarrow$ ma 0 è uguale a 0 stesso, quindi
nessun elemento copre 0

1 è coprto da tutti e soli i numeri primi

↳ ESEMPIO:

Se prendo un certo numero primo p , di certo 1 | p

Se prendo un certo $x \in \mathbb{N} \cdot 1|x \wedge x|p \rightarrow x=1 \vee x=p$

$\begin{matrix} m \\ b \\ \downarrow \\ \begin{matrix} a & & \\ \leftarrow & 2 & \end{matrix} \end{matrix} \leftarrow$ prendo un non primo $\rightarrow m = ab$ con $1 < a, b < m$
 $\downarrow \rightarrow m \text{ non copre } 1$

2 è coprto da tutti e soli i numeri divisibili

per due e non per quattro

↳ ESEMPIO: $\frac{1}{2} \rightarrow \frac{1}{2} \text{ non copre } 2 \text{ perché}$

$$\begin{array}{c} 1 \\ | \\ 6 \\ | \\ 2 \end{array}$$

c) (\mathbb{Q}, \leq) Dato che \mathbb{Q} è denso, nessun numero è
coperto da alcun numero

ESEMPIO: Preso $x \in \mathbb{Q} \quad (\forall y \in \mathbb{Q} \setminus \{x\}) (\exists z \in \mathbb{Q}) (x \leq z \leq y \vee y \leq z)$

Esiste sempre un numero z tra x e y

\downarrow
Nessun numero è coperto da nessun
altro numero

RETIColo

P DEVE ESSERE DI ORDINE LARGO

(S, p) è un reticolo $\Leftrightarrow (\forall a, b \in S)(\exists \sup_{(S,p)}(\{a, b\}) \wedge \exists \inf_{(S,p)}(\{a, b\}))$

- Se a e b sono confrontabili, ad esempio se $a \leq b$, allora $\sup_{(S,p)}(\{a, b\}) = \{b\}$ Dopo aver detto tutti i maggioranti di $\{a, b\}$ ma non che tutte le basi siano il sup è proprio $b \rightarrow$ gli altri maggioranti sarebbero detti basi

- Nel caso in cui abbiamo:

$S = \mathbb{N} \cup \{x\}$, per tutti gli elementi di \mathbb{N} poniamo trovare il sup e l'inf perché gli elementi sono confrontabili

Ma, se tutti i numeri n sono più grandi di 0 , non poniamo confrontare x con altri numeri

$\hookrightarrow \sup_{(S,p)}(\{0, x\})$ perché solo x è confrontabile con x , quindi non ci sono maggioranti

- Dato l'insieme $(P(S), \subseteq)$, con $t, u \in P(S)$

• $\sup_{(S,p)}(\{t, u\}) = t \cup u$

• $\inf_{(S,p)}(\{t, u\}) = t \cap u$ COME SI DEMOSTRA?
t e u è un minorante?

Si, dato che $t \cap u \subseteq t \wedge t \cap u \subseteq u$, di conseguenza

$t \cap u \in \text{MINOR}(\{t, u\})$

E' IL PIÙ
GRANDE
DEL MINOR?

Basta $x \in \text{MINOR}(\{t, u\})$, cioè $x \subseteq t \wedge x \subseteq u$, allora $x \subseteq t \cap u$. Di conseguenza $t \cap u = \inf_{(S,p)}(\{t, u\})$

Quindi $(P(S), \subseteq)$ è un reticolo ed è completo dato che ogni parte di $P(S)$ ha sup e inf

\hookrightarrow Se $t \subseteq P(S)$, $\inf(t) \in t$

$\sup(t) = t$

- Presso (\mathbb{N}, \leq) , questo è un reticolo, è limitato perché 1 è il minimo e ∞ è il massimo, ma non è completo
- Presso $(\mathbb{N} \setminus \{0\}, \leq)$, questo non è un reticolo limitato perché $\exists \sup(2\mathbb{N})$
una parte che non ha sup
- (\mathbb{Q}, \leq) non è limitato e non è nemmeno completo perché non ha sup, ma è un reticolo perché tutti gli elementi sono confrontabili

PRINCIPIO DI DUALITÀ (PER I RETICOLI)

Sia (S, p) un reticolo, dico (S, \bar{p}) il reticolo
duale di (S, p) .

Se E è un enunciato sui reticolati, dico enunciato
duale (\bar{E}) l'enunciato che si ottiene cambiando in
 E tutti i p con \bar{p} , i " \wedge " con " \vee " e " \vee " con " \wedge ".
Sono i sup e inf \rightarrow NON I CONNESSIONI

TEOREMA (PRINCIPIO DI DUALITÀ PER I RETICOLI)

Se E è una formula solida per ogni reticolo, allora
anche \bar{E} lo è.

DIM

Se E è solida per ogni reticolo, allora E è solida
anche per (S, \bar{p}) → dato che (S, \bar{p}) è comunque un reticolo
ma in (S, \bar{p}) gli inf sono i sup di (S, p) e viceversa,
per cui E riferito a (S, \bar{p}) è esattamente \bar{E}
riferito a (S, p)

Possiamo, così, risparmiare molto tempo nelle dimostrazioni dei teoremi sui reticolati.

TEOREMA

In un reticolo, ogni elemento minima è minima

50

DIM

Sia m un elemento minima e $x \in S$. Prendi l'inf di $\{m, x\}$.

Poiché $(m \wedge x) \leq m$ ma m è minima - ha che $m \leq x$,

ovvero $m \leq x \rightarrow \max_{\text{PIÙ PRECISO DI } m} \in \text{l'INF DI } \{m, x\}$, quindi $\max_{\text{PIÙ PRECISO DI } m} \in \text{l'INF DI } \{m, x\}$ è il minimo.

↳ m è il minimo perché confrontabile con ogni $x \in S$

Per il principio di dualità, posso scrivere che:

In un reticolo, ogni elemento minima (rispettivamente massima) è minima (rispettivamente massima)

TEOREMA

Sia (S, \leq) un reticolo. Allora, ogni parte finita di S ha inf e sup in (S, \leq)

DIM ← PER IL PRINCIPIO DI DUALITÀ POSSANO LIMITARSI A INF

1) Siamo a, b parti finite di S . Allora,

$\text{MINOR}(a \cup b) = \text{MINOR}(a) \cap \text{MINOR}(b)$

→ DII (1) Prende $x \in \text{MINOR}(a \cup b) \rightarrow x \leq a \cup b$

O ANCHE POSSANO DEDUCERLO PER ESTENSIONALITÀ
X $\in \text{MINOR}(a \cup b) \leftrightarrow (\forall y \in a \cup b)(x \leq y)$ ma ciò significa che x è minore o uguale di tutti gli elementi di a e di tutti gli elementi di b .
cioè $x \in \text{MINOR}(a) \cap x \in \text{MINOR}(b)$

(2) Vole anche il verso contrario per le stesse motivazioni a ritroso, quindi:

$x \in \text{MINOR}(a \cup b) \leftrightarrow x \in \text{MINOR}(a) \cap x \in \text{MINOR}(b)$

2) Sia $m = \inf_{(S, \leq)}(a)$, se esiste.
 Allora $\text{MINOR}(a) = \text{MINOR}(\{m\}) = \{x \in S \mid x \leq m\}$
 ↳ Dato che m è più piccolo di ogni elemento di a ,
 è ovvio che per trasversalità ogni minorante di m lo
 è anche di a e viceversa.

3) Siamo $m_1 = \inf(a)$ e $m_2 = \inf(b)$, se esistono.

Allora, per 1) e 2) ho che:

$$\begin{aligned}\text{MINOR}(a \cup b) &= \text{MINOR}(a) \cap \text{MINOR}(b) = \\ &= \text{MINOR}(\{m_1\}) \cap \text{MINOR}(\{m_2\}) = \text{MINOR}(\{m_1, m_2\})\end{aligned}$$

✓ I minoranti di $a \cup b$ non sono altro che i minoranti della coppia con cui m_1 e m_2

9) Inclusione sull'ordine di una parte finita t di S)

↪ Se $|t| = 1$, allora è ovvio che quell'unico elemento
 è sia inf che sup. $\rightarrow t = \{x\}, \inf(t) = \{x\} = t$

↪ Se $|t| > 1$ e chiamiamo m l'ordine di t , $m = |t|$

Quindi $m > 1$ e sia zero l'asserto per tutte le parti
 di S di ordine $m-1$.

• Prendo $x \in t$, quindi $t = v \cup \{x\}$

Di conseguenza, $v = t \setminus \{x\}$ e $|v| = m-1$. Quindi, per
 l'ipotesi di induzione prendo $m = \inf(v)$.

Allora per il punto 3):

$$\text{MINOR}(t) = \text{MINOR}(v \cup \{x\}) = \text{MINOR}(\{m, x\})$$

↪ Poiché siamo in un reticolo, $\text{MINOR}(\{m, x\})$
 ha massimo.

$\rightarrow \{m, x\} \in \text{RETIColo}$

Di conseguenza t ha inf.

ATTENZIONE!

Se prendiamo una parte infinita l'asserto non vale,
 infatti in (\mathbb{N}, \leq) , \mathbb{N} non ha il sup.

DATO CHE ABBIANO DI OLTRE
 L'ASSERTO PER UNA PARTE
 DI ORDINE m DI UNA DI
 ORDINE $m-1$, L'ASSERTO
 VALE PER TUTTA PARTE FINITA

PROPRIETA' DI (S, \wedge, \vee)

Già saffiamo che (S, \wedge, \vee) è una struttura algebrica tra

PROPRIETA' COMMUTATIVA

In (S, \wedge, \vee) vale la proprietà commutativa, infatti:

DIM Preso $x, y \in S$:

$$x \wedge y = \inf_{(S, P)} (\{x, y\}) = \inf_{(S, P)} (\{y, x\}) = y \wedge x. \text{ Inoltre,}$$

$$x \vee y = \sup_{(S, P)} (\{x, y\}) = \sup_{(S, P)} (\{y, x\}) = y \vee x$$

Quindi vale la proprietà commutativa per \vee e \wedge .

Inoltre vale sempre che:

$$\cdot x \leq (x \vee y) \quad e \quad y \leq (x \vee y)$$

$$\cdot (x \wedge y) \leq x \quad e \quad (x \wedge y) \leq y$$

PROPRIETA' ASSOCIATIVA

Le le proprietà associative per \vee e per \wedge in (S, \wedge, \vee)

DIM Considero \vee .

sono elementi

Siamo $x, y, z \in S$. Vale $(x \vee y) \vee z = x \vee (y \vee z)$. Inoltre vale che
 $(y \vee z) \leq (x \vee (y \vee z))$; Per lo stesso motivo vale:

$y \leq (y \vee z) \leq z$; Quindi per transitività vale che:

$$y \leq (x \vee (y \vee z)) \leq z \leq (x \vee (y \vee z)),$$

Allora $(x \vee y) \leq (x \vee (y \vee z))$, vale a dire $((x \vee y) \vee z) \leq (x \vee (y \vee z))$,

Analogamente ho che $(x \vee (y \vee z)) \leq ((x \vee y) \vee z)$ e, per

l'assimmetria, ho che $(x \vee (y \vee z)) = ((x \vee y) \vee z)$.

Inoltre, per il principio di dualità, anche \wedge è associativa.

PROPRIETA' DI ASSORBIMENTO

$$(\forall x, y \in S)((x \vee (x \wedge y) = x) \wedge (x \wedge (x \vee y) = x))$$

$\wedge x \text{ ASSORBE } (x \wedge y)$

PROPRIETA' DI ITERATIVITA' (O IDEMPOTENZA)

$$(x \wedge x = x \wedge x \vee x = x) \rightarrow \begin{array}{l} \text{SEGUONO PROPRIETÀ} \\ \text{DI ASSORBIMENTO} \end{array}$$

STRUTTURE ALGEBRICHE CON COMMUTATIVITA'

ASSOCIAITVITA' E ASSORBIMENTO SONO RETICOLI

Allora consideriamo (S, p) come reticolo (con $\text{PEOL}(S)$)

\wedge_p e \vee_p sono gli inf e sup definiti attraverso la relazione d'ordine \rightarrow sono operazioni su S che dipendono da p
e si esprimono con \wedge_p e \vee_p

- Quindi, in (S, \wedge_p, \vee_p) non le commutativita', l'associativa' e l'assorbimento, e notiamo che queste strutture algebriche, con queste proprie', in realtà sono dei reticoli.

TEOREMA ↴

Sia S un insieme non vuoto, sia π l'insieme delle relazioni d'ordine p su S tali che:

$p \in \pi \Leftrightarrow (S, p)$ è un reticolo. *INSTEDE IL E' FATTO SOLO DA RELAZIONI D'ORDINE CHE DEFINISCONO UN RETICOLI*

Sia b l'insieme delle copie ordinate di operazioni binarie interne di S . Tali che:

una certa $(\alpha, \beta) \in b \Leftrightarrow$ sono associative, commutative e in (S, α, β) non la legge di assorbimento.

Allora l'applicazione che: $p \in \pi \mapsto (\wedge_p, \vee_p) \in b$ è biettiva.

↳ Possiamo parlare indistintamente di reticolo nel senso dell'ordine e di reticolo nel senso di struttura algebrica (e con quelli, i due sentiti).

PER FAR NESSUNO
END C'È ESTATE

D14 Voglio trovare l'inverso di \wedge per $\rightarrow (\wedge, \vee) \in b$

Sia $(\wedge, \vee) \in b$. Definisco: DA QUESTO SEGUE CHE
 $(\forall x, y \in S)(x \wedge y \Leftrightarrow x = x \wedge y) \rightarrow x \wedge y = (x \wedge y) \vee y =$ PER ASSORBIMENTO
 $x \wedge y \quad$ QUINDI SICURAMENTE VALE CHE
 $x \wedge y \Leftrightarrow x = x \wedge y \Leftrightarrow y = x \vee y^*$

1) \wedge è d'ordine largo?

- $x = x \wedge x$ per l'iteratività. Dunque $(\forall x \in S)(x \wedge x)$, quindi \wedge è riflessiva
- Se $x = x \wedge y$ e $y = y \wedge x$, allora $x = x \wedge y \wedge y = y \wedge x = y$, quindi \wedge è antisimmetrica
- Se $x \wedge y \wedge y \wedge z$, $x = x \wedge y \wedge y = y \wedge z$ Quindi vale che $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$, quindi \wedge è transitivo

2) Vogliamo che $\forall x, y \in S$, $\inf_{(S, \wedge)}(\{x, y\}) = x \wedge y$ e che $\sup_{(S, \wedge)}(\{x, y\}) = x \vee y$ cioè sto appurando f a \wedge

Per assorbimento $(x \wedge y) \vee x = x$, ovvero, per definizione con \vee , ha $\cdot (x \wedge y) \wedge x$. Questo perche' PRENDIAMO $(x \wedge y) \wedge x = y^*$

Alla stessa modo anche $\cdot (x \wedge y) \wedge y$ vale.

Dunque $x \wedge y \in \text{MINOR}_{(S, \wedge)}(\{x, y\})$ Punto $z \in \text{MINOR}_{(S, \wedge)}(\{x, y\})$.

Cioè vale $z \wedge y \wedge z \wedge x$, di conseguenza $z = z \wedge y \wedge z = z \wedge x$.

$z = z \wedge x$, quindi $z = z \wedge x = (z \wedge y) \wedge x = z \wedge (x \wedge y)$.

Per definizione, quindi, $z \wedge (x \wedge y)$, cioè:

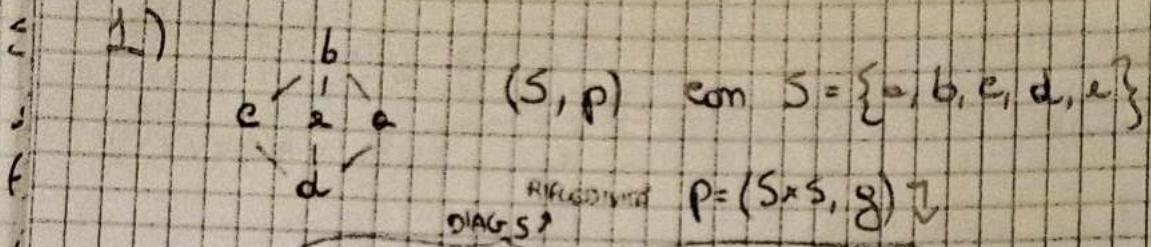
$$x \wedge y = \inf_{(S, \wedge)}(\{x, y\}).$$

Analogamente si puo' dimostrare per \sup .

Allora dimostriamo che $(\wedge, \vee) \in b \rightarrow$ per i

l'inverso di f , infatti applicando queste funzioni a poi f riotteniamo gli stessi \sup e \inf

Correzione esercizi 25/11/2021 (LEZIONE 27)



$$g = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (a, c), (a, d), (a, e), (b, c), (b, d), (b, e), (c, d), (c, e), (d, e)\}$$

Per far vedere che (S, p) è un reticolo dobbiamo vedere se esiste il sup e l'inf per tutte le copie di 8

$\bullet \text{INF}_{(S,p)}(\{a, c\}) = d$

\hookrightarrow CIOE $(c, a), c$
NON HA PECHE I
ELEMENTI DI (c, a)
E' d, QUINDI (S,p)
E' UN RETICOLO

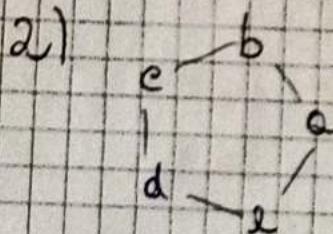
$\bullet \text{MAGGIOR}_{(S,p)}(\{d, e\}) = \text{MAGGIOR}_{(S,p)}(\{e\})$

\downarrow
 $\min(\{a\}) = a$

\hookrightarrow SE $a > d$

ALLORA C

ETTICOLO CHE $\rightarrow q \cdot x \wedge \neg q \cdot x = q \cdot x$
PERCHE' SE $x \in Q$ ALLORA E'
ANCHE MAGGICRE SI E' PERCHE'
 $d < e$



I minoranti di (e, a) sono solo e ,
stessa cosa anche per (a, a)

\hookrightarrow Quindi l'inf è sempre a

\hookrightarrow CIOE', I MINORANTI SONO TUTTI GLI ELEMENTI TALI CHE $x \leq a$ E' $x \in Q$

RICAPITO DELLA SCORSA VOLTA

$(S, p) \rightsquigarrow (S, \wedge_p, \vee_p) \rightarrow$ STESSO RETICOLO MA IN MODO DIVERSO

ESEMPIO:

- $(P(S), \subseteq) \rightsquigarrow (P(S), \cap, \cup)$

$\text{INF}_{(P(S), \subseteq)}(\{x, y\}) = x \cap y$

ISOMORFISMO TRA RETICOLI

Sia (S, \wedge, v) un reticolo e (S', \wedge', v') un'altra reticolo.

Se funzione $f: S \rightarrow S'$ si dice isomorfismo delle strutture algebriche (S, \wedge, v) in (S', \wedge', v') se f è biettiva e tale che:

$$(\forall x, y \in S) (f(x \wedge y) = f(x) \wedge' f(y) \wedge f(x \vee y) = f(x) \vee' f(y))$$

EGO CHE SI PARLA DI STRUTTURE ALGEBRICHES CON LE OPERAZIONI, L'ISOMORFISMO DEVE PRESERVARE PER ENTRAMBI LE OPERAZIONI

Se, invece, vediamo i reticolati come strutture ordinate (S, p) e (S', p') , allora f si dice isomorfismo se e solo se $x \leq y \Leftrightarrow f(x) \leq' f(y)$ ed f è una funzione biettiva.

TEOREMA → FAR L'ISOMORFISMO DI RETICOLI E' UNA SISTRAURE ALGEBRICA O STRUTTURA ORDINATA E' LA STESSA COSA

Siamo (S, \wedge, v) e (S', \wedge', v') reticolati e sia $f: S \rightarrow S'$ biettivo.

f è un isomorfismo tra (S, \wedge, v) e (S', \wedge', v') se e solo se f è un isomorfismo tra $(S, p_{(x,y)})$ e $(S', p'_{(x,y)})$.

DIM

Siamo (S, p) e (S', p') reticolati.

(\leftarrow) Sia f un isomorfismo tra (S, p) e (S', p') , ovvero tale che $x \leq y \Leftrightarrow f(x) \leq' f(y)$.

(S, p) lo possiamo anche vedere come (S, \wedge_p, v_p)

(S', p') lo possiamo anche vedere come $(S', \wedge'_{p'}, v'_{p'})$

VOLGONO FAR VEDERE CHE QUESTO E' ANCHE UN ISOMORFISMO TRA STRUTTURE ALGEBRICHES

CIO'E CHE CONSERVA LE OPERAZIONI

Dimostriamo che si conserva \wedge

• Sappiamo che $\forall x, y \in S$ valgono $(x \wedge_p y) p x$ e $(x \wedge_p y) p y$

CIO'E' MINORE DI ENTRAMBI

Essendo f un isomorfismo, posso fare f a entrambi le relazioni e otto che:

$(X \wedge_p Y) p X \leftrightarrow f(X \wedge_p Y) p' f(X)$ e ho che
 $(X \wedge_p Y) p Y \leftrightarrow f(X \wedge_p Y) p' f(Y)$, cioè sto dicendo
che $f(X \wedge_p Y) \in \text{MINOR}_{(S, P)}(\{f(X), f(Y)\})$
 $f(X \wedge_p Y)$ è l'inf di (S, P) ?

• Ora devo forse vedere che $f(X \wedge_p Y)$ è il più grande
dei minoranti, quindi prendo un certo z tale che
 $z \in \text{MINOR}_{(S, P)}(\{f(X), f(Y)\})$.

Cioè sto prendendo z tale che $z p' f(X)$ AND $z p' f(Y)$

DATO CHE E' BIETTIVA ESSENDO
UN ISOMORFISMO

Essendo la funzione suriettiva, posso trovare un
certo $w \in S$ tale che $f(w) = z$.

Quindi ho che $f(w) p' f(X)$ AND $f(w) p' f(Y)$.

Visto che f è un isomorfismo, ho che vale:

$w p X$ AND $w p Y$.

Ma questa cosa vuol dire che $w p X \wedge_p Y \rightarrow$ SE E' PIÙ
PICCOLO DI
ENTRAMBI
ALLORA E' PIÙ
PICCOLO DELL'
INF TRA I
DUE

Applicando di nuovo f ho che $f(w) p' f(X \wedge_p Y)$, ma
dato che $f(w) = z$ allora sto dicendo che vale
 $z p' f(X \wedge_p Y)$, ovvero che $f(X \wedge_p Y) = \text{INF}_{(S, P)}(f(X), f(Y)) =$

ISOMORFISMO $\rightarrow = f(X) \wedge_p f(Y)$

ALLO STESSO MODO SI PUO' DEMONSTRARE
CHE $f(X \vee_p Y) = f(X) \vee_{P'} f(Y)$

HO DIMOSTRATO CHE
DALL'ISOMORFISMO TRA STRUTTURE
D'ORDINE HO L'ISOMORFISMO
DELLE STRUTTURE ALGEBRAICHE
ASSOCIATE

(\rightarrow) Sia f un isomorfismo tra (S, \wedge_p, \vee_p) e $(S', \wedge_{P'}, \vee_{P'})$

Premolo $x, y \in S$ tali che $x p y$.

\rightarrow VOGLIO DEMONSTRARE CHE
VALE $x p y \leftrightarrow f(x) p' f(y)$

* \rightarrow Per definizione ho che $X = X \wedge_p Y \rightarrow$ SE X E' PIÙ PICCOLO TRA X E Y,
ALLORA E' L'INF TRA I DUE

Applico f e, essendo suriettiva, ho che:

$f(X) = f(X \wedge_p Y)$, ma essendo f un isomorfismo

ho che $f(X \wedge_p Y) = f(X) \wedge_{P'} f(Y)$

\rightarrow Per definizione ho che $f(X) p' f(Y) \rightarrow$ PER DEMONSTRARE L'ALTRO VERSO,
 $f(X) p' f(Y) \rightarrow X p Y$ SEGNA LO
STESO ARGOMENTO AL
CONTARIO, ESSENDO
SURIETTIVA ALLORA ANCHE LE
PRESTIMMAGINI SONO UGUALI

\rightarrow DI $\wedge_{P'}$

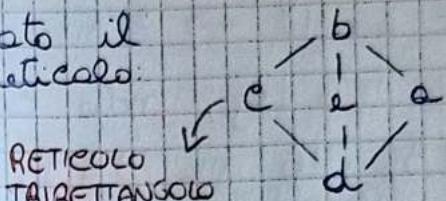
E' UN SOTTOINSIEME
DI S NON VUOTO

SOTTORETICOLI

Sia (S, \wedge, \vee) un reticolo e sia $t \in P(S) \setminus \{\emptyset\}$
Se t è una parte chiusa rispetto a \wedge e \vee ,
 t è detto sottoreticolo di (S, \wedge, \vee)

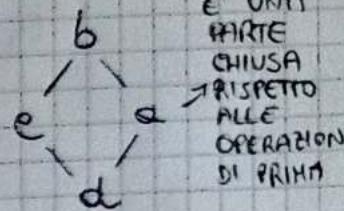
ESEMPIO:

- Dato il reticolo:



RETIColo
TRIETTANGolo

Il reticolo:

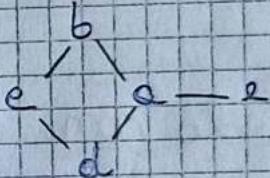


E' UNA
PARTe
CHIUSA
RISPETTO
ALLE
OPERATION
DI PRIMA

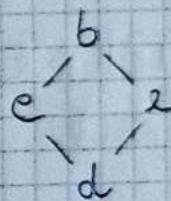
è un suo sottoreticolo

- Non è un reticolo perché: $\exists \sup(\{b, e\})$

- Dato il reticolo:



e il reticolo:



Pur entrambi essendo entrambi dei reticolati, il secondo non è un sottoreticolo del primo perché nel primo abbiamo che $b \wedge e = a$, mentre nel secondo $b \wedge e = \perp$

GO ANCHE: $e \wedge a = e$ MENTRE $e \wedge a = d$

INTERVALLO (CHIUSO)

Sia (S, ρ) un insieme ordinato e $p \in \text{COL}(S)$.

$I \subseteq S$ si dice intervallo (chiuso) di (S, ρ) se:

$$(\forall x, y \in I)(\forall z \in S)(x \rho z \text{ AND } z \rho y \rightarrow z \in I)$$

PER OGNI
COPPIA DI
ELEMENTI CHE
STANNO IN
I, ALLORA EL
SONO TUTTI
QUELLI IN
MEZZO

ESEMPIO:

- In (\mathbb{N}, \leq) $\{1, 2, 3\}$ è un intervallo

$\{1, 3\}$ non è un intervallo \Rightarrow NON c'e' 2
che sta in
mezzo

- (\mathbb{Q}, \leq) $\{1, 2\}$ non è un intervallo perché, dato che \mathbb{Q} è un insieme denso, tra due numeri ne me sono infiniti in meno
- (\mathbb{N}, \mid) $\{m \in \mathbb{N} \mid m \mid m\}$ è un intervallo
 - $\hookrightarrow \forall x, y \in I, \exists z \in I : x \mid z \wedge z \mid y \rightarrow x \mid y$
 - Se ho $I = \{1, 2, 4, 6, 12\}$, noto che c'è 3 che: $1|3, 3|6$ ma $3 \notin I$, quindi I non è un intervallo
- (\mathbb{Q}, \mid) non ci sono intervalli perché ogni numero è divisibile da ogni numero (tranne 0)

PROPOSIZIONE

Gli intervalli di un reticolo sono dei sotto reticolati

ESEMPIO:

- In (\mathbb{N}, \mid) , $\{1, 2, 3, 4, 6, 12\}$ è un sotto reticolo

ELEMENTO NEUTRO DI UN RETICOLATO LIMITATO

Se (S, \wedge_p, \vee_p) è un reticolo limitato, con $M = \max(S)$ e $m = \min(S)$, allora M è l'elemento neutro di \wedge_p e m è l'elemento neutro di \vee_p

DIM → Facciamo con il massimo si dimostra con il minimo

c'è il
massimo e il
minimo del
reticolo

Prendo $x \in S$

(\rightarrow) Considero $M \wedge_p x$, per definizione di massimo, vale $x \leq M$

Per definizione di \wedge_p ho che $M \wedge_p x = x \rightarrow M$ è neutro

(\leftarrow) Se M è l'elemento neutro, allora:

$(\forall x \in S)(M \wedge_p x = x) \rightarrow$ Per definizione $(\forall x \in S)(x \leq M) \rightarrow M$ è il massimo

RETICOLO COMPLEMENTATO

Sia (S, \wedge, \vee) un reticolo limitato. Il reticolo si dice complementato se:

$$(A x \in S)(\exists y \in S)(x \wedge y = \text{MIN}(S) \text{ AND } x \vee y = \text{MAX}(S))$$

Inoltre, y si dice complemento di x se

x si dice complementato da y

ESEMPIO:

- Un insieme totalmente ordinato con più di due elementi non è complementato

$\hookrightarrow (IN, \leq)$ non lo è perché infinito
non ha nemmeno il massimo

• c è il successivo
non esiste un complemento
di b perché $a \wedge b = \text{MIN}(S)$
ma $a \vee b \neq b$ che non è il massimo di S

- In (IN, \leq) , se prendo m elementi, non ci sono divisori comuni con $m+1$ divisori

$\hookrightarrow m \mid m+1 - 1$, quindi per ogni elemento di IN
 \downarrow si ha il $\text{MIN}(S)$

Ma $(\forall m \neq 0)(\exists \neg m)(m \vee m = 0)$ quindi (IN, \leq) è un reticolo limitato ma non complementato

- e è a come complemento e b è come complemento d

TEOREMA → QUANDO SE DUE ELEMENTI SONO COMPLEMENTATI MA NON SONO MINIMO E MASSIMO ALLORA QUESTI DUE ELEMENTI NON SONO CONFRONTABILI

Due elementi sono complementati e confrontabili se

e solo se sono il minimo e il massimo

DIM

\leftarrow MIN e MAX sono chiaramente confrontabili e complementari tra loro

\rightarrow (COMPLEMENTARI + CONFRONTABILI) $\Rightarrow (x \wedge y = \text{MIN} + x \vee y) \rightarrow x \wedge y = x = \text{MIN}$

DISTRIBUTIVITA' DEL RETICOLO

Un reticolo (S, \leq) si dice distributivo se:

$$(\forall a, b, c \in S) (a \wedge_p (b \vee_p c)) = (a \wedge_p b) \vee_p (a \wedge_p c) \text{ AND}$$

$$\text{AND } a \vee_p (b \wedge_p c) = (a \vee_p b) \wedge_p (a \vee_p c))$$

Si puo' dimostrare che se vale che $a \wedge_p (b \vee_p c) = (a \wedge_p b) \vee_p (a \wedge_p c)$ allora vale anche l'altro \rightarrow quindi solo questa prima e la condizione necessaria affinché si ottenga la distributività.

•

TEOREMA

Se (S, \leq) e un reticolo distributivo, allora ogni complemento e unico.

DIM

Sia $x \in S$ un elemento complementato. Siamo y e z complementi di x .

Suppongo (S, \leq) limitato. Dico $M = \text{MAX } S$ e $m = \text{MIN } S$

E' vero che:

$y \in M$ è un complemento

$y \in z$ sono elementi che sono complementi

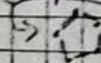
$y \in z$ è un complemento

$$\begin{aligned} y &= y \wedge_p M = y \wedge_p (x \vee_p z) = (y \wedge_p x) \vee_p (y \wedge_p z) \\ &= y \wedge_p z \end{aligned}$$

Cioè $y \leq z$, analogamente $z \leq y$, dunque $y = z$

CRITERIO DI DISTRIBUTIVITA' DI BIRKHOFF

Un reticolo e distributivo se e solo se non contiene sottoreticolli isomorfi al reticolo triviettante o al reticolo pentagonale



NO DIM

Correzione esercizi 26/11/2021

(LEZIONE 28)

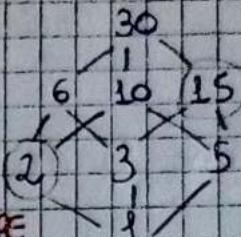
2) (S, \leq) è (IN, \leq) è complementato? \rightarrow

CIOE', SE $\forall m, \exists n$ HO
CHE $m \leq n$, $n = m + d$
 $\in m \wedge n, m = 1 \rightarrow$
MAX E
MIN
DI S

$$S = \{m \in \mathbb{N} \mid m \mid 30\} = \{1, 2, 3, 5, 6, 10, 15, 30\}$$

Il reticolo

disegnato sono:



CHI È IL COMPLEMENTARE
DI 2?

IL SUP DELLA
DIVISIONE \rightarrow 30

- Esiste $x \in S$ tale che $2 \vee x = 30$?

Dobbiamo trovare x tra gli elementi non confrontabili a 2 nel massimo

Infatti, se $x = 6$, il minimo dei maggioranti è 6

↳ Quindi dobbiamo cercare tra gli elementi non confrontabili

Se $x = 15$ allora $2 \vee 15 = 30$

L'INF DELLA DIVISIONE \rightarrow 30

- Inoltre, esiste $x \in S$ tale che $2 \wedge x = 1$, e notiamo che x è proprio 15 $\rightarrow 2 \wedge 15 = 1$

Quindi 15 è complementare di 2

Notiamo che: • 15 è 2 sono complementari

• 3 è 10 sono complementari

• 5 è 6 sono complementari

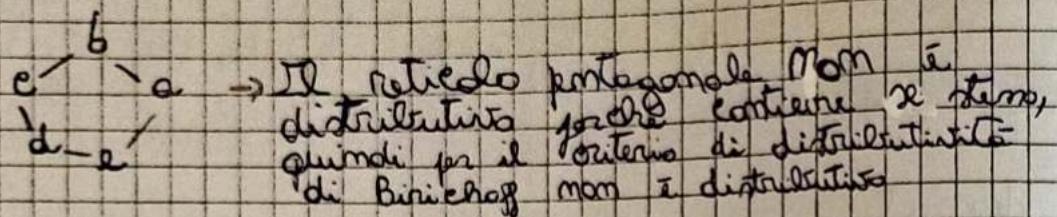
PERCOME MINIMO E MASSIMO \nwarrow • 30 e 1 sono complementari

TUTTI GLI ELEMENTI SONO COMPLEMENTARI

IL RETICOLO E' COMPLEMENTATO

• IL RETICOLO PENTAGONALE È DISTRIBUTIVO.

Consideriamo il reticolo pentagonale:



Impossibile mostrare che c'è uno termo di elementi che:

$$\begin{array}{l} \bullet c \wedge (d \vee e) = c \wedge b = c \\ \quad \quad \quad (c \wedge d) \vee (c \wedge e) = d \vee e = d \end{array} \quad \left. \begin{array}{l} \text{NON È DISTRIBUTIVA} \end{array} \right\}$$

DISTRIBUTIVITÀ DI RETICOLI E SOTTORETICOLI

- Se il reticolo è distributivo, tutti i suoi sottoreticolari sono distributivi
- Se il reticolo non è distributivo, tutti i sottoreticolari non sono distributivi

È RETICOLO BOOLEANO

Sia (S, p) un reticolo booleano. Il reticolo booleano è un reticolo distributivo e complementato

ALGEBRA BOOLEANA (o ALGEBRA DI BOOLE)

La struttura alg. $(S, \wedge_p, \vee_p, ')$ è chiamata algebra di Boole

↓
E' il reticolo booleano visto come struttura algebrica

↓
WEDGE VEL
OPERAZIONI BINARIE INTERNE

↓
COMPLEMENTAZIONE (UN APSTROFO)
↓
OPERAZIONE UNARIA INTERNA

PROPRIETA' DELL' ALGEBRA BOOLEANA

- 1) \wedge_p e \vee_p sono commutative
 - 2) \wedge_p e \vee_p sono assosiative
 - 3) Tra \wedge_p e \vee_p vengono le leggi di assorbimento
 - 4) Vale la distributività
 - 5) \wedge_p e \vee_p hanno gli elementi neutri. In particolare
1 è l'elemento neutro di \wedge_p perché $1 \wedge x = x$ e il massimo
0 è l'elemento neutro di \vee_p perché $0 \vee x = x$ e il minimo
 - 6) Vale che: POSSO METTERE L'APICE PERCHÉ SO CHE PER OGNI ELEMENTO, IL SUO COMPLEMENTATO È UNICO DEFINISCO "COME IL COMPLEMENTARE"
- $$(\forall x \in S)(x \vee_p x' = 1 \text{ AND } x \wedge_p x' = 0)$$

Absiamo già visto che è possibile passare, grazie a un teorema, da un reticolo Booleano all'algebra di Boole e viceversa.

$$\hookrightarrow (S, \rho) \text{ RETICOLO BOOLEANO} \iff (S, \wedge_p, \vee_p, ') \text{ ALGEBRA BOOLEANA}$$

ESEMPIO:

• $(P(S), \cap, \cup, \setminus)$ è un'algebra di Boole

ANELLO BOOLEANO A UN ANELLO BOOLEANO POSSO DEFINIRE UN RETICOLO BOOLEANO

$(\mathbb{Q}, +, \cdot)$ è un anello Booleano se è un anello unitario e si ha che $(\forall x \in \mathbb{Q})(x^2 = x)$

$\hookrightarrow (\mathbb{Q}, \cdot)$ è un monoido \rightarrow ESISTE L'ELEMENTO NEUTRO DI \cdot .

ESSENDO UN ANELLO, SI HA CHE: $(\mathbb{Q}, +)$ È UN GRUPPO ABELIANO

(\mathbb{Q}, \cdot) È UN SEMIGRUPPO

VALE LA DISTRIBUTIVITÀ DI \cdot RISPETTO A $+$

SI È DIMOSTRATO CHE GLI ANELLI BOOLEANI SONO COMMUTATIVI

$\hookrightarrow (\mathbb{Q}, \cdot)$ È COMMUTATIVO MENTRE $(\mathbb{Q}, +)$ LO È GIÀ PER DEFINIZIONE

INOLTRE, NEGLI ANELLI BOOLEANI, $(\forall x \in \mathbb{Q})(2x = 0)$

$$(\forall x \in \mathbb{Q})(x + x = 0)$$

RETICOLO BOOLEANO E ANELLO BOOLEANO

SE CI PONIAMO NEL CASO CONCRETO DI $(\{0,1\}, \wedge, \vee, \neg)$,
 IL \cdot E' L'INTERSEZIONE,
 MA IL $+$ NON E' PROPRIO
 L'UNIONE

Sia $(\alpha, +, \cdot)$ un anello booleano \rightarrow CONCRETO

Definisco che $(\forall x, y \in \alpha)(x \cdot p \cdot y \leftrightarrow x \cdot y = x)$

Allora, (α, p) è un reticolo booleano

DIM (\rightarrow) ANELLO BOOLEANO \rightarrow RETICOLO BOOLEANO

- p è una relazione di ordine largo?

1) p è riflessiva, infatti, essendo l'anello booleano,

$$x \cdot x = x \text{ quindi per l'ipotesi vale } x \cdot p \cdot x$$

2) p è assimmetrica, infatti:

$$x \cdot p \cdot y \text{ AND } y \cdot p \cdot x \leftrightarrow x \cdot y = x \text{ AND } y \cdot x = y, \text{ ma}$$

dato che l'anello booleano è commutativo

$$\text{allora } x = x \cdot y = y \cdot x = y, \text{ cioè } y = x$$

3) p è transitiva, infatti:

$$x \cdot p \cdot y \text{ AND } y \cdot p \cdot z \rightarrow x \cdot y = x \text{ AND } y \cdot z = y$$

$$\text{Allora } x \cdot z = (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot y = x, \text{ cioè } x \cdot p \cdot z$$

- Affinché $(\alpha, +, \cdot)$ sia un reticolo, dobbiamo dimostrare che per ogni coppia di elementi di α ci sono sup e inf e devo vedere chi sono
- \hookrightarrow Voglio dimostrare che $x \vee_p y = x + y + x \cdot y$, e $x \wedge_p y = x \cdot y$

1) $x + y + x \cdot y$ è un maggiorante, infatti:

$$\begin{aligned}
 &\text{ALLO STESSO MODO} \quad x \cdot (x + y + x \cdot y) = x^2 + x \cdot y + x^2 \cdot y = x + x \cdot y + x \cdot y = x, \text{ cioè} \\
 &\text{DIMOSTRO} \quad x \vee_p y = x + y + x \cdot y, \text{ ovvero } x + y + x \cdot y \text{ è un maggiorante}
 \end{aligned}$$

LA DEMOSTRAZIONE
E' SULLO STESSO
PROCEDIMENTO

2) $x + y + x \cdot y$ è il più piccolo dei maggioranti, infatti:

Preso $z \in \alpha$ tale che $x \cdot p \cdot z$ e $y \cdot p \cdot z$ ho che

$$x \cdot z = x \text{ e } y \cdot z = y. \text{ Di conseguenza avrò che}$$

$$(x + y + x \cdot y) \cdot z = x \cdot z + y \cdot z + x \cdot y \cdot z = x + y + x \cdot y, \text{ cioè vale}$$

$(x + y + x \cdot y) \cdot p \cdot z$, ovvero $x + y + x \cdot y$ è il più piccolo dei maggioranti

• (\mathcal{Q}, ρ) è limitato?

↪ Prendo $x \in \mathcal{Q}$, vale che $0 \cdot x = 0$, cioè $0 \leq x$, cioè 0 è il minimo di (\mathcal{Q}, ρ)

↪ Prendo $x \in \mathcal{Q}$, vale che $x \cdot 1 = x$, cioè $1 \geq x$, cioè 1 è il massimo di (\mathcal{Q}, ρ)

• (\mathcal{Q}, ρ) è distributivo?

↪ Presi $x, y, z \in \mathcal{Q}$, vogliamo dimostrare che:

$$x \wedge_{\rho} (y \vee_{\rho} z) = (x \wedge_{\rho} y) \vee_{\rho} (x \wedge_{\rho} z), \text{ AND } x \vee_{\rho} (y \wedge_{\rho} z) = (x \vee_{\rho} y) \wedge_{\rho} (x \vee_{\rho} z)$$

$$\begin{aligned} (x \wedge_{\rho} y) \vee_{\rho} (x \wedge_{\rho} z) &= (x \cdot y) \vee_{\rho} (x \cdot z) = xy + x^2yz + xz = \xrightarrow{\substack{x^2=y \\ \text{PER LE PROPRIETÀ DI UN ANELLO}}} \\ &= xy + xyz + xz = x \cdot (y + yz + z) = x \wedge_{\rho} (y + yz + z) = x \wedge_{\rho} (y \vee_{\rho} z) \end{aligned}$$

↪ STEPS D'
PROCEDIMENTO
PER IL LISSO

• (\mathcal{Q}, ρ) è complementato?

Se $x \in \mathcal{Q}$, vale che $x \wedge_{\rho} (1+x) = x(1+x) = x+x^2 = x+x = 0$

vale che $x \vee_{\rho} (1+x) = x+1+x = 1$

Quindi $x+1 = x'$ → x' è il complemento di x

• Abbiamo così dimostrato che dall'anello booleano non puoi passare a un reticolo booleano.

RETICOLO BOOLEANO → ANELLO BOOLEANO

(\leftarrow) Dimostreremo che da un reticolo booleano si può passare a un anello booleano

↪ Sia (S, ρ) un reticolo booleano con almeno

due elementi → SERVONO ALMENO DUE ELEMENTI PERCHÉ PER OTTENERE UN ANELLO Hanno bisogno dell'elemento neutro della somma e del prodotto

↪

• Definisco $x+y = (x \wedge_{\rho} y') \vee_{\rho} (x' \wedge_{\rho} y)$ e $x \cdot y = x \wedge_{\rho} y$

Dimostra che $(S, +, \cdot)$ è un anello booleano

• ASSOCIAZIONE

1) DI \cdot : $x \cdot (y \cdot z) = x \wedge (y \wedge z) = (x \wedge y) \wedge z = (x \cdot y) \cdot z$

2) DI $+$: PROCEDIMENTO ANALOGO MA MOLTO LUNGO. SARÀ TRA GLI ESERCIZI DELLA LEZIONE 29

• COMMUTATIVITÀ DI $+$:

$$x+y = (x \wedge y') \vee (x' \wedge y) = (y \wedge x') \vee (y' \wedge x) = (y \wedge x) \vee (y' \wedge x) = y+x$$

CONTRACCITTIVITÀ DI \wedge E \vee

P COMMUTATIVITÀ DI ·

$$x \cdot y = x \wedge_p y = y \wedge_p x = y \cdot x$$

DISTRIBUTIVITÀ DI · SUL VENIRE DI M
SI DEDICA TRAMITE ESEMPI, NEGLI ESEMPI
DELLA LEZIONE 29

C MINIMO E MASSIMO: Definiamo $m = \min(S)$ e $M = \max(S)$

$$x + m = (x \wedge m) \vee (x' \wedge m) = (x \wedge M) \vee (x' \wedge M) = x \vee M = x \rightarrow m = 0_S$$

$$x \cdot M = x \wedge M = x \rightarrow M = 1_S \rightarrow \text{L'UNITÀ DEL } \cdot \text{ È IL MASSIMO}$$

L'UNITÀ DEL \cdot
È IL MINIMO

(-) ANELLO BOOLEANO: $x^2 = x \cdot x = x \wedge_p x = x$

Abbiamo così dimostrato che un'anello booleano, reticolo booleano e algebre di Boole sono strutture equivalenti
→ ANCHE GLI ISOMORFISMI SONO EQUIVALENTI

ESEMPIO:

Sia $S \neq \emptyset$ e consideriamo il reticolo booleano

$(P(S), \subseteq)$. Questo reticolo è corrispondente all'algebra di Boole $(P(S), \cap, 0, ')$

↓

→ SAREBBE S

S MENO QUICCOSA

$(P(S), \subseteq) \leftrightarrow (P(S), \cap, 0, ')$

Presso $X, Y \in P(S)$, $X \cdot Y = X \cap Y \rightarrow$ perche $X \cdot Y = X \wedge_p Y$

$$\begin{aligned} X + Y &= (X \Delta S \setminus Y) \cup (Y \Delta S \setminus X) = (X \setminus Y) \cup (Y \setminus X) = \\ &= X \Delta Y \end{aligned}$$

Quindi l'anello booleano associato è $(P(S), \Delta, \cap)$

TEOREMA DI STONE

Sia $a \neq \emptyset$ e $(a, +, \cdot)$ un'anello booleano.

Allora, esiste $S \neq \emptyset$ tale che:

$(a, +, \cdot) \cong (P(S), \Delta, \cap)$ → TUTTI GLI ANELLI BOOLEANI SONO ISOMORFI A $(P(S), \Delta, \cap)$

→ Inoltre, se a è finito, potrò scegliere S finito non vuoto tale che $(a, +, \cdot) \cong (P(S), \Delta, \cap)$

Il teorema di Stone si affida allo stesso modo per i reticolati booleani con almeno 2 elementi.
→ Sono tutti isomorfi a $(P(S), \subseteq)$

NO DIM

PER PASSARE
DELL'ANELLO AL
RETICOLATO, HA IN
REALTÀ IL TEOREMA
VALE ANCHE SE IL
RETICOLATO HA UN
ELEMENTO

COROLLARI DEL TEOREMA DI STONE

1) Se $(\alpha, +, \cdot)$ è un anello booleano e $|\alpha| = m$
 dove $m \in \mathbb{N}_2$, MENNE $m > 2$ DATO CHE UN ANELLO
BOOLEANO HA ALMENO DUE ELEMENTI
 Allora $(\exists m \in \mathbb{N} \setminus \{0\})(m = 2^m)$

DIM

Essendo un anello booleano isomorfo a $(P(S), \Delta, \cap)$,
 dato che $|P(S)| = 2^m$ allora anche l'anello booleano
 ha $|\alpha| = 2^m$ perché non è un'applicazione biettiva

2) Se (α, p) è un reticolo booleano e $|\alpha| = m$
 dove $m \in \mathbb{N}_1$ MENNE $m \geq 1$

Allora $(\exists m \in \mathbb{N})(m = 2^m)$ LA DIFFERENZA È CHE IL RETICOLO
PUÒ ANCHE AVERE UN SOLO ELEMENTO

3) Due anelli booleani finiti sono isomorfi
 se e solo se hanno lo stesso ordine
↪ PERCHÉ SONO ENTRAMBI ISOMORFI A $(P(S), \Delta, \cap)$

ALGEBRE DI BOOLE E FUNZIONI CARATTERISTICHE

PER RICORDARE PARI DISPARI

- $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\}$
- $X \equiv_2 0 \iff (\exists k \in \mathbb{Z})(X - 0 = 2k)$
- FUNZIONE CARATTERISTICA: dato $t \subseteq S$, $\chi_{t,S}: X \in S \mapsto \begin{cases} 0 & \text{SE } X \in t \\ 1 & \text{SE } X \notin t \end{cases}$

INSIEME DELLE STRINGHE CON 0 ∈ 1

Considerato $m \in \mathbb{N} \setminus \{0\}$, definisco $\alpha = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2 \approx$
≈ stringhe di "0" e "1" di lunghezza m

ESEMPIO:

• $m = 3$ LA TERNA

$([0]_2, [0]_2, [1]_2) \in \alpha$ POSSO VEDERLA COME

$\{\} (0, 0, 1) \in \alpha \approx 001 \in \alpha$

PRODOTTO CARTESIANO
m VOLTE

SOMMA PONTUALE E MOLTIPLICAZIONE PONTUALE
 Sia $X = x_1 \dots x_m$ e $Y = y_1 \dots y_m$ con $x_1, \dots, x_m, y_1, \dots, y_m \in \{0,1\}$

Definisco la somma puntuale $X+Y$:

$$([x_1 + y_1]_2, [x_2 + y_2]_2, \dots, [x_m + y_m]_2)$$

Definisco la moltiplicazione puntuale $X \cdot Y$:

$$([x_1 \cdot y_1]_2, [x_2 \cdot y_2]_2, \dots, [x_m \cdot y_m]_2)$$

ESEMPIO:

$$\cdot ([0]_2, [0]_2, [1]_2) + ([1]_2, [1]_2, [0]_2) = (1, 1, 1)$$

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

$$\cdot 11 + 10 = 01$$

$$\cdot 11 \cdot 10 = 10$$

FUNZIONE CARATTERISTICA E STRINGHE

Prendo l'insieme S tale che $|S| = m$ con $m > 0$

Dato $t \subseteq S$ ho che:

$$\chi_{t,S}: X \in S \mapsto \begin{cases} 0 & \text{SE } X \notin t \\ 1 & \text{SE } X \in t \end{cases}$$

Dunque $\chi_{t,S} \in \{0,1\}^S \approx a$ (stringhe)

ESEMPIO:

$$S = \{1, 2, 3, 4, 5\} \quad e \quad t = \{1, 3, 4\}$$

$$\begin{matrix} \chi_{t,S} \\ \downarrow \\ 1 \end{matrix} \quad \begin{matrix} \downarrow \\ 0 \end{matrix} \quad \begin{matrix} \downarrow \\ 1 \end{matrix} \quad \begin{matrix} \downarrow \\ 1 \end{matrix} \quad \begin{matrix} \downarrow \\ 0 \end{matrix}$$

Quindi ogni funzione caratteristica possiamo vederla come una stringa di "1" e "0" lunga m elementi.

$$\hookrightarrow \chi_{t,S} = 10110$$

ALL'IMMAGINE DEL PRIMO ELEMENTO
 SONO LA PRIMA POSIZIONE, ALL'IMMAGINE
 DEL SECONDO LA SECONDA POSIZIONE ECC.

TEOREMA

Sia $m \in \mathbb{N} \setminus \{0\}$ e $S = \{1, 2, \dots, m\}$

Allora $\varphi: t \in P(S) \mapsto x_{t,S} \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2$ è
un isomorfismo tra: m volte m volte

$(P(S), \Delta, \cap)$ e $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2, +, \cdot)$ con
 $+$ e \cdot somma e prodotto funzionale

NO DIM

OPERAZIONI BIT A BIT (BIT-BY-BIT)

ESEMPIO:

Se prendiamo le operazioni funzionali operazioni su $P(S)$
abbiamo che:

SOMMA: Si comporta
come lo XOR di
differenze simmetriche

$$\begin{array}{r} 0011 \\ + 0101 \\ \hline 0110 \end{array}$$

MOLTIPLICAZIONE. Si
comporta come l'AND
o l'intersezione

$$\begin{array}{r} 0011 \\ \times 0101 \\ \hline 0001 \end{array}$$

Correzione esercizi 30/12/2021 (LEZIONE 29)

4. a)

$$210 \quad (n, 1) \quad n = \{m \in \mathbb{N} \setminus \{0\} \mid m \mid 210\}$$

$$\begin{array}{c} 30 \quad 92 \quad 70 \quad 105 \\ \cancel{1} \cancel{X} \end{array}$$

$$\begin{array}{c} 6 \quad 10 \quad 14 \quad 15 \quad 21 \quad 35 \\ \cancel{2} \cancel{3} \cancel{5} \end{array}$$

$$\begin{array}{c} 2 \quad 3 \quad 5 \\ \cancel{1} \end{array}$$

b) $\max(n) = 210$
 $\min(n) = 1$

e) $2 \wedge 6 = 2$
 $2 \wedge 7 = 14$
 $7 \wedge 5 = 35$

e) $6 + 10 = (6 \wedge 10) \vee (6 \wedge 10)$
 $= (6 \wedge 21) \vee (35 \wedge 10) \wedge$
 $= 3 \vee 5 = 15$

\Leftarrow DIVISIBILITÀ

Sia (S, \cdot) un semigruppo commutativo. Poniamo $X, Y \in S$.

X divide Y ($X \mid Y$) se:

$$(\exists z \in S)(Y = Xz)$$

L'INSIEME DEI DIVISORI DI X

L'insieme dei divisori di $X \in S$ lo indico con $\text{DIV}_S(X)$.

$$\text{DIV}_S(X) = \{y \in S \mid y \mid X\}$$

L'INSIEME DEI MULUPI DI X

L'insieme dei multipli di $X \in S$ lo indico con $\text{MULT}_S(X)$.

$$\text{MULT}_S(X) = \{y \in S \mid X \mid y\}$$

ELEMENTO ASSOCIATO

Ad esempio, in \mathbb{Z} ho che $-5 \in S$ e sono associati per le regole $5 \cdot 5$ e $-5 \cdot 5$ ma $-5 \neq 5$

x e y appartenenti ad S si dicono associati se:

$$x \in \text{DIV}_S(y) \quad \& \quad y \in \text{DIV}_S(x) \rightarrow \begin{array}{l} \text{cioè } x \text{ e } y \text{ si dividono} \\ \text{a vicenda} \end{array}$$

\hookrightarrow NON POSSO FARLO
SE NON HO L'UNITÀ

L'INSIEME DEGLI ASSOCIATI A X

L'insieme degli elementi associati di X lo indico con $\text{ASSOC}_S(X)$

TEOREMA

Sia (S, \cdot) un monoido commutativo.

Se X è cancellabile, $\text{ASSOC}_S(X) = \{x \cdot u \mid u \in U(S)\}^*$

SE TUTTI GLI ELEMENTI DI X SONO CANCELLABILI ALLORA QUESTA COSA VALE PER TUTTI GLI ELEMENTI

* Scrutto come FBF:

$$\text{ASSOC}_S(X) = \{x \cdot u \mid u \in U(S)\} = \{y \in S \mid (\exists u \in U(S))(y = x \cdot u)\}$$

$$u \in U(S) \iff (\exists r \in S)(ru = 1_S \text{ AND } ur = 1_S)$$

IL PRODOTTO TRA X E UN ELEMENTO INVERTIBILE

GLI INVERTIBILI

DIM

$$\frac{4 \cdot 3 \cdot \frac{1}{3}}{3} = 4$$

(2) Sia $u \in U(S)$. Allora $X|X \cdot u$, ma $(X \cdot u) \cdot u^{-1} = X$. Dunque $X \cdot u | X$. Quindi dato che $X \cdot u \in \text{DIV}_S(X)$ e $X \in \text{DIV}_S(X \cdot u)$ allora $X \cdot u \in \text{ASSOC}_S(X)$.

(\subseteq) Considero $y \in \text{ASSOC}_S(X)$, ovvero $X|y$ e $y|X$.

Allora ci sono $w, z \in S$ tali che $y = Xw$ e $x = yz$.

Di conseguenza $x = X \cdot w \cdot z$, ma dato che

X è cancellabile allora $w \cdot z = 1$. → STAMO IN UN MONDO

Allora $w \in U(S)$ e di conseguenza $y \in U(S)$.

Quindi i due insiemi sono uguali.

TEOREMA

Sia (S, \cdot) un monoide commutativo. Allora ho che:

$$y \in \text{ASSOC}(x) \stackrel{1}{\leftrightarrow} \text{DIV}(x) = \text{DIV}(y) \stackrel{2}{\leftrightarrow} \text{MULT}(x) = \text{MULT}(y)$$

DIM

1. (\rightarrow) Per definizione, $y \in \text{ASSOC}(x) \leftrightarrow x \in \text{DIV}(y)$ e $y \in \text{DIV}(x)$. Ma allora tutti i divisori di x dividono anche y e tutti i divisori di y dividono anche x .

Cioè per le trasmutate di "1", $y \in \text{ASSOC}(x) \rightarrow \text{div}(x) = \text{div}(y)$.

(\leftarrow) Dato che (S, \cdot) è un monoide allora

$$y \in \text{DIV}(y). \text{ Di conseguenza } y \in \text{DIV}(x) \rightarrow \text{div}(x) = \text{div}(y)$$

Stesse cose vale per x , dunque $y \in \text{ASSOC}(x)$.

2. (\leftrightarrow) Ogni divisore di x è divisore di y e viceversa.

Se prendo $z \in \text{MULT}(x)$, z sarà del tipo

$z = x \cdot k$. Ma $y|x$, quindi $x = y \cdot h$. Cioè significa

che $z = y \cdot h \cdot k$, ovvero $z \in \text{MULT}(y)$. Stesso ragionamento

al contrario per l'altro verso.

MASSIMO COMUN DIVISORE

Sia (S, \cdot) un monoido commutativo t.c.s.

$$\text{MED}_s(S) = \left\{ d \in \bigcap_{x \in S} \text{DIV}_s(x) \mid (\forall z \in \bigcap_{x \in S} \text{DIV}_s(x)) (z \mid d) \right\}$$

• L'insieme dei divisori comuni di x_1, x_2, \dots, x_n

• Devono essere
divisori comuni
quindi devono
essere divisori
di tutti i divisori

• Questi devono
essere divisori
tutti gli altri
divisori comuni

ESEMPIO:

Quando non è facile fare il MCD, è meglio trovare il massimo dei divisori comuni (cioè il più grande divisore che sia comune a tutti gli elementi di T), avendo in mente il massimo dei minoranti (l'inf) nella relazione di divisione.

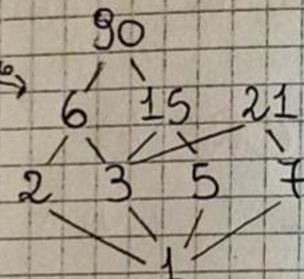
• Se ho $S = \{1, 2, 3, 5, 6, 7, 15, 21, 30\}$

con $T = \{30\}$, l'inf è 30

Con $T = \{30, 3\}$, l'inf è 3

Con $T = \{30, 7\}$, l'inf è 1 → È IL PIÙ GRANDE DEI DIVISORI COMUNI

In questo caso "1" è una relazione d'ordine.



- 30 È 30-
MA 30 ≠ 30

NON È ASIMMETRICO

• In \mathbb{Z} , la divisibilità non è una relazione d'ordine

Se ho $(\{-5, 1, 5, 10, 15\}, |)$, i divisori comuni tra 10 e 15 sono $\{-5, 1, 5\}$ → DIV(10) ∩ DIV(15) CHI È IL SUP DEI MINORANTI?

↳ Voglio trovare i divisori di 10 e 15 che siamo divisi da tutti gli altri divisori → Sono -5 e 5

↳ In \mathbb{Z} abbiamo più massimi comuni divisori dato che \mathbb{Z} non è ordinato con la divisione, quindi il massimo comun divisore è un insieme

$$S = \{-5, 1, 5, 10, 15\}$$

APPENDESE
E SUPERIEURE

$$\text{MED}_s(\{-5, 1, 5, 10, 15\}) = \text{MED}_s(10, 15) = \{-5, 5\} \subseteq \{-5, 1, 5\}$$

MCD

I DIVISORI COMUNI

↳ NOTA CHE SONO TUTTI E SOLO GLI ASSOCIATI A UN MASSIMO COMUNE DIVISORE
↳ TUTTI E SOLO GLI ASSOCIATI A S SONO S PER GLI INVERTIBILI (IN Z SONO -1 E 1)

MINIMO COMUNE MULTIPLO (mcmm)

Sia (S, \cdot) un monade commutativa e $x \in S$

$$mcmm_s(x) = \left\{ d \in \bigcap_{x \in S} \text{MULT}_s(x) \mid (\forall z \in \bigcap_{x \in S} \text{MULT}_s(x)) (d \mid z) \right\}$$

Esempio:

$$\text{Im } \{-5, 1, 5, 10, 15\}$$

$$mcmm(1) = \{1\}$$

$$mcmm(5) = \{-5, 5\} \rightarrow \begin{matrix} \text{I multipli di 5} \\ \text{sono } 5, -5, 10, 15 \end{matrix} \rightarrow \begin{matrix} \text{PRENDI I} \\ \text{MINIMI} \end{matrix}$$

DEVE ESSERE
GOTTO D'CHE
INVOCARE TUTTI
GLI ALTRI
MULTIPLO

7(2)

MULTIPLI IN \mathbb{Q}

Notiamo che $\text{im } (\mathbb{Q}, 1) = \text{MULT}_{\mathbb{Q}}(3) = \mathbb{Q}$

↳ Ad esempio, $1 \cdot \frac{1}{3} = 3$, quindi tutti i numeri sono multipli di 3 $\rightarrow 1 \in \text{MULTIPO DI } 3$

Di conseguenza $mcmm_{\mathbb{Q}}$ è vuoto perché tutti sono multipli di tutti.

DIVISORI BANALI

Sia (S, \cdot) un monade commutativa e sia $x \in S$ di insieme dei divisori banali, che indica con $BDIV_s(x)$, è uguale a:

$$BDIV_s(x) = \text{INV}(S) \cup \text{ASSOC}_s(x)$$

di chiamano divisori banali perché è ovvio che questi sono divisori.

↳ Cioè tutti gli invertibili sono divisori dell'intero, mentre gli associati sono divisori di x per definizione.

Im \mathbb{Q} tutti sono divisori banali

IRRIDUCIBILE

IN \mathbb{Z} I PRIMI SONO TUTTI I SOLI GLI IRRIDUCIBILI

Sia (S, \cdot) un monoido di integrità e sia KES ,
 X si dice irriducibile se: $X \notin U(S)$ e $\text{DIV}_S(X) = \text{BDIV}_S(X)$

NON E' INVERTIBILE E TUTTI I DIVISORI SONO QUELLI BANALI

PRIMO

E Sia (S, \cdot) un monoido commutativo, e sia PES ,
(p si dice primo se $(\forall a, b \in S)(p \mid ab \Rightarrow p \mid a \vee p \mid b)$)

COPRIMI

(S, \cdot) un monoido commutativo,

Sia $x, y \in S$, se $1_S \in \text{MCD}_S(\{x, y\})$, x e y si dicono coprimi

SE UNO DEI MED E' 1, ESEMPIO:
PURA I NUMERI SI $\rightarrow \text{MCD}(\{2, 3\}) = \{1, -1\}$
ARANO COPRIMI

CANCELLATIVI

Un monoido commutativo con tutti elementi cancellativi si dice cancellativo.

MONOIDE FATTORIALE \rightarrow COME VALE IN \mathbb{Z} MA NEI MONOIDI

Sia (m, \cdot) un monoido commutativo cancellativo,
 (m, \cdot) si dice fattoriale se vale almeno una tra:

- 1) Ogni $x \in m \setminus U(m)$ è prodotto di primi.
- 2) Ogni $x \in m \setminus U(m)$ è prodotto di irriducibili e ogni irriducibile è primo.
- 3) Ogni $x \in m \setminus U(m)$ è prodotto di irriducibili e ogni fattorizzazione è unica a meno dell'ordine dei fattori e del prodotto per invertibili.

NO DIM

ANELLO FATTOORIALE

Un anello $(\mathbb{A}, +, \cdot)$ è commutativo e unitario
si dice fattoriale se $(\mathbb{A} \setminus \{0\}, \cdot)$ è un monoido
fattoriale

ESEMPIO:

- $(\mathbb{N} \setminus \{0\}, \cdot) \rightarrow$ SONO MONOIDI FATTORIALI PER IL
TEOREMA FONDAMENTALE DELL'ARITMETICA

- $(\mathbb{Z} \setminus \{0\}, \cdot) \rightarrow$

$(\mathbb{Z}, +, \cdot)$ è UN ANELLO FATTOORIALE ANCHE SG
c'è lo 0 visto che $(\mathbb{Z} \setminus \{0\}, \cdot)$ è cancellativa
 \hookrightarrow Non si può scrivere $(\mathbb{Z} \setminus \{0\}, +, \cdot)$ perché
altrimenti il + non sarebbe più
definito

7. Sia (S, \cdot) un monoide commutativo. Allora
 $m \in \text{MCD}(x, y) \leftrightarrow (\text{ASSOC}(m) = \text{MCD}(x, y))$

DIM $\rightarrow m \in \text{MCD}(x, y) \leftrightarrow$ Per definizione, $m|x \wedge m|y \wedge (\forall z \in S)(z|x \wedge z|y \rightarrow z|m)$

(\subseteq) Considero un $m \in \text{ASSOC}(m)$, cioè, per definizione,
 $m \in \text{DIV}(m) \wedge m \in \text{DIV}(m)$, ciò significa che
 $m|x \wedge m|y \wedge (\forall z \in S)(z|x \wedge z|y \rightarrow z|m)$

(\supseteq) Se no prendo un altro massimo comune divisor

m' , ho che:

perché
 $m' \in \text{MCD}(x, y)$

perché
 $m' \in \text{MCD}(x, y)$

$m' \in \text{MCD}(x, y) \rightarrow m|m' \wedge m'|m$,

MASSIMI COMUNI
 DIVISORI SI
 DIVIDONO TRA
 LORO

di conseguenza $m' \in \text{ASSOC}(m)$

\leftarrow $m \in \text{ASSOC}(m)$ dato che (S, \cdot) è un monoide,
 quindi per ipotesi $m \in \text{MCD}(x, y)$, dato che per
 estensione $\text{ASSOC}(m) = \text{MCD}(x, y)$

TEOREMA

Sia (S, \cdot) un monoide commutativo. Allora:

$m \in \text{mem}(x, y) \leftrightarrow \text{ASSOC}(m) = \text{mem}(x, y)$

DIM

La dimostrazione è simile alle precedenti

$m \in \text{mem}(x, y) \stackrel{\text{def}}{\leftrightarrow} (x|m \wedge y|m) \wedge (\forall z \in S)(x|z \wedge y|z \rightarrow m|z)$

$\rightarrow m \in \text{ASSOC}(m) \leftrightarrow m \in \text{DIV}(m) \wedge m \in \text{DIV}(m)$

Cio' significa che $x|m \wedge y|m \wedge (\forall z \in S)(x|z \wedge y|z \rightarrow m|z)$

Preso $m' \in \text{mem}(x, y) \rightarrow m'|m \wedge m|m' \rightarrow m \in \text{ASSOC}(m)$

\leftarrow Essendo (S, \cdot) un monoide, $m \in \text{ASSOC}(m)$.
 $\text{ASSOC}(m) = \text{mem}(x, y)$, allora $m \in \text{mem}(x, y)$. Dato che, per ipotesi,

TEOREMA

Se (m, \cdot) è un monoidale fattoriale. Sia $a \in m \setminus U(m)$, possiamo scrivere a come prodotto di primi: \rightarrow si trovano in un monoidale fattoriale

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}, \quad \forall k_1, k_2, \dots, k_m \in \mathbb{N}$$

com p_1, p_2, \dots, p_m numeri primi

Notiamo che i divisori di a sono tutti e soli gli associati ad elementi del tipo: \rightarrow gli associati perché in \mathbb{Z} ci sono anche divisori negativi

$$\checkmark p_1^{l_1} \cdot p_2^{l_2} \cdots p_m^{l_m} \quad \text{com } 0 \leq l_i \leq k_i$$

SE SCENOLO DI ESPONENTE AVRAI UN DIVISORE DI 0

$$\text{e com } 1 \leq i \leq m$$

IN UN MONOIDALE FATTORIALE DOGLI $\langle x \rangle = \{x \cdot u \mid u \in \mathcal{U}(2)\}$

ESEMPIO:

Se ho $2^4 \cdot 3^2 \cdot 5$, i divisori sono del tipo $2^3 \cdot 3, 2 \cdot 3^2 \cdot 5, -2^4 \cdot 5$ ecc...

COROLLARIO

Se $a = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m} \in \mathbb{N}$, allora a ha $m(k_1 + k_2 + \dots + k_m)$ divisori

→ SONO TUTTE LE POSSIBILI COMBINAZIONI DI ESPONENTI GLI ASSOCIATI DI a IN \mathbb{N} E' SOLO m PERCHE' L'UNICO 0 E' 1

COROLLARIO

Se $a = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m} \in \mathbb{Z}$, allora a ha $2m(k_1 + k_2 + \dots + k_m)$ divisori

→ ORA DOBBIANO PRENDERE ANCHE I NUMERI NEGATIVI PERCHE' IN \mathbb{Z} GLI INVERTIBILI SONO ± 1

ESEMPIO:

$$6 = 2^1 \cdot 3^1 \quad \stackrel{\text{IN } \mathbb{N}}{\downarrow} \quad \rightarrow \text{I divisori di } 6 \text{ sono } 2(1+1) = 4$$

LA SOMMA DEGLI ESPONENTI

IL NUMERO DI PRIMI

\downarrow

\pm divisori di 6 in \mathbb{Z} sono:
 $2 \cdot 2(1+1) = 8$, infatti $\{m \in \mathbb{Z} \mid m \mid 6\} = \{-1, 1, -2, 2, -3, 3, -6, 6\}$

NEI MONOIDI FATTORIALI ESISTONO
SEMPRE IL MMCM E IL MCD

Sia (m, \cdot) un monomio fattoriale.

Sia $a = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$ e sia $b = p_1^{l_1} \cdot p_2^{l_2} \cdots p_m^{l_m}$

Inoltre, sia che:

$\begin{matrix} \text{E' IL MASSIMO TRA} \\ \text{GLI ESPONENTI} \end{matrix}$

$\begin{matrix} \text{E' IL MINIMO TRA} \\ \text{GLI ESPONENTI} \end{matrix}$

$$(\forall i \in \mathbb{N}) (1 \leq i \leq m \rightarrow \alpha_i := \max(k_i, l_i) \wedge \beta_i := \min(k_i, l_i))$$

Allora vale che $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m} \in \text{mem}(a, b)$

e che $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_m^{\beta_m} \in \text{MCD}(a, b)$

ATTENZIONE!

Perché ho che la decomposizione di a e b ha lo stesso numero m di fattori?

↳ L'esponente è compreso tra 0 e k_m (o tra 0 e l_m), quindi posso scrivere che se:

$$a = 2 \cdot 3^2 \cdot 5 \quad \text{e} \quad b = 3 \cdot 5^2 \cdot 11 \cdot 13, \quad \text{allora posso riscrivereli come } a = 2^1 \cdot 3^2 \cdot 5^1 \cdot 11^0 \cdot 13^0 \quad \text{e} \quad b = 2^0 \cdot 3^1 \cdot 5^2 \cdot 11^1 \cdot 13^1$$

Anzi che i massimi d'assorso:

$$\alpha_1 = \max(1, 0) = 1, \quad \alpha_2 = \max(2, 1) = 2, \quad \alpha_3 = 2, \quad \alpha_4 = 1, \quad \alpha_5 = 1$$

COROLLARIO

Sia (m, \cdot) un monomio fattoriale.

Sia $a = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$ e sia $b = p_1^{l_1} \cdot p_2^{l_2} \cdots p_m^{l_m}$

Se $m \in \text{mem}(a, b)$ e $m' \in \text{MCD}(a, b)$, allora

$$m \cdot m' \in \text{ASSOC}(a, b)$$

→ QUANDO FACCIO $a \cdot b$ STO SOMMANDO GLI ESPONENTI CHE E' LA STESSA COSA DI SOMMARE IL MASSIMO E IL MINIMO DEGLI ESPONENTI

ESEMPIO:

$$a = 2^2 \cdot 3^0 \cdot 5^1$$

$$b = 2^1 \cdot 5^0 \cdot 3^1$$

$$a \cdot b = m \cdot m' = p_1^{k_1 + l_1} \cdot p_2^{k_2 + l_2} \cdots p_m^{k_m + l_m}$$

FANNO PARTE DEGLI ASSOCIATI PERCHE' CI PUO' STARE IL -

$$\text{mem}: 2^2 \cdot 3 \cdot 5 \in \text{mem}(a, b)$$

$$\text{MCD}: 2 \in \text{MCD}(a, b)$$

$$\left\{ \begin{array}{l} a \cdot b = 2^3 \cdot 3 \cdot 5 \\ m \cdot m' = 2^3 \cdot 3 \cdot 5 \end{array} \right\}$$

$$a \cdot b = m \cdot m'$$

$$m' = \frac{a \cdot b}{m}$$

DAL M₁
TROVO
ANCORA
VIECCHI

TEOREMA

Se $(\mathbb{Q}, +, \cdot)$ è un anello commutativo unitario, siamo $b, c \in \mathbb{Q}$ e $d \in \text{DIV}_{(b,c)}(b) \cap \text{DIV}_{(b,c)}(c)$ \Rightarrow d APPARTIENE AI DIVISORI COMUNI

Allora $(\forall x, y \in \mathbb{Q})(d | (x \cdot b + y \cdot c)) \Leftrightarrow$ UN DIVISORE COMUNE DI b E c DIVIDE OGNI QUALE COMBINAZIONE DI b E DI c

VALORE ASSOLUTO

E' una funzione $\mathbb{Z} \rightarrow \mathbb{N}$ e te:

$$|m| = m \quad \text{se } m \in \mathbb{N}$$

$$|m| = -m \quad \text{se } m \in \mathbb{Z} \setminus \mathbb{N}$$

$b = d \cdot k, c = d \cdot l$, nato in evidenza d (PER LA DISTRIBUTIVITÀ) E HO CHE
 $b+c = d(n+l)$, cioè $d | (b+c)(n+l)$, cioè $d | ((n+l) \cdot b + (n+l) \cdot c)$

TEOREMA DELLA DIVISIONE EUCLIDEA (o CON RESTO)

$$(\forall m, n \in \mathbb{Z}) (m \neq 0 \rightarrow (\exists ! (q, r) \in \mathbb{Z} \times \mathbb{N}) (m = mq + r \wedge \begin{array}{l} \text{NON POSSA} \\ \text{DIVIDERE NULLA} \\ \text{(TRAMME 0) PERO} \end{array} \wedge 0 \leq r < |m|))$$

ESEMPIO: $98 \mid 13$

$$\begin{array}{r} 98 \\ \overline{)13} \\ 7 \\ \hline 6 \end{array}$$

$$\text{Quindi } 98 = 13 \cdot 7 + 6$$

E, INFATTI, $0 \leq 6 < 13$
 LA COPPIA E' $(13, 6)$

DIM DI SECONDA FORMA SU m

• Suppongo $m > 0$.

BASE DI INDUZIONE

• Se $m=0$, scelgo $q=0$ e $r=0 \rightarrow 0=0 \cdot 1 + 0$, $0 < 0$ ✓

• Se $m=|m|$ allora:

$$\text{Se } m=|m|, q=1 \text{ e } r=0$$

$$\text{Se } m=-|m|, q=-1 \text{ e } r=0$$

$$\begin{array}{r} 13 \mid 20 \\ \overline{)20} \\ 13 \\ \hline 7 \end{array}$$

• Suppongo che $0 < m < |m|$. Posso scegliere $q=0$ e $r=m$

• Suppongo $|m| < m$ PERCHE PER L'IPOTESI $|m| \neq 0$

DATO CHE NO! SUPPOSTO VERO L'ASSERTO
 $\forall x \in m$

Allora $m - |m| < m$ Per ipotesi di induzione, allora

$$m - |m| = mq_1 + r_1 \text{ con } 0 \leq r_1 < |m|$$

Di conseguenza vale che $m = mq_1 + |m| + r_1$

Visto che $m = mq_1 + l|m| + r_1$,

Se $m > 0$, prendo $q = q_1 + 1$ e $r_1 = r$

Se $m < 0$, prendo $q = q_1 - 1$ e $r_1 = r$

Quindi per induzione di seconda forma, vale $\forall m \in \mathbb{N}$ l'asserto

• Per i numeri negativi, invece:

Suppongo $m \in \mathbb{Z} \setminus \mathbb{N}$.

ESSENDO $-m$ POSITIVO E AVENDO APENNA
DIMOSTRATO L'ASSERTO $\forall m \in \mathbb{N}$

Vale che $-m = mq_1 + r_1$ con $0 \leq r_1 < |m|$

Di conseguenza $m = m(-q_1) - r_1$, ma $-r_1 \leq 0 \rightarrow$ NON VA BENE
PERCHÉ NON È
CONTENUTO TRA 0
E |m|

Poco aggiungerà e sottrarre $|m|$, quindi entro che:

$$m = m(-q_1) - r_1 + |m| - |m|$$

↓ QUESTA PARTE È SEMPRE POSITIVA E < |m|

Allora, se $r_1 \neq 0$:

Se $m > 0$, secolo $q = -q_1 - m$, e $r = m + r_1 < |m|$

Se $m < 0$, secolo $q = -q_1 + m$, e $r = -m - r_1 < |m|$

Se $r_1 = 0$, allora nè basta avere $m = m(-q_1)$

→ PER DIMOSTRARE L'UNICITÀ DELLA COPPIA IN $\exists! (q, r) \in \mathbb{Z} \times \mathbb{N}$

• Consideriamo due copie $(q_1, r_1), (q_2, r_2) \in (\mathbb{Z}, \mathbb{N})$

con $0 \leq r_1 \leq r_2 < |m|$ e $m = mq_1 + r_1$ e $m = mq_2 + r_2$
LO SUPPOSSO IN

↪ Allora posso supporre che $mq_1 + r_1 = mq_2 + r_2$, cioè
 $m(q_1 - q_2) = r_2 - r_1$. Ci faccio i valori assoluti, quindi
ho che $|m||q_1 - q_2| = |m(q_1 - q_2)| = |r_2 - r_1| < |m|$

Da ciò segue che $q_1 = q_2$, di conseguenza $r_1 = r_2$

NON POSSO AVERE
 $|m||q_1 - q_2| < |m|$
SE $|q_1 - q_2| \neq 0$

COROLLARIO (FUNZIONE DE(m, n))

Visto che la copia è unica, posso scrivere una funzione che per ogni coppia (m, n) associa quell'unica ^{copia}

$$DE(m, n) = (q, r)$$

ALGORITMO DELLE DIVISIONI SUCCESSIVE

ESEMPIO:

- $\text{MCD}(12, 15)$, $15 = 12 \cdot 1 + 3$

*MI RIUNGO A
CALCOLARLO
IN IN E Poi
METTO L'INVERSO*

MI FERMO CON
 $r=0$ E VEDO
IL RESTO CHE
STA PRIMA,
INFATTI $3|12$ E
 $3|15$, MCD = 3

VOGLIANO
TROVARE IL
MED TRA
DUE NUMERI
↓

- $\text{MCD}(313, 17)$,

$$\begin{aligned} 313 &= 17 \cdot 18 + 11 \rightarrow 313 \\ 17 &= 9 \cdot 1 + 8 \quad | 17 \\ 9 &= 8 \cdot 1 + 1 \quad | 15 \\ 8 &= 1 \cdot 8 + 0 \quad | 13 \end{aligned}$$

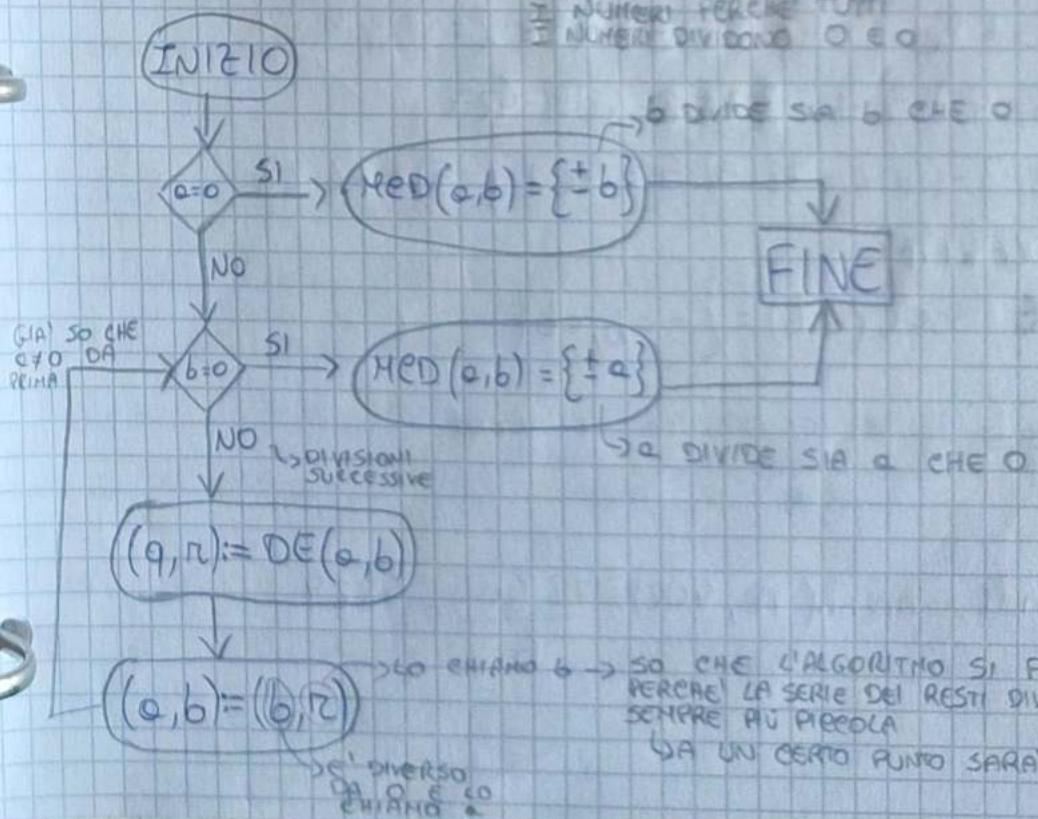
POSSO RISALIRE
PER TRANSITIVITÀ

APPLICO TANTE
OLTE IL
TEOREMA DELLA
DIVISIONE
EUCLIDEA

IN GENERALE:

$$\text{MCD}(a, b) \text{ con } (a, b) \neq (0, 0) \text{ e } a, b \in \mathbb{N}$$

• SE $\text{MCD}(0, 0)$ SONO TUTTI
I NUMERI PERCHE' TUTTI
I NUMERI DIVIDONO 0 E 0



SE CHIAMO $b \rightarrow$ SO CHE L'ALGORITMO SI FERMA
PERCHE' LA SERIE DEI RESTI DIVENTA
SEMPRE PIÙ PICCOLA
DA UN CERTO PUNTO SARÀ 0

SE DIVERSO
CHIAMO a

3,4) d) MCD(1111231, 111123)

PUNTO 4 $\sqrt{1111231 = 10 \cdot 111123 + 1} \rightarrow \text{MCD}(1111231, 111123) = 1$

$\text{MCD} = 1 = 11112311 + 111123 \cdot (-10)$

a) $\sqrt{\text{MCD}(72, 402) = 6}$

$$\begin{aligned} 72 &= 402 \cdot 0 + 72 && \text{SE IL PRIMO} \\ 402 &= 72 \cdot 5 + 42 && \text{È MINORE} \\ 72 &= 42 \cdot 1 + 30 && \text{DEL SECONDO} \\ 42 &= 30 \cdot 1 + 12 && \text{POSSANO} \\ 30 &= 12 \cdot 2 + 6 && \text{FARE QUESTO} \\ 12 &= 6 \cdot 2 + 0 && \text{PASSAGGIO} \\ &&& \text{IN MODO} \\ &&& \text{IMPLICITO} \end{aligned}$$

PUNTO 4

OTTO CHE SO
 $42 = 30 \cdot 1 + 12$

ALGORITMO DELLE DIVISIONI SUCCESSIONI

$$a = b q_1 + r_1$$

$$b = r_1 q_2 + r_2$$

$$r_1 = r_2 q_3 + r_3$$

:

$$r_{t-4} = r_{t-3} \cdot q_{t-2} + r_{t-2}$$

$$r_{t-3} = r_{t-2} \cdot q_{t-1} + r_{t-1}$$

$$r_{t-2} = r_{t-1} \cdot q_t + \textcircled{0} \quad r_t$$

$a, b \in \mathbb{N}$

PER A, B E Z
PRENDIAMO
IL MCD ANCHE
NEGATIVO

$$0 = r_t < r_{t-1} < \dots < r_2 < r_1 < b$$

TEORIA
DI BEEZOUT

$$\begin{aligned} 6 &= 30 - 12 \cdot 2 = 30 - (42 - 30) \cdot 2 = \\ &= (72 - 42) - (42 - (72 - 42)) \cdot 2 = \text{NETTO IN} \\ &= 30 + 30 \cdot 2 - 42 \cdot 2 = 30 \cdot 3 - 42 \cdot 2 = \text{SERVIRÀ 30 CON C} \\ &= (72 - 42) \cdot 3 - 42 \cdot 2 = 72 \cdot 3 - 42 \cdot 5 = \\ &= 72 \cdot 3 - (402 - 72 \cdot 5) \cdot 5 = 402 \cdot (-5) + 72 \cdot 28 \end{aligned}$$

PARTICOLARITÀ

$$m \cdot M \in \text{ASSOC}(a, b) = \{-ab, ab\}$$

$m = \frac{ab}{M} \rightarrow$ SE HO TROVATO M , OVVERO
IL MCD, POSSO TROVARE
ANCHE IL m mem

Quindi, $\text{mem}(72, 402) = \frac{72 \cdot 402}{6} = 9824$

TEOREMA DI BEZOUT

ASSIEME ALL'ALGORITMO DELLE DIVISIONI SUCCESSIVE FA
L'ALGORITMO DELLE DIVISIONI
SUCCESSIONI ESTESA

Prese la coppia $(a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0, 0)\}$ ho che:

$$(\forall (a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0, 0)\}) ((\exists d \in \text{MCD}(a, b)) (\exists u, v \in \mathbb{Z}) (d = a \cdot u + b \cdot v))$$

QUALSIASI SIA UN COUPPI A QUALSIASI SIA IL MCD(a, b).
IL MCD LO POSSO SCRIVERE COME COMBINAZIONE LINEARE DI a E b

DIM (INDUZIONE DI SECONDA FORMA SU t)

Scegli t il minimo numero di passi tale che $R_t = 0$
Supponiamo $a, b \in \mathbb{N}$

- Se $t=1$, $r_1=0 \rightarrow a = b \cdot q_1$

Allora il MCD di a è b stessa. Ovvio:

$$b \in \text{MCD}(a, b) \quad \& \quad b = a \cdot 0 + b \cdot 1 \quad \text{OK}$$

- Se $t=2$, $r_1 \neq 0 \quad \& \quad r_2=0$

Allora il MCD è r_1 . Quindi:

$$r_1 \in \text{MCD}(a, b), \text{ quindi posso scrivere } r_1 = a \cdot 1 + b \cdot (-q_1) \quad \text{OK}$$

I RESTI MINORI DI t

- Suppongo vero l'asserto per i R_i con $1 \leq i < t$

✓ Visto che $t > 1$, implica che esiste R_{t-1} .

In particolare, $r_{t-1} \in \text{MCD}(a, b)$

✓ Posso scrivere

$$r_{t-1} = r_{t-3} + r_{t-2} \cdot (-q_{t-1})$$

STIAMO
PROCEDENDO
PER INDUT.
LA SECONDA
FORMA HA
NON LO
FACCIAVANO IN
MOLTO RIGOROSO
PERCHE NOIOSO

Tuttavia per ipotesi di induzione $\exists u, v, w, x \in \mathbb{Z}$

tali che: $r_{t-3} = a \cdot u + b \cdot v$ AND $r_{t-2} = a \cdot w + b \cdot x$

Quindi avremo che:

$$\begin{aligned} r_{t-1} &= r_{t-3} + r_{t-2} \cdot (-q_{t-1}) = a \cdot u + b \cdot v + (a \cdot w + b \cdot x) \cdot (-q_{t-1}) = \\ &= a(u - w \cdot q_{t-1}) + b(v - x \cdot q_{t-1}) \end{aligned}$$

Cioè ho scritto r_{t-1} come combinazione lineare
di a e di b , quindi per induzione l'asserto
vale anche per r_t

LEMMA DI EUCLIDE

Siamo $a, b, c \in \mathbb{Z}$.

Siamo a, b coprimi. \rightarrow cioè si ha $\text{MCD}(a, b) = 1$

Allora, $x \equiv a/b \pmod{c}$, dove a/c .

ESEMPIO:
SE $a=3$ E $b=5$ E
 $a|30 \rightarrow a|15 \cdot 6$,
ALLORA $a|6$

DIM

a, b sono coprimi, quindi $1 \in \text{MCD}(a, b)$.

Per il teorema di Bezout, trovo $u, v \in \mathbb{Z}$ tali che:

$$1 = au + bv$$

Moltipico tutto per c e ottengo che:

$$c = c \cdot u + b \cdot c \cdot v \quad \rightarrow \begin{array}{l} \text{SE } X=c \cdot u \text{ E } Y=b \cdot c \cdot v \text{ HO CHE} \\ Q \in \text{DIV}(X) \cap \text{DIV}(Y) \text{ E PER IL TEOREMA} \\ \text{PRIMA DEL VALORE ASSOLUTO ALLORA} \\ a|X \cdot u + Y \cdot v, \text{cioè } a|c \end{array}$$

Quindi $a|c$

TEOREMA

NUMERI PRIMI

→ DIMOSTRARE PRIMA QUESTO TEOREMA
E' FONDAMENTALE PER ALLEGGERIRE IL TEOREMA
FONDAMENTALE DELL'ARITMETICA

I primi in \mathbb{Z} sono tutti e solo gli irriducibili

sono quelli che se dividono un
prodotto allora dividono uno
dei due fattori

(\rightarrow) Sia p un numero primo

Siamo $a, b \in \mathbb{Z}$ tali che:

$$p = a \cdot b$$

Per ipotesi $p|a$ V $p|b$.

Suppongo che $p|a$, cioè:

$$p \in \text{DIV}(a)$$

→ vogliamo
dimostrare
che p è
irriducibile

Ma noto anche che $a \in \text{DIV}(p)$, quindi:

$$p \in \text{ASSOC}(a) = \{a, -a\} \rightarrow \text{Quindi } p = a \vee p = -a$$

→ IN UN MONDO COMMUTATIVO $\text{ASSOC}(a) = \{x \cdot a \mid x \in U(a)\}$ MA
IN \mathbb{Z} , Gli UNICI INVESTITORI SONO $\{1, -1\}$

Segue che $b = 1$ V $b = -1$, quindi p ha solo
divisori banchi $\rightarrow p$ è irriducibile

(\leftarrow) Se p irriducibile, cioè $\text{DIV}(p) = \{-1, 1, p, -p\}$

Suffongo che $p|ab \rightarrow$ POSSO FAR VEDERE CHE
 $p|a \vee p|b$

Suffoco, anche che $p|a$

\hookrightarrow Visto che $p|a$ è dato che $\text{MCD}(p, a) \subseteq \text{DIV}(p)$,

può dire che in $\text{MCD}(p, a)$ non c'è zero $p \neq p$

Quindi $\text{MCD}(p, a) \subseteq (\text{DIV}(p) \setminus \{-p, p\})$, cioè $1 \in \text{MCD}(p, a)$,

cioè p e a sono coprimi

\hookrightarrow Per il lemma di Euclide, $p|b$

ALTRIMENTI
AVREMMO
CHE $p|c$,
MA PER
IPOTESI
 $p|c$

Congruenze modulo m (con m intero)

Preso un $m \in \mathbb{Z}$, definisco che:

$$(\forall a, b \in \mathbb{Z})(a \equiv_m b : \leftrightarrow m | (a-b)) \rightarrow \begin{array}{l} a \equiv_m b \leftrightarrow a \equiv b \\ \text{perché } 0 \text{ divide} \\ \text{solo } 0 \end{array}$$

SAPPIAMO CHE:

\equiv_m è una relazione di equivalenza

$$[a]_{\equiv_m} = [a]_m$$

$$[0]_2 = [19]_2 \rightarrow \text{DATO CHE } 21(19-0)$$

$$\mathbb{Z}_m := \mathbb{Z}_{\equiv_m} \text{ e inoltre, } \mathbb{Z}_m = \mathbb{Z}_{-m} \rightarrow \begin{array}{l} \text{INFATI SE } m(a-b), \text{ È} \\ \text{OSSIA } a \equiv_m -m(a-b) \end{array}$$

$$\mathbb{Z}_2 = \{[0]_2, [1]_2\}$$

↑
PAIR ↑
DISPARMI

SPESO CONSIDERIAMO
SOLO LE CLASSI DI
CONGRUENZA POSITIVE
(QUELLI NEGATIVE SONO UGUALI)

COME POSSO SCRIVERE $[a]_m$ COME INSIEME?

Sappiamo che, per $b \in \mathbb{Z}$ tale che $m | (a-b)$, $b = a + km$.

$$[a]_m = \{b \in \mathbb{Z} \mid m | (a-b)\}, \text{ quindi posso scrivere } [a]_m$$

$$[a]_m := \{a + km \mid k \in \mathbb{Z}\}$$

TUTTI GLI ELEMENTI IN
RELATIONE \equiv_m CON a

$$[0]_2 = \{0 + k \cdot 2 \mid k \in \mathbb{Z}\}$$

$$[1]_2 = \{1 + k \cdot 2 \mid k \in \mathbb{Z}\}$$

OPERAZIONE (PARZIALE) MOD

$$(\forall (a, m) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) (a \text{ MOD } m := \min([a]_m \cap \mathbb{N}))$$

↳ IL PIÙ PICCOLO
NELLA CLASSE
DI EQUIVALENZA

ESEMPIO:

$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\} \rightarrow \text{INFATTI } [3]_3 = [0]_3 \text{ DATO CHE IN } [x]_3 \text{ HO } x+3k$$

↳ $[3]_3$ HO $3+3k$ CHE POSSO AVERE
ANCHE IN $[0]_3$, CON $0+3j,k$

- $0 \text{ MOD } 3 = 0$
- $1 \text{ MOD } 3 = 1$
- $2 \text{ MOD } 3 = 2$
- $3 \text{ MOD } 3 = 0$

Se $m \in [a]_m$, ho che $[a]_m = [m]_m = [0]_m$.
quindi $a \text{ MOD } m = 0$. Quindi ho che
 $a \text{ MOD } m < |m|$

Notiamo che $a \text{ MOD } m$ è proprio il Resto in DE(a, m), infatti, a volte $a \text{ MOD } m$ lo indichiamo con REST(a, m) o anche $a \% m$.

DIVISIONE EUCLIDEA
* INFATTI PER LA DIVISIONE EUCLIDEA $a = qm + r$, con $0 \leq r < |m|$
DA CUI $r = a + (-q)m$, ELORE $r \in [a]_m$ ED È IL PIÙ PICCOLO AD APPARTENERVI

TEOREMA

Sia $m \in \mathbb{N} \setminus \{0\}$, allora $\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$

In particolare $|\mathbb{Z}_m| = m$

→ L'ORDINE DI \mathbb{Z}_m

OSS

• Sia $a \in \mathbb{Z}$.

$DE(a, m) = (q, r)$, cioè $a = qm + r$ e $0 \leq r < |m|$,
quindi $[a]_m = [r]_m \rightarrow$ QUALUNQUE NUMERO IO PRENDA, POSSO TROVARE UN RAPPRESENTANTE DELLA CLASSE CHE È UN RESTO DEL NUMERO

STESSO
RAGIONAMENTO
DI PRIMA *

Ciò ha fatto vedere che $\mathbb{Z}_m \subseteq \{[0]_m, [1]_m, \dots, [m-1]_m\}$

QUALUNQUE
SIA a , LA
SUA PUSSÈ
DI EGUALI
E' UNO DI
QUESTI

• Siamo $0 \leq i \leq j < |m|$ e $[i]_m = [j]_m$

↪ Date che $0 \leq i \leq j < |m|$, segue che $0 \leq j-i < m$

↪ Visto che $[i]_m = [j]_m$, allora $(\exists k \in \mathbb{Z})(j = i + km)$

Quindi $j-i$ è un multiplo di $m \rightarrow j-i=0 \rightarrow i=j$

sempre che $j-i < m$

CLASSI
USUALI
SOPRA
I E J
USUALI

VOCAPMO DI MOSTRARE
CHE TIME OLTRE CLASSI
SONO DISTINTE, QUINDI
CHE I E J SONO DIVERSI
VALORI SE $[i]_m = [j]_m$

CONGRUENZE

COMPATIBILE A SINISTRA

- UNA RELAZIONE:
- RIFLESSIVA
- SIMMETRICA
- TRANSITIVA

Sia $S \neq \emptyset$ e $*$ un'operazione binaria interna di S . Sia \sim una relazione di equivalenza su S .

\sim si dice compatibile a sinistra in $(S, *)$ se:

$$(\forall a, b, c \in S)(a \sim b \rightarrow c * a \sim c * b)$$

COMPATIBILE A DESTRA

Sia $S \neq \emptyset$ e $*$ un'operazione binaria interna di S .

Sia \sim una relazione di equivalenza su S

\sim si dice compatibile a destra in $(S, *)$ se:

$$(\forall a, b, c \in S)(a \sim b \rightarrow a * c \sim b * c)$$

CONGRUENZA

Sia $S \neq \emptyset$ e $*_1, *_2, \dots, *_m$ operazioni binarie interne di S . \sim , relazione di equivalenza, si dice congruenza in $(S, *_1, *_2, \dots, *_m)$ se:

cioè se ho due rappresentanti diversi

$$(\forall a, b, c, d \in S)((\forall i \in \mathbb{N})(0 \leq i \leq m \rightarrow (a \sim b \wedge c \sim d \rightarrow$$

CONTINUO AD
AVERE SEMPRE LA
STESSA CLASSE
DI EQUIVALENZA

ALLORA ANCHE FAR E
IL PRODOTTO DEI
SINGOLI RAPPRESENTANTI
NON CAMBIA LA RELAZIONE
DI EQUIVALENZA

cioè se ho due
rappresentanti diversi

$a *_i c \sim b *_i d$)

Se \sim è congruenza in $(S, *_1, *_2, \dots, *_m)$, allora

sono ben poste:

$$\bullet (*_i)_{\sim} : ([x]_{\sim}, [y]_{\sim}) \in S_{\sim} \times S_{\sim} \mapsto [x *_i y]_{\sim} \in S_{\sim}$$

$$\bullet \Pi : X \in S \mapsto [x]_{\sim} \in S_{\sim} \rightarrow \Pi \text{ è un epimorfismo}$$

LE STRUTTURE NON SONO

TANTO DIVERSE, POSSO

PORTARMI LE OPERAZIONI DA

S A S_{\sim} SE IL \sim SI COMPORTA

BENE RISPETTO ALLE OPERAZIONI

BENE RISPETTO ALLE OPERAZIONI

tra $(S, *_1, *_2, \dots, *_m)$ e

$(S_{\sim}, (*_1)_{\sim}, (*_2)_{\sim}, \dots, (*_m)_{\sim})$

cioè se vace
la congruenza

TEOREMA

UNA RELAZIONE
DI EQUIVALENZA

\sim è congruente se e solo se è compatibile a destra ed è compatibile a sinistra con ogni $*_i$ di S

DIM \rightarrow SE $(S, *_1, *_2, \dots, *_n)$ È UNA STRUTTURA AD n OPERAZIONI INTERNE

Suppongo ci sia un'unica operazione $*$ in $(S, *)$

(\rightarrow) Per ipotesi ho $a \sim b$. Dato che \sim è una relazione di STESO RAGIONAMENTO PER LA COMPATIBILITÀ A DESTRA congruenza, allora vale anche $c \sim c$. Quindi $a * c \sim b * c$ \downarrow PER LA CONGRUENZA

(\leftarrow) Suppongo $a \sim b$ e $c \sim d$.

- Per compatibile a destra, $a * c \sim b * c$,
- Per compatibile a sinistra, $b * c \sim d * c$
- Quindi, per transitività di \sim , $a * c \sim b * d$

ESEMPIO:

• Dato $m \in \mathbb{N} \setminus \{0\}$, un esempio è \equiv_m in $(\mathbb{Z}, +, \cdot)$.

Possiamo riportare le operazioni di $(\mathbb{Z}, +, \cdot)$ in $(\mathbb{Z}_m, +, \cdot)$ tramite epimorfismo

$$\hookrightarrow (\mathbb{Z}, +, \cdot) \xrightarrow{\pi} (\mathbb{Z}_m, +, \cdot) \rightarrow \begin{array}{l} \text{POSSIAMO SOMMARE} \\ \text{E MOLTIPLICARE LE} \\ \text{CLASSI DI EQUIVALENZA} \\ \text{COME ABBIANO DEFINITO} \\ \text{PRIMA} \end{array}$$

$$[1]_3 \cdot [2]_3 = [1 \cdot 2]_3 = [2]_3$$

SI PUÒ VEDERE CHE SONO CONGRUENTI IN $(\mathbb{Z}, +, \cdot)$

ANELLI QUOTIENTE DI $(\mathbb{Z}, +, \cdot)$

$(\mathbb{Z}_m, +, \cdot)$ lo chiamiamo anello quoziante di $(\mathbb{Z}, +, \cdot)$, infatti:

- TAVOLA DI QUOTIENTE UNO
- $(\mathbb{Z}_m, +)$ è un gruppo $\rightarrow [1]_3 + [2]_3 = [3]_3 = [0]_3 \rightarrow$ ELEMENTO NEUTRO IN $(\mathbb{Z}_m, +)$
 - (\mathbb{Z}_m, \cdot) è un gruppo $\rightarrow [2]_3 : [2]_3 = [4]_3 = [1]_3 \rightarrow$ ELEMENTO NEUTRO IN (\mathbb{Z}_m, \cdot)

ALTRI (\mathbb{Z}_m, \cdot) NON HANNO L'INVERSO!

CSEMPI:

In \mathbb{Z}_6 , $[2]_6 \cdot [3]_6 = [0]_6 \rightarrow \mathbb{Z}_6$ NON È UN DOMINIO DI INTEGRITÀ

\downarrow DIVISORI DI 0 CON .

TEOREMA

Se $m \in \mathbb{Z} \setminus \{0\}$ è un numero:

- 1) $(\mathbb{Z}_m, +, \cdot)$ è un campo
- 2) $(\mathbb{Z}_m, +, \cdot)$ è un dominio di integrità
- 3) m è primo

DIM

1) \rightarrow 2) E' ovvio perché ogni campo è un dominio di integrità.

VOGLIO FAR VEDERE CHE m HA SOLO
DIVISORI BANALI

2) \rightarrow 3) Considero $m = a \cdot b$, allora:

$$[m]_m = [0]_m = [a \cdot b]_m = [a]_m \cdot [b]_m$$

Siamo in un dominio di integrità, quindi vale che:

$$[a]_m = [0]_m \vee [b]_m = [0]_m \rightarrow \text{caso est} \quad [a]_m \cdot [b]_m = [0]_m$$

Suppongo $a \not\equiv_m 0$, cioè $(\exists x \in \mathbb{Z})(a = k \cdot m)$, cioè $a - 0 = km$

↳ Allora $m = a \cdot b = k \cdot m \cdot b$, quindi, dato che m è concrollabile, $1 = k \cdot b$

↳ Allora $b = \pm 1$ e $a = \pm m \rightarrow$ Allora m è irriducibile, quindi primo.

3) \rightarrow 1) Considero $[a]_m \neq [0]_m \rightarrow$ VOGLIO FAR VEDERE TUTTI GLI ELEMENTI NON NULLI SONO RESTO DI DE INVERTIBILI AFFINCHÉ SIA UN CAMPO

Posso scegliere $0 < a' < |m|$

m è irriducibile, cioè $\text{DIV}(m) = \{1, -1, m, -m\}$

Quindi $\text{MCD}(a, m) = \{-1, 1\}$

Per il teorema di Bezout, trovo $u, v \in \mathbb{Z}$ tali che

$$1 = a \cdot u + m \cdot v$$

SE AGGIUNGO UN MULTIPLO DI m NON CAMBIA NULLA

$$\text{Quindi } [1]_m = [\overbrace{a \cdot u + m \cdot v}^{\sim}]_m = [a \cdot u]_m = [a]_m \cdot [u]_m$$

Quindi $[a]_m$ è invertibile $\rightarrow (\mathbb{Z}_m, +, \cdot)$ è un campo

EQUAZIONI DIOFANTEE

Si sono $a, b, c \in \mathbb{Z}$

$\epsilon[a, b, c]: (m, n) \in \mathbb{Z} \times \mathbb{Z} \mapsto a \cdot m + b \cdot n - c \in \mathbb{Z}$

ESEMPIO:

$$\bullet \epsilon[1, 2, 3](10, -2) = 1 \cdot 10 + 2(-2) - 3 = 3$$

$\epsilon[a, b, c]$ si chiama equazione diophantea di
1° grado e due incognite con termini a, b, c .
Sinteticamente scrivo " $a \cdot x + b \cdot y = c$ "

SOLUZIONE DI $\epsilon[a, b, c]$

Se $\epsilon[a, b, c](m, n) = 0$, le coppie $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ si dirà
soluzione di $\epsilon[a, b, c]$

ESEMPIO:

$$2u - 1 = k \cdot 3$$

$$2u + (-k) \cdot 3 = 1 \rightarrow u = 2$$

$$(u, k) = (2, -1)$$

TEOREMA

Si sono $a, b \in \mathbb{Z} \setminus \{0\}$ e sia $d \in \text{MCD}(a, b)$.

Allora sono equivalenti:

1) Il teorema di Bezout

2) a e b sono esprimibili e solo x :

$$(\exists u, v \in \mathbb{Z})(1 = a \cdot u + b \cdot v)$$

3) $\langle a, b \rangle = d \cdot \mathbb{Z}$ in $(\mathbb{Z}, +)$

4) L'equazione diophantea $a \cdot x + b \cdot y = c$ ha soluzioni
 x e solo x di c

DIM

1) \rightarrow 2)

(\rightarrow) Per Bézout, dato che a e b sono coprimi

vuol dire che $1 \in \text{MCD}(a, b)$ e quindi $1 = a \cdot u + b \cdot v$

SUL TEOREMA PRIMA DEL VALORE ASSOLUTO HO CASO DI BÉZOUT,

(\leftarrow) $d | a \wedge d | b$, quindi $d | 1$, quindi $1 \in \text{MCD}(a, b)$,

PER IPOTESI $d \in \text{MCD}(a, b)$ cioè sono coprimi

DAL TEOREMA DI BÉZOUT
 $au + bv = 1$

2) \rightarrow 3)

(\subseteq) $a, b \in d\mathbb{Z}$ dato che $d \in \text{MCD}(a, b)$

$\langle a, b \rangle$ è il più piccolo sottogruppo che contiene a, b , ma $d\mathbb{Z}$ è un sottogruppo di \mathbb{Z} , quindi $\langle a, b \rangle \subseteq d\mathbb{Z}$

(\supseteq) Siamo $a = a_1 \cdot d$ e $b = b_1 \cdot d$

Poiché $d \in \text{MCD}(a, b)$, ho che $a_1 \in b_1$ sono

TUTTI I DIVISORI COMUNI SONO IND.

Coprimi \rightarrow Per 2), trovo due numeri $u, v \in \mathbb{Z}$ tali che $1 = a_1 u + b_1 v$ → MOLTIPLICATO TUTTO PER d

Quindi $d = au + bv \in \langle a, b \rangle$, cioè $d\mathbb{Z} \subseteq \langle a, b \rangle$

ESSENDO $au + bv$ SOMME DI a E b VARIE VOLTE

$d \in \langle a, b \rangle$, QUINDI d È TUTTI I SUOI MULTIPLI APPARTENGONO A $\langle a, b \rangle$

3) \rightarrow 4)

(\rightarrow) Ci sono $m, n \in \mathbb{Z}$: $am + bn = c$

Ma dato che $d | a \wedge d | b$, allora $d | c$

(\leftarrow) Sia $d | c$, allora $c \in d\mathbb{Z}$ ma $d\mathbb{Z} = \langle a, b \rangle$

per 3). cioè $(\exists m, n \in \mathbb{Z})(c = am + bn) \rightarrow$ L'EQUAZIONE DI FERANTE HA SOLUZIONI

COSÌ SI SCRIVONO GLI ELEMENTI DEI SOTTOGRUPPI GENERATI DA a E b

4) \rightarrow 1) Se prendo $d = c$, per le 4), vuol dire che $ax + by = d$ ha soluzioni, cioè $(\exists m, n \in \mathbb{Z})(cm + bn = d)$

SE' PROPRIO BÉZOUT

TEOREMA

Sia $ax+by=e$ una equazione differente con soluzione (x_0, y_0) .

Allora, se $d \in \text{MCD}(a, b)$, l'insieme delle soluzioni dell'equazione è: $\{(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k) \mid k \in \mathbb{Z}\}$

POSSO FARLO PERCHE'
 $d \in \text{MCD}(a, b)$

VAL VARIARE
DI k EN \mathbb{Z}

DIM

L'insieme delle soluzioni dell'equazione $ax+by=e$ lo chiamo S e l'insieme $\{(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k) \mid k \in \mathbb{Z}\}$ lo chiamo H → VOGLIO FAR VEDERE CHE $H=S$

Sostituendo si vede che $H \subseteq S$

$$a(x_0 + \frac{b}{d}k) + b(y_0 - \frac{a}{d}k) = ax_0 + by_0 + \frac{ab}{d}k - \frac{ab}{d}k = e$$

(x_0, y_0) È SOLUZIONE PER IPOTESI E
LE HO TROVATE SOSTITUENDO LA COPPIA
DI H NELL'EQUAZIONE

(2)

Sia $(x, y) \in S$, cioè $ax+by=e=ax_0+by_0$, quindi

$$a(x-x_0) = b(y_0-y) \rightarrow \text{cioè, } ax+by = ax_0+by_0 \rightarrow ax-ax_0 = by_0-by \text{ È METTO IN EVIDENZA}$$

↪ visto che $d \in \text{MCD}(a, b)$, posso dividere tutto per d :

$$\frac{a}{d}(x-x_0) = \frac{b}{d}(y_0-y)$$

Dal lemma di Euclide, ho che, visto che a e b sono coprimi, $(\exists k, h \in \mathbb{Z}) \left(\begin{array}{l} h \cdot \frac{a}{d} = y_0 - y \\ k \cdot \frac{b}{d} = x - x_0 \end{array} \right)$ DATO CHE $\frac{a}{d} \mid y_0 - y$ E $\frac{b}{d} \mid x - x_0$ ALLORA $\frac{a}{d} \mid x - x_0$ E $h \in k$ SONO UGUALI?

Sostituisco il sistema in $\frac{a}{d}(x-x_0) = \frac{b}{d}(y_0-y)$ e ho che:

$$\frac{a}{d}(k \cdot \frac{b}{d}) = \frac{b}{d}(h \cdot \frac{a}{d}) \rightarrow h=k$$

Quindi: $x = x_0 + k \cdot \frac{b}{d}$ e $y = y_0 - k \cdot \frac{a}{d}$

↪ La soluzione generica è proprio uguale alle copie di H

1) $[41]_5 \cap \{m \in \mathbb{Z} \mid m^2 \leq 20\}$

Osserviamo:

$\bullet [41]_5 = [1]_5 = \{1 + k \cdot 5 \mid k \in \mathbb{Z}\}$

$\bullet \{m \in \mathbb{Z} \mid m^2 \leq 20\} = \{0, -1, 1, -2, 2, -3, 3, -4, 4\}$

$[41]_5 \cap \{m \in \mathbb{Z} \mid m^2 \leq 20\} = \{1, -4\}$, infatti:

DOBBIAMO TROVARE
SA QUI QUELLI
CHE POSSO
SERVIRE CORRETTAMENTE
 $1+4 \cdot 5 = 21$ è troppo grande

$$DE(1, 5) = (1, 1)$$

$\bullet DE(-1, 5) = (-1, 4) \rightarrow \text{PERCHÉ } 0 \leq n < |m|, \text{ QUINDI}$

Quindi dai fattori

$\frac{1}{5} = 0 \cdot 5 + 1$

\rightarrow IL RESTO NON PUÒ ESSERE NEGATIVO

notiamo: $[-1]_5 = [9]_5$

$$-1 = 0 \cdot 5 - 1 = (0 \cdot 5 - 5) + (5 - 1) = (-1) \cdot 5 + 1$$

• Inoltre, $[-2]_5 = [3]_5$

$\left. \begin{array}{l} \frac{-2}{5} = 0 \cdot 5 + 3 \\ \text{FINEHE' NON} \\ \text{ARRIVIAMO A} \\ \text{UNA CLASSE} \end{array} \right\} \text{BASTA AGGIUNGERE} \\ \text{(O SOTTRARRE) } 5$

$$[-3]_5 = [2]_5$$

$\left. \begin{array}{l} \frac{-3}{5} = 0 \cdot 5 + 2 \\ \text{FINEHE' NON} \\ \text{ARRIVIAMO A} \\ \text{UNA CLASSE} \end{array} \right\} \text{BASTA AGGIUNGERE} \\ \text{(O SOTTRARRE) } 5$

$$[-4]_5 = [1]_5$$

$\left. \begin{array}{l} \frac{-4}{5} = 0 \cdot 5 + 1 \\ \text{FINEHE' NON} \\ \text{ARRIVIAMO A} \\ \text{UNA CLASSE} \end{array} \right\} \text{BASTA AGGIUNGERE} \\ \text{(O SOTTRARRE) } 5$

$\frac{1}{5} = 0 \cdot 5 + 1$

AGGIUNGO E SOTTRAIGO 1

4) $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$

$\underbrace{[30]_3}_{\substack{\frac{30}{3} = 10}} = [0]_3 ; [2]_3 = [1]_3 ; \underbrace{[-8]_3}_{\substack{\frac{-8}{3} = -2 \\ \text{AGGIUNGO 3}}} = [1]_3$, si

5) $[30]_5 = [0]_5 ; [2]_5 ; [1]_5 ; [-8]_5 = [-8 + 10]_5 = [2]_5 ; [3]_5$

$\hookrightarrow 30$ È UN
MULTIPLO
DI 5

Quindi abbiamo: $[0]_5 ; [2]_5 ; [1]_5 ; [3]_5$ ma manca

$[4]_5$, quindi questo insieme non è \mathbb{Z}_5

6) $484289374098279340! \bmod 3879374 = 0$ perché

essendo il primo numero un fattoriale e maggiore del secondo tra i prodotti dei fattoriali c'è anche il secondo numero.

EQUAZIONI CONGRUENZIALI

- Sia $m \neq 0$ appartenente a \mathbb{Z} ($m \in \mathbb{Z} \setminus \{0\}$)
 - Siamo $a, b \in \mathbb{Z}$
 - Sia $\text{ec}[a, b, m]: [m]_m \in \mathbb{Z}_m \mapsto [a \cdot m - b]_m \in \mathbb{Z}_m$
 - $\text{ec}[a, b, m]$ si dice **equazione congruenziale** di primo grado con una incognita, di termini a, b e modulo m .

È come risolvere UNA EQUAZIONE DI PRIMO GRADO CON LE CLASSI DI RESTO MODULO m

Per essere sintetici le scriveremo come: $ax \equiv_m b$

- $m \in \mathbb{Z}$ si dice **soluzione** di $\text{ec}[a, b, m]$ se $\text{ec}[a, b, m]([m]_m) = [0]_m$.

Ovvvero se $a \cdot m \equiv_m b$

↓

Se m è soluzione, tutti gli interi im $[m]_m$ sono soluzioni.

ESEMPIO:

$$2x \equiv_5 4 \quad 2 \cdot 2 \equiv_5 4 \Leftrightarrow 2 \cdot \overbrace{(2 + k \cdot 5)}^{UN ALTRÒ MEMBRO DELLA CLASSE DI EQUIVALENZA [2]_5} = 4 + 2k \cdot 5 \equiv_5 4 \quad \begin{array}{l} 5 | 8 + 2k \cdot 5 - 4 \\ 5 | 2k \cdot 5 \text{ essendo} \\ 2k \cdot 5 \text{ È UN TUTTO} \end{array}$$

$$4x \equiv_2 3 \quad \text{non ha soluzione dato che } [4x]_2 = [0]_2$$

$$\text{e } [3]_2 = [1]_2. \quad \text{Quindi stiamo dicendo che } 0 \equiv_2 1$$

$4x$ È SEMPRE PARI

↪ FALSO

- Trovare soluzioni di $ax \equiv_m b$ equivale a trovare le soluzioni di $ax + my = b \rightarrow$ EPOE NOI STIPMO TUTTI QUEGLI X PER CUI ESISTA UN CERTO Y TALE CHE $ax + b$ È UN MULTIPLO DI m

↪ C'è una corrispondenza biunivoca tra le equazioni diogene e le equazioni congruenziali

TEOREMA

Diamo $a, b \in \mathbb{Z}$, $m \in \mathbb{Z} \setminus \{0\}$ e $d \in \text{MCD}(a, m)$,
allora $a \times \exists_m b$ ha soluzione x e solo se $d \mid b$

↳ Il teorema è già dimostrato perché abbiamo semplicemente sostituito b con il c dell'altro teorema.

Questo teorema ci dà informazioni sulle classi di equivalenza. Infatti, ad esempio, $3x \equiv_5 1 \leftrightarrow [3]_5[x]_5 = [1]_5$ che equivale a chiedersi se 3 ha un inverso nella classe

COROLLARIO 1

Se $m \in \mathbb{Z} \setminus \{0\}$, $[a]_m \in U(\mathbb{Z}_m)$ se e solo se $a \in m$ sono coprimi. ↳ cioè $d \neq 1$ con $d = \text{MCD}(a, m)$

COROLLARIO 2

Se $m \in \mathbb{Z} \setminus \{0\}$, $[a]_m \in U(\mathbb{Z}_m)$ se e solo se $[a]_m$ non è divisore dello zero.
POSSO FARE UN ALGORITMO PER TROVARE IL DIVISORE DELLO 0 ASSOCIATO A $[a]_m$ SE NON INVERTIBILE

DIM

$$[a]_m \text{ È DIVISORE DELLO ZERO} \Leftrightarrow (\exists [b]_m \in \mathbb{Z}_m) ([a]_m \cdot [b]_m = [0]_m)$$

↓
NELL'ESEMPIO
A PROSSIMA
PAGINA

(→) Per Assurdo, $[a]_m$ è divisore dello 0, cioè trovo $[b]_m \in \mathbb{Z}_m \setminus \{[0]_m\}$: $[a]_m \cdot [b]_m = [0]_m$
essendo $[a]_m$ invertibile allora è anche comodivisibile quindi $[b]_m = [0]_m$ ↳

(←) Per Assurdo, $[a]_m$ non è invertibile

Per il corollario 1, a ed m non sono coprimi, allora prendo $d \in \mathbb{Z}$ con $d \neq 1$: $a \cdot d = k \cdot m$.

$$\text{Quindi } [a]_m \cdot [d]_m = [a \cdot d]_m = [m]_m = [0]_m$$

ESEMPIO:

$$\begin{aligned} & \cdot a=6 \\ & \cdot m=10 \\ & \text{ZED}(6,10) \end{aligned} \quad \left. \begin{array}{l} \text{DIVISORI DI } \\ \text{PER } 3\mid 6 \\ \text{NED} \end{array} \right\} \rightarrow \begin{array}{l} \text{IL NUMERO TALE CHE} \\ \text{DIVISORI DELLO } 0 \\ \text{SIA } 5 \neq 1 \wedge 0 \leq 5 < 10 \\ \text{DIVISORI DI } 10 \text{ SONO } [5]_{10}, [6]_{10} \text{ E } [10]_{10} \\ \text{DIVISORI DI } 6 \text{ SONO } [1]_{10}, [2]_{10}, [3]_{10}, [6]_{10} \\ \text{DIVISORI DI } 5 \text{ SONO } [1]_{10}, [5]_{10} \\ \text{DIVISORI DI } 10 \text{ SONO } [1]_{10}, [2]_{10}, [5]_{10}, [10]_{10} \\ \text{DIVISORI DI } 6 \text{ SONO } [1]_{10}, [2]_{10}, [3]_{10}, [6]_{10} \\ \text{DIVISORI DI } 5 \text{ SONO } [1]_{10}, [5]_{10} \end{array} \right\}$$

$$\begin{aligned} & [5]_{10} \neq [0]_{10} \\ \Rightarrow & [6]_{10} \cdot [5]_{10} = [3 \cdot 2]_{10} \cdot [5]_{10} = [3]_{10} \cdot [2 \cdot 5]_{10} = \\ & = [3]_{10} \cdot [10]_{10} = [0]_{10} = 0 \end{aligned}$$

RISOLUZIONE EQUAZIONI CONGRUENZIALI

Sia $a, b \in \mathbb{Z}$, $m \in \mathbb{Z} \setminus \{0\}$ e dico "e" l'equazione congruenziale $ax \equiv_m b$

- Se $a' \in [a]_m$ e $b' \in [b]_m$, allora $a'x \equiv_m b'$ ha lo stesso insieme di soluzioni di "e".

ESEMPIO:

$$100x \equiv_{11} 2 \quad \begin{array}{l} \text{DEVO TROVARE UN NUMERO CHE} \\ \text{MOLTIPLICATO PER } 100 \text{ MI DIA } [2]_{11} \end{array}$$

$$1 \in [100]_{11} \rightarrow \text{DATO CHE } 100 = 3 \cdot 11 + 1$$

$$\text{Cerco la soluzione di } 1 \cdot x = x \equiv_{11} 2 \rightarrow [x] = [2]_{11}$$

- Se $k \in \mathbb{Z} \setminus \{0\}$, l'equazione $a \cdot k \cdot x \equiv_m b \cdot k$ ha lo stesso insieme di soluzioni di "e"

↳ In effetti, nelle equazioni diafamte, DATO CHE a E b
 $a \cdot k \cdot x + m \cdot k \cdot y = b \cdot k \leftrightarrow a \cdot k \cdot x + m \cdot k \cdot y = b \cdot k \rightarrow$ SONO MOLTO SIMILI
 \rightarrow ALLE E, ALLORA LO
 \rightarrow STESMO RIGIONAMENTO
 \rightarrow PUOI ESSERE RIPORTATO

ESEMPIO:

$$\begin{array}{ll} \text{MOLTIPLICO} & \text{SI PONE } \equiv \text{ E } \\ \text{PER } -1 & \text{VALORE A } \equiv_3 1 \end{array} \quad \begin{array}{l} \text{SI PONE } \equiv \text{ E } \\ \text{VALORE A } \equiv_3 1 \end{array}$$

$$-4x \equiv_3 -1 \leftrightarrow 4x \equiv_{-3} 1 \leftrightarrow 4x \equiv_3 1$$

- Se esiste $k \in \mathbb{Z}$: $a = a'k$, $b = b'k$ e $m = m'k$, l'equazione $a \cdot x \equiv_m b'$ ha lo stesso insieme di soluzioni di "e"

$$ax + my = b \leftrightarrow a \cdot k \cdot x + m \cdot k \cdot y = b \cdot k$$

ESEMPIO:

$$2x \equiv_6 4 \leftrightarrow x \equiv_3 2$$

Per ogni K congruente con (m) , l'equazione
 $aKx \equiv_m bK$ ha lo stesso insieme di soluzioni
 da " x "

- 1) Ora inversamente $[a \cdot X]_m = [b]_m \rightarrow [a \cdot K \cdot X]_m = [b \cdot K]_m$
- 2) $[a \cdot K \cdot X]_m = [b \cdot K]_m \rightarrow [a \cdot X]_m = [b]_m$ perché vista è inverso di K

ESEMPIO: trovo x inverso
come

$$5x \equiv_{19} 3 \rightarrow [5]_{19} [x]_{19} = [3]_{19}$$

TROVO
L'INVERSO

INVERTIBILE
PER LA CLASSE
CHE CLASSE
VIAZIONE
PER IL RESTO

QUESTO DEVE ESSERE POSSIBILE PER K E RESTO
IN PRIMO, ALLORA K E INVERTIBILE, CIÒ
POSSANO TROVARE UN NUMERO N, TALE
CHE $n \cdot m \equiv 1$

$$[5]_{19} \cdot [9]_{19} = [20]_{19} = [1]_{19} \rightarrow [9]_{19} \in \text{l'insieme di } [5]_{19}$$

$$\text{Quindi: } [5]_{19} \cdot [X]_{19} = [3]_{19} \leftrightarrow [5]_{19} \cdot [X]_{19} \cdot [9]_{19} = [3]_{19} \cdot [9]_{19} \leftrightarrow [X]_{19} = [12]_{19}$$

è la soluzione

METODO DI RI SOLUZIONE DI $aX \equiv_m b$

- 1) Ridurre a e b a numeri compresi tra 0 e $m-1$
- 2) Premolare $d \in \text{MCD}(a, m)$

↳ Se $d \nmid b$, l'equazione non ha soluzioni

↳ Se $d \mid b$ procedo al punto 3

- 3) Scrivo $a = a' \cdot d$, $b = b' \cdot d$ e $m = m' \cdot d$ DICO CHE:
 $d \mid b$ E $d \mid m$, dà
- Passo all'equazione $a'x \equiv_{m'} b'$ EQUIVALENTE
ALLA PRIMA

- 4) Trovo l'inverso in $(\mathbb{Z}_{m'}, \cdot)$ di $[a']_{m'}$ ecm
POSso FARLO
PERCHE' a'
e m' SONO
COPRIMI
AVENDO FATTO
IL MCD(a, m)
- l'algoritmo delle divisioni successive estese) e
 lo chiamo $[k]_{m'}$ SE QUI TROVANDO CHE
 $a'k + m'q = 1$

- 5) L'insieme delle soluzioni è $[b' \cdot k]_{m'}$

↳ E' una classe di resto modulo m/d con $d \in \text{MCD}(a, m)$

PERIODICO

• E ASSOCIATIVA
• C'È L'ELEMENTO NEUTRO
• TUTTI GLI ELEMENTI SONO INVERTIBILI } COME (\mathbb{Z}, \cdot)

Sia (g, \cdot) un gruppo e sia $x \in g$

x si dice periodico se:

$(\exists m \in \mathbb{N} \setminus \{0\})(x^m = 1_g) \rightarrow$ sarebbe $\underbrace{x \cdot x \cdot x \cdots x}_{m \text{ VOLTE}} = 1_g \rightarrow$ ELEMENTO NEUTRO

$! \exists m \in \mathbb{N}$ ($\mathbb{Z}, +$) è come dire " $m \cdot x = 0$ ", PERCHE' E' COME DIRE $\underbrace{x+x+x+\cdots+x}_{m \text{ VOLTE}} = 0$

ESEMPIO:

$(\mathbb{Z}, +)$ non ha elementi periodici diversi da 0 perché solo $0+0+0+0+\cdots+0=0$

PERIODO DI X

Il minimo $m \in \mathbb{N} \setminus \{0\}$: $x^m = 1$ si dice periodo di x e si scrive $|x| = m$

Equivalente a dire $|\langle x \rangle| = m$ ORDINE

TEOREMA

Se (g, \cdot) è un gruppo e $x \in g$ con $|x| = m \in \mathbb{N} \setminus \{0\}$, allora:

$$(\forall a, b \in \mathbb{Z})(x^a = x^b \Leftrightarrow a \equiv_m b)$$

DIN l'ALTO VERSO SI DEMOSTRA CON IL STESSO ARGOMENTO AL CONTRARIO

C'INVERSO DI $x^b \rightarrow$ ESISTE PERCHE' (g, \cdot) E' UN GRUPPO

$$(\Rightarrow) x^a = x^b \Rightarrow x = x^{a-b} = x^a \cdot x^{-b} = x^a \cdot 1_g = x^a \cdot x^b = 1_g = x^0$$

Brendo $\text{DE}(a-b, m) = (q, r)$

$$\text{Quindi } 1_g = x^{a-b} = x^{qm+r} = x^{qm} \cdot x^r = (x^m)^q \cdot x^r$$

$$\text{Per ipotesi } x^m = 1_g, \text{ quindi } (x^m)^q \cdot x^r = 1_g^q \cdot x^r = x^r$$

DATO CHE R E' DATO ALLAR DE(a-b, m)
So che $0 \leq r < m$, quindi $r=0$.

\hookrightarrow Infatti mi sono tracato che $1_g = x^r$, cioè r è il periodo di x , ed essendo il minimo dei valori compresi tra 0 e m , allora $r=0$

Cio' significa che $a \equiv_m b$ dato che $r=0$

DATO CHE
 $a-b = q \cdot m + r$,
cioe' $a-b = q \cdot m$

POLINOMI

Sia A un anello commutativo unitario (ACU)
e dico $0 = 0_A \in 0$ DELL'ANELLO

SUCCESSIONE

Una funzione da \mathbb{N} ad A si dice successione di elementi di A .

Scrivo $(a_m)_{m \in \mathbb{N}}$ per indicare che è immagine di $a \in A$, che è l'immagine di $1 \in \mathbb{Z}$ ecc...
 a_0 è l'immagine di $0 \in \mathbb{Z}$

POLINOMIO A COEFFICIENTI IN A

Dico $(a_m)_{m \in \mathbb{N}}$ un polinomio a coefficienti in A

o:

$(\exists k \in \mathbb{N})(\forall m \geq k)(a_m = 0)$ → SONO DELLE SUCCESSIONI CHE DA UN CERTO PUNTO IN POI HANNO SEMPRE IMMAGINE UGUALE A 0

COEFFICIENTI DEL POLINOMIO

Gli a_i di $(a_m)_{m \in \mathbb{N}}$, polinomio, si dicono coefficienti del polinomio

INSIEME DEI COEFFICIENTI IN A

l'insieme dei polinomi a coefficienti in A lo scrivo come $A[X]$

Inoltre, $0 := (0)_{m \in \mathbb{N}}$, ovvero, $(\forall m \in \mathbb{N})(a_m = 0)$ → SUCCESSIONE NULLA

GRADO DI f

Sia $f \in A[X] \setminus \{0\}$.
Sappiamo che esiste per definizione

il minimo $k \in \mathbb{N}$: $(\forall m > k)(a_m = 0)$ lo dico grado di f . lo scrivo come $gr(f)$

COEFFICIENTE DIRETTORE

Se $\beta \in A[X] \setminus \{0\}$, $a_{\beta(0)}$ è detto coefficiente diretore
e lo denoto $\text{ed}(\beta)$

a_0 lo dice termine nato

ESEMPIO:

$(0, 2, 0, 0, 0, 6, 0, 0, \dots, 0, \dots)$ ha grado 5

PER LA SUCCESSIONE NULLA

Definisco $\text{ed}(0) = 0$ e $g_2(0) = -\infty$

\hookrightarrow Già mi fongo in $(\mathbb{N} \cup \{-\infty\}, \leq)$ dato $-\infty$ è il valore

POLINOMIO MONICO

Se $a_{\beta(0)} = 1$ lo dice polinomio monico

SOMMA E PRODOTTO

Se $(a_m)_{m \in \mathbb{N}}$ e $(b_n)_{n \in \mathbb{N}}$ appartengono a $A[X]$, definisco:

$\cdot (a_m + b_n)_{m,n \in \mathbb{N}} = (a_m)_{m \in \mathbb{N}} + (b_n)_{n \in \mathbb{N}}$ è la somma \rightarrow SOMMA CON COMPONENTE A COMPONENTE

$\cdot \left(\sum_{i \in \mathbb{N}} a_i \cdot b_i \right)_{m \in \mathbb{N}} = (a_m)_{m \in \mathbb{N}} \cdot (b_n)_{n \in \mathbb{N}}$ è il prodotto \rightarrow IL PRODOTTO DEI SINGOLI TERMINI ESSERE TALI CHE LA SOMMA DEI PRODOTTI FAZIA IN P. NOI SOMMO I RISULTATI

ESEMPIO:

$$\cdot (1+x) \cdot (2+x^2) \rightarrow (1, 1, 0, 0, \dots) \cdot (2, 0, 1, 0, 0, \dots)$$

$$2+x^2+2x+x^3$$

$$(2, 2+0, 1+0+0, \dots)$$

Per questo,
no che $i+j=2$

$$m=2 \rightarrow i+j=2 \quad \text{QUINDI}$$

$$0+2=1+1=2$$

$$1+1=2 \quad 0=0$$

$$2+0=0 \cdot 2=0$$

TUTTE LE COMBINAZIONI

DI i E j

PER IL CHE

$i+j=2$

SENTO FARLE LA

SOMMA DI QUINDICI

$i=0 \rightarrow j=2$ E

DI QUANDO $i=1$ E $j=1$

$i=2 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=0$

$i=2 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=2$

$i=2 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

$i=1 \rightarrow j=2$

$i=0 \rightarrow j=0$

$i=1 \rightarrow j=1$

$i=0 \rightarrow j=2$

$i=1 \rightarrow j=0$

$i=0 \rightarrow j=1$

</

TEOREMA

$F[x]$, +, \cdot) è un anello commutativo unitario

- l'opposto additivo di (a_0, a_1, \dots) è $-(a_0, a_1, \dots)$

- 0 è neutro rispetto a +

- $(1, 0, 0, 0, \dots)$ è neutro rispetto a \cdot

$$\hookrightarrow (a_0, a_1, a_2, \dots) \cdot (1, 0, 0, 0, \dots) = (a_0, a_1, a_2, \dots)$$

POLINOMIO COSTANTE

Un elemento del tipo $(a, 0, 0, 0, \dots)$ si dice polinomio costante

MONOMORFISMO DI ANELLI

- $\mu: a \in A \mapsto (a, 0, 0, 0, \dots) \in F[x]$ è un monomorfismo di anelli.

- In particolare $A \xrightarrow{\sim} \text{Im } \mu$

- Per ogni $a \in A$, pongo $a := (a, 0, 0, 0, \dots)$

- Pongo $x := (0, 1, 0, 0, 0, \dots)$

$$\hookrightarrow x^2 = ?$$

$$(0, 1, 0, 0, 0, \dots) \cdot (0, 1, 0, 0, 0, \dots) = (0, 0, 1, 0, 0, \dots)$$

$$\text{Quindi } x^2 = (0, 0, 1, 0, 0, 0, \dots)$$

- È facile provare per induzione che:

$$x^m = (\underbrace{0, 0, 0, \dots, 0}_{m \text{ volte}}, 1, 0, 0, 0, \dots)$$

- Anche facile vedere che: m volte

$$\begin{aligned} a \cdot x^m &= (a, 0, 0, 0, 0, \dots) \cdot (\underbrace{0, 0, 0, \dots, 0}_{m \text{ volte}}, 1, 0, 0, \dots) = \\ &= (\underbrace{0, 0, 0, 0, \dots, 0}_{m \text{ volte}}, a, 0, 0, 0, \dots) \end{aligned}$$

• Se $m \in \mathbb{N}$ e $\text{gr}(f) = m$ con $f = (a_0, a_1, \dots, a_m, \underbrace{0, 0, \dots}_\text{SEMPRE 0})$
 ho subito che $f = a_0 + a_1 x + \dots + a_m x^m$.
 $a_m \neq 0$ per definizione di $\text{gr}(f)$ ($a_m \neq 0$ è QUELLO CHE ANCORA NON È 0)

PROPRIETÀ

Dalle distributività in $(A[x], +, \cdot)$, segue che se:

- $f, g \in A[x]$
- $m = \text{gr}(f)$
- $n = \text{gr}(g)$
- $M = \max\{m, n\}$

Allora:

$$\bullet f + g = \sum_{i=0}^M (a_i + b_i) x^i$$

$$\bullet f \cdot g = \sum_{i=0}^{m+n} \left(\sum_{j=0}^i a_j \cdot b_{i-j} \right) x^i$$

LE SOMME DI j E $i-j$ FARÀ I,
CHE È PROPRIO L'ESPOENTE DI X,
CHE NON È ALTRO CHE LA POSIZIONE
 $\rightarrow (0, 0, \dots, 0, 1, 0, 0, \dots)$ DEL PONTEGGIO

Possiamo fare un elenco dei polinomi su:

$$\mathbb{Z}[x] \rightarrow \mathbb{Z}_m[x] \text{ e c'è un isomorfismo}$$

ESEMPIO:

$$\cdot (a_m)_{m \in \mathbb{N}} \rightarrow ([a_m]_{m \in \mathbb{N}})_{m \in \mathbb{N}}$$

→ QUELLO CHE A UN CERTO POLINOMIO ASSOCIA I COEFFICIENTI CHE STANNO TUTTI NELLE CLASSE DI CONGRUENZA ASSOCIATE

GRADO NELLA SOMMA DI POLINOMI

Siamo $f, g \in A[x] \setminus \{0\}$ allora: Se $\text{gr}(f) = \text{gr}(g)$ e $\text{ed}(f) = -\text{ed}(g)$ allora $\text{gr}(f+g) < \text{gr}(f) = \text{gr}(g)$ → E' OVVIO PERCHE SE IL ED E L'OPPOSTO, QUEL GRADO SI CANCELLA E CI SARÀ 0

• Se $\text{gr}(f) \neq \text{gr}(g)$ oppure $\text{ed}(f) \neq -\text{ed}(g)$ allora:

$$\text{gr}(f+g) = \max\{\text{gr}(f), \text{gr}(g)\} \rightarrow \text{IL MASSIMO DEI GRADI}$$

GRADO NEL PRODOTTO DI POLINOMI

ESEMPIO: In $\mathbb{Z}_4[x]$:

$$(\underbrace{[1]}_{{\text{gr}(f)=1}} + \underbrace{[2]}_{{\text{gr}(g)=0}} x)(\underbrace{[2]}_{{\text{gr}(f+g)=0}})_4 = [2]_4 + \underbrace{[4]}_{{\text{gr}(f \cdot g)=0}} x = [2]_4$$

IN \mathbb{Q} NON SUCCIDE,
IL GRADO È LA
SOMMA DEI GRADI

1) Se $\text{ed}(f) \cdot \text{ed}(g) = 0$, allora $\text{gr}(f \cdot g) < \text{gr}(f) + \text{gr}(g)$

SE IL COEFFICIENTE DIRETTORE DI UN POLINOMIO A GELLA POSIZIONE AVRE' O

2) Se $\text{ed}(f) \cdot \text{ed}(g) \neq 0$, allora

$$\text{gr}(f \cdot g) = \text{gr}(f) + \text{gr}(g) \quad \text{e} \quad \text{ed}(f \cdot g) = \text{ed}(f) \cdot \text{ed}(g)$$

FORMULA DI
ADDITIONE
DEI GRADI
(F.A.G.)

QUESTA FORMULA VALE FINCHE' PER LA SUCESSIONE NULLA

$$\begin{aligned} f = 0 \quad \text{gr}(f \cdot g) &= \text{gr}(0) = -\infty = -\infty + \text{gr}(g) \\ \text{ed}(f \cdot g) &= 0 = \text{ed}(f) \cdot \text{ed}(g) \end{aligned}$$

3) Se $\text{ed}(f)$ è cancellabile, anche f è cancellabile.

In particolare se f vale la formula di addizione dei gradi

DIM

Esempio $\text{ed}(f)$ cancellabile, non è un divisore dello 0. Quindi da 2) segue che:

$\forall g \in A[X]$ vale la formula di addizione dei gradi cioè f non è divisore dello 0 e quindi è cancellabile

4) $A[X]$ è dominio di integrità se e solo se lo è

anche A \rightarrow (\rightarrow) SE $A[X]$ È UN DOMINIO DI INTEGRAZIONE, A STA CENTRO AD $A[X]$, QUINDI È ANCHE UN DOMINIO DI INTEGRAZIONE

(\leftarrow) SE A È UN DOMINIO DI INTEGRAZIONE ALLORA $A[X]$ È ANCHE L'ANELLO DI INTEGRAZIONE

5) Se $f \in A[X]$ è cancellabile e il grado di f è strettamente maggiore di 0 ($\text{gr}(f) > 0$) allora f non è invertibile

DIM

Per Assurdo, sia f invertibile e sia $g = f^{-1}$ $\text{gr}(f) + \text{gr}(g) = 0$, QUINDI

Per 2) ho che $\text{gr}(f) + \text{gr}(g) = \text{gr}(f \cdot g) = \text{gr}(1) = 0 \Rightarrow \text{gr}(f) = 0 \Rightarrow f = 0 \Rightarrow 0 \cdot g = 0$

Quindi $\text{gr}(f) = 0$

FAB VALG
PERCHÉ f
È CANCELLABILE

OSSERVAZIONE
(1,0,0,0,...) COSTANTE

6) Se A è dominio di integrità, $\mathcal{U}(A[x]) = \mathcal{U}(A)$

ESEMPIO:

SEGGI DA 5), PERCHE' GLI SINGOLARI DI 5 SONO SOLO THOSE CON GRADO 0, CIOE' THOSE CHE STANNO IN A

$$\cdot ([1]_4 + [2]_4 x)([1]_4 + [2]_4 x) = [1]_4 + [2]_4 x + [2]_4 x + ([2]_4 x)^2 = \\ = [1]_4 + \underbrace{[4]}_0 x + \underbrace{[4]}_0 x^2 = [1]_4 \rightarrow \begin{array}{l} \text{3) NON E' UN DOMINIO DI INTEGRITA'} \\ \text{E HO TROVATO DUE ELEMENTI INVERTIBILI CHE} \\ \text{NON SONO IN U(A) PERCHE' CON GRADO MAGGIORI DI 0} \end{array}$$

7) Il polinomio x non è mai invertibile (perché il $\text{ed}(x) = 1$ che è sempre comodabile) $\rightarrow \frac{1}{x} \notin A[x]$

In particolare $A[x]$ non è mai un campo

TEOREMA (DIVISIONE LUNGA) \rightarrow LA DIVISIONE TRA I POLINOMI

Sia A un anello commutativo unitario e siamo $f, g \in A[x]$. Se $\text{ed}(g) \in \mathcal{U}(A)$, esiste una ed una sola coppia $(q, r) \in A[x] \times A[x]$ tale che:

$$f = g \cdot q + r \quad \text{e} \quad \text{gr}(r) < \text{gr}(g)$$

DIV INDUZIONE DI II FORMA SU $m := \text{gr}(f)$

(ESISTENZA) Pongo $m := \text{gr}(g)$ e $n := \text{gr}(f)$.

• Se $m < m$, è ovvio perché pongo $q = 0$ e $r = f$

• Se $m \geq m$, $m \neq 0$ si voterà su $\text{ed}(g)$

Pongo $a := \text{ed}(f)$ e $b := \text{ed}(g)$ \rightarrow USO INDUZIONE DI SECONDA FORMA SU m
Sia $k = \underbrace{ab^{-1}}_{\substack{-1 \\ \text{POSSO FARLO PERCHE'}}} \cdot x^{m-m} \cdot g.$

Tras $a \cdot b^{-1} \cdot x^{m-m}$ e g vale la formula di addizione dei gradi per 2).

$$\text{Di conseguenza } \text{gr}(k) = \text{gr}(ab^{-1} \cdot x^{m-m}) + \text{gr}(g) = \\ = m - m + m = m \quad \text{e} \quad \text{ed}(k) = a.$$

Dico $h := f - k$, dunque $\text{gr}(h) < m$. \rightarrow UN POLINOMIO CHE HA IL GRADO PIÙ E IL SUO STESSO COEFFICIENTE DIRETTORE

Per induzione ci sono q_1 e r_1 tali che:

$$g - K = g \cdot q_1 + r_1 \text{ con } gr(r_1) < gr(g)$$

$$\text{Scrivo } g = g \cdot q_1 + r_1 + ab^{-1} \cdot x^{m-m} \cdot g = g(q_1 + ab^{-1} \cdot x^{m-m}) + r_1$$

NETTO IN
CALCULAZIONE g

(UNICITÀ) Siamo $(q_1, r_1) \neq (q_2, r_2)$ come da ipotesi.

$$\text{Quindi } g(q_1 - q_2) = r_2 - r_1$$

$$\hookrightarrow gr(r_2 - r_1) < (gr(g) = m)$$

Poi da 2) segue che $gr(g(q_1 - q_2)) = gr(g) + gr(q_1 - q_2) =$

$$= m + gr(q_1 - q_2) \quad \cancel{\text{il } q_1 \text{ lo ho scritto}} \rightarrow m + gr(q_1 - q_2) > m$$

NON CI INTERESSA
QUALE SIA

dato che $gr(g(q_1 - q_2)) = gr(r_2 - r_1)$, quindi

$$\text{Quindi } m + gr(q_1 - q_2) < m \quad \text{POTREI NON SCRIVERE MA } gr(q_1 - q_2) < 0$$

Di conseguenza $gr(q_1 - q_2) = -\infty$, cioè $q_1 - q_2 = 0$

Allora $q_1 = q_2$ e $r_1 = r_2$

TEOREMA

Se A è un anello fattoriale, anche $A[x]$ è fattoriale

ESEMPIO:

$\mathbb{Z}[x] \dots \mathbb{Q}[x], \mathbb{R}[x]$

7)* Inoltre, se X fosse invertibile allora dovrebbe le formule di addizione dei gradi

\hookrightarrow CHI È IL GRADO DI $\frac{1}{X}$?

Il grado di X è ± ($gr(x)=\pm 1$)

Se faccio una cosa tipo $X \cdot f = 1$, visto che $gr(x)=1$ allora dalle formule di addizione dei gradi, essendo cancellabile. Allora avrei che:

$$gr(x) + gr(f) = gr(1) = 0, \text{ ma } gr(x)=1 \text{ e dato che}$$

$$gr(x) \leq gr(x) + gr(f) \text{ io sto dicendo che } 1 \leq 0 \downarrow$$

SE X HA UNO
INVERTIBILE
ALLORA CD È
CANCELLABILE
E POLINOMI
CON LO
CANCELLABILI
SO ANCHE SESS
Sono CANCELLABILI
E PER LORO
VALGONO LE FAS

3) • $\langle g, \cdot \rangle$ è un gruppo ciclico di ordine 19: $g = \langle x \rangle$
 VEDI 19 ELEMENTI

Per definizione, $g = \langle x \rangle = \{x^m \mid m \in \mathbb{Z}\}$, di

conseguenza $g = \{x^0, x^1, x^2, \dots, x^{18}\}$

↳ $x^0 = 1_g$ (l'elemento neutro di g)

↓

$$x^m \cdot x^0 = x^{m+0} = x^m$$

Dopo x^{18} c'è x^0 perché vogliano che g ABBIA 19 ELEMENTI

$$\hookrightarrow x^{19} = x^0 = 1_g$$

$$x^m = x^m \Leftrightarrow m \equiv_{19} m \rightarrow$$

Dato che $x^0 = x^6 \Leftrightarrow 0 \equiv_6 b$ con $m = \langle x \rangle$
 DAL TEOREMA PRIMA DEI POLINOMI

Quindi possiamo vedere $g = \mathbb{Z}_{19}$ → PERÒ IN \mathbb{Z}_{19} ABBIAMO IL INVECE DEL $+$, MA LA NOTAZIONE ADDITIVA LA TEDIAMO NEGLI ESPONENTI

$$x^{23} = x^5 \cdot x^{18} = x^4(x \cdot x^{18}) = x^4 \cdot x^{19} = x^4 \cdot 1_g = x$$

↳ Infatti notiamo che $23 \equiv_{19} 4$

Quindi, dire che x ha periodo m vuol dire che

$| \langle x \rangle | = m \rightarrow$ Se $| \langle x \rangle | = 11$, allora $\langle x \rangle = \{1, x^1, x^2, x^3, \dots, x^{10}\}$
 perché $x^{11} = 1$, cioè 11 è il periodo di x

• Esiste una potenza di 5 tale che sia uguale a x

$$\hookrightarrow (x^5)^k = x? \rightarrow \text{Esiste } k \in \mathbb{N}: 5k \equiv_{19} 1$$

DOMANDA: SEACHE MEZZ MA LI FRENDAMO SOLO POSITIVI?

Anche se $\langle x \rangle = \{x^m \mid m \in \mathbb{Z}\}$, prendiamo gli esponenti solo positivi perché, in realtà, essendo il gruppo ciclico, ogni esponente negativo può essere riscritto con esponente positivo.

$$\text{ESEMPIO: } x^{-30} = x^{-30} \cdot (1_g)^2 = x^{-30} \cdot (x^{19})^2 = x^{-30} \cdot x^{38} = x^8$$

$$\text{Infatti, } \text{DE}(-30, 19) = (-, 8)$$

POTREBBE ESSERE DIFFICILE TROVARLO, COME NEL CASO DI: $5k \equiv_{19} 1$

Io voglio dire se esiste, non chi è

PERÒ VOGLIO TROVARE L'INVERSO DI $[5]_{19}$

↳ Si, esiste, perché sapremo che $[5]_{19} \cdot [k]_{19} = [1]_{19}$ esiste

x e solo x 5 e 19 sono coprimi → IN QUESTO CASO

$$k=4 \text{ PERCHÉ } 4 \cdot 5 = 20 \in 20 - 19 = 1$$

$\langle X^5 \rangle = ? \rightarrow$ cioè quanti elementi ci sono in $\langle X^5 \rangle$

$$\langle X^5 \rangle = \{ (X^5)^0, X^5, (X^5)^1, (X^5)^2, (X^5)^3, (X^5)^4, (X^5)^5, \dots \}$$

$\begin{matrix} " \\ 1 \\ g \end{matrix} \quad \begin{matrix} " \\ X^{20} \end{matrix} \quad \begin{matrix} " \\ X^{15} \end{matrix} \quad \begin{matrix} " \\ X^{10} \end{matrix} = X^{15} \cdot X = X \rightarrow$ IN REALTA' IN OGNI SOTTO-GRUPPO C'È UNA POTENZA CHE FA' L'UNITÀ PERCHÉ QUI SONO COPRIMI QUINDI AL E SEMPRE INVERTIBILE

$(X^5)^4 = X$, cioè mi sono tronato che:

$$x \in \langle X^5 \rangle \rightarrow \langle x \rangle \leq \langle X^5 \rangle \rightarrow g = \langle X^5 \rangle$$

$$\hookrightarrow q \equiv_{25} -1 \quad \text{se } q \not\equiv 0$$

↪ cioè $\langle X^5 \rangle$ a un certo punto arriva al generatore di $\langle x \rangle$, ma se ritrovo x allora ritrovo tutto g , quindi $\langle X^5 \rangle = g$

$$5) 12001 + 47^{202} (5^{36} - 15 \cdot 64) + 5 \text{ P.M. ORE}$$

↪ POST-MODULARE

Sappiamo che se somma le 5 di pomeriggio,
dopo 24 ore saremo ancora le 5 di pomeriggio,
dopo 25 ore saremo le 6 di pomeriggio

↓

$$[12001 + 47^{202} (5^{36} - 15 \cdot 64)]_{24} \rightarrow$$

Sfruttiamo le proprietà

↪ così calcoliamo il resto della DE di questo numero con 24, cioè quante ore di differenza ci sono con quelle iniziali (5 P.M.)

$$[c+b] = [c] + [b]$$

$$[c \cdot b] = [c] \cdot [b]$$

$$[12001]_{24} + [47^{202}]_{24} \cdot ([5^{36}]_{24} - [15]_{24} \cdot [64]_{24})$$

$$24 | 12000$$

$$\hookrightarrow 12001 \bmod 24 = 1, \text{ quindi } [12001]_{24} = [1]_{24}$$

$$47 \equiv_{24} -1$$

$$\hookrightarrow 47 = 48 - 1 = 2 \cdot 24 + 1 \Leftrightarrow 47 \bmod 24 = 23, \text{ quindi } [47^{202}]_{24} = [-1]_{24}$$

Bisogna scegliere il rappresentante che nego, infatti:

$$4^2 \equiv_5 16 \equiv_5 1 \quad \text{ma } 4^2 = f_4^2 = 1$$

NON POSSIAMO
FARE 23^{202}
CI CONVIENE
CONSIDERARE
UN RAPPRESENTANTE
DELLA CLASSE
PIÙ SEMPLICE

INVECE DI ANDARE
AVANTI CON IL
RAPPRESENTANTE
VADO INDietro

Quindi:

SONO IN REALTA' $[3 \cdot 5 \cdot 8 \cdot 8]_{24}$, QUINDI POSSO USARE LA COMMUTATIVITA' → FACCIO USEIRE UN 24 COSÌ LA CLASSE E' O

$$\begin{aligned} & [1200]_{24} + [47^{202}]_{24} \left([5^{36}]_{24} - [15]_{24} \cdot [69]_{24} \right) = \\ & = [1]_{24} + [-1^{202}]_{24} \left([25^{18}]_{24} - [3 \cdot 8]_{24} \cdot [5 \cdot 8]_{24} \right) = [1]_{24} + [1]_{24} \left([1^{18}]_{24} + [0]_{24} \right) = [2]_{24} \end{aligned}$$

$\in [1]_{24}$ " "

Quindi sono le 7 P.M.

Se avessi scritto $[12]_{24}$ avrebbero state le 5 A.M.

13) $4x^4 + 3x^3 + 2x + 1 : x^2 - x + 2$

SIVIOZ I COEFFICIENTI DIVISORE
E FACCIO MM-M

$\mathbb{Q}[x] \rightarrow$ POSSO FARE LA DIVISIONE PERCHÉ
ED. $(x^2 - x + 2)$ E' INVERTIBILE
LO E' PERCHE' IN \mathbb{Q}
TUTTI I NUMERI SONO INVERTIBILI

$$4x^4 + 3x^3 + 0x^2 + 2x + 1 \quad | x^2 - x + 2$$

$$\overline{4x^4 + 4x^3 + 8x^2} \quad | x^2 - x + 2$$

SOTTRAGGO

$$\begin{array}{r} // -1x^3 - 8x^2 + 2x + 1 \\ - x^3 - x^2 - 2x \end{array}$$

$$\begin{array}{r} // -7x^2 + 9x + 1 \\ -7x^2 - 7x - 19 \end{array}$$

$$\begin{array}{r} // 11x + 15 \end{array}$$

POSSIAMO FARE
LA PROVA

↪ L'ALGORITMO SI E' FERMATO PERCHE' IL GRADO
DEL RESTO E' MINORE DI $x^2 - x + 2$

$$\begin{array}{r} f = g \cdot q + r \\ \boxed{f = 8 \cdot g + r} \end{array}$$

$$4x^4 + 3x^3 + 2x + 1 = (x^2 - x + 2)(4x^2 - x - 7) + 11x + 15$$

NON POSSO
CONTINUARE
PERCHE' X
NON E' MAI
INVERTIBILE

$$\hookrightarrow \frac{1}{x} \notin \mathbb{Q}[x]$$

TEOREMA

Se un gruppo ciclico ha ordine primo allora tutti i suoi sottogruppi ciclici diversi dall'unite sono tutto quanto il gruppo

↪ PER CAPIRE VEDERE L'ESERCIZIO 3 DI OGGI!

ONOMORFISMO DI SOSTITUZIONE

Sia $f \in A[x]$ con $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$
e con $a_n \neq 0 \rightarrow$ cioè a_n è il coefficiente diretto
l'UN POLINOMIO

Sia $c \in A$. Definisco:

$$f(c) := a_0 + a_1c + a_2c^2 + \dots + a_nc^n \in A \rightarrow$$

APPARTIENE AD A PERCHE'
SONO ANCORA SOMMA E
PRODOTTO DI ELEMENTI DI A

Definisco l'omomorfismo di sostituzione:

$$f \in A[x] \mapsto f(c) \in A \rightarrow$$

DIMOSTRARE CHE E'
UN ONOMORFISMO
DI ANELLI PER ESERCIZIO

APPLICATION POLINOMIALE

Sia $f \in A[x]$, definisco l'applicazione polinomiale
di f la funzione:

$$f: c \in A \mapsto f(c) \in A \rightarrow$$

E' COME VEDIANO I → L'APPLICATION POLINOMIALE
POLINOMI IN ANALISI → X E Y = X

Se $f = a_0$, allora $(\forall c \in A)(f(c) = a_0)$

RADICI DEL POLINOMIO

Se $f(c) = 0$, c si dice radice di f.

Si vede facilmente che se $f, g \in A[x]$ e $c \in A$, allora:

APPUBI
POLINOMI

$$\left. \begin{array}{l} f + g(c) = \bar{f}(c) + \bar{g}(c) \\ f \cdot g(c) = \bar{f}(c) \cdot \bar{g}(c) \end{array} \right\} \begin{array}{l} \text{METTERA O NON METTERA} \\ \text{IL SECONDO E UGUALE} \end{array} \rightarrow$$

L'APPLICATION POLINOMIALE
E' UN ONOMORFISMO

Se c è radice di f, allora $\forall g \in A[x]$, c è
radice di fg e di gf.

TEOREMA DEL RESTO

Sia A un anello commutativo unitario,
 $f \in A[x]$ e $e \in A$.

Allora $f(e)$ è il resto della divisione lunga tra
 f e $(x-e)$

↳ POSSO FARE LA DIVISIONE
 PERCHE' IL COEFFICIENTE DIRETTORE
 DI $x-e$ E' 1, CHE E'
 CANCELLABILE

DIM ↳ SOE FARCI LA DIVISIONE LUNGA

Punto $\bar{f} = \overbrace{(x-e) \cdot \bar{q}}^{\in A[x]} + \bar{r}$ con $gr(\bar{r}) < gr(x-e)$,
 allora dato che $gr(\bar{r}) < 1$, \bar{r} è un polinomio
 costante. Quindi: $f(e) = \underbrace{(e-e)}_{e=0} \bar{q}(e) + \bar{r}(e) = \bar{r}_0$ ↳ QUINDI
 $f(e) = \bar{r}_0$
 ↳ e COSTANTE
 QUINDI LO CHIAMO r_0

NON POSSO FARE
 BX: 5 IN $\mathbb{Z}[x]$
 PERCHE' SE O 5 NON
 E' INVERTIBILE
 IN $\mathbb{Z}[x]$

TEOREMA DI RUFFINI

Sia A un anello commutativo unitario, $f \in A[x]$ e $e \in A$

Allora e è radice di f se e solo se $(x-e) | f$ ↳ DIM DEL TEOREMA
 ↳ QUINDI $f(e) = 0$,
 cioè $a_0 = 0$

↳ $\Leftrightarrow e=0$
 QUINDI e E'
 RADICE

TEOREMA DI RUFFINI GENERALIZZATO

Sia A un dominio di integrità, sia $f \in A[x]$ e
 zero $e_1, e_2, \dots, e_m \in A$, a 2 a 2 distinti. ↳ UN POLINOMIO
di $A[x]$

($\forall i, j \in \mathbb{N} (1 \leq i, j \leq m \rightarrow (e_i = e_j \Leftrightarrow i = j)) \rightarrow e_1 \neq e_5$)

Allora e_1, e_2, \dots, e_m sono radici di f se e solo se

$\prod_{i=1}^m (x - e_i)$ divide f .

↳ si legge: se esiste i da 1 ad m si $x-e$ con i

↳ cioè, $(x - e_1) \cdot (x - e_2) \cdot (x - e_3) \cdot \dots \cdot (x - e_m)$

DIM Per dimostrarlo useremo l'induzione di I forma
 (\rightarrow) su m

Basis Basis) $m=1 \rightarrow$ Per $m=1$ si vede il teorema
 di Ruffini

Primo Induttivo)

l'asserto)

Suppongo $m > 1$ e $\forall n \in \mathbb{N} \quad f \mid_{\mathbb{P}} m - 1$

Dato che e_m è radice, ho $f(e_m) = 0$, allora per Bubbini abbiamo che $f = (x - e_m) \cdot g$, cioè $x - e_m \mid f$

- Se $1 \leq i < m$, $f(e_i) = (e_i - e_m) \cdot g(e_i)$. Allora:

Dato che siamo in un dominio di integrità e che $i \neq m$ sono a due a due distinti, otteniamo $(e_i - e_m) \neq 0$, essendo $f(e_i) = 0$ perché e_i è una radice di f (per ipotesi), dunque, per le leggi di annullamento del prodotto, $g(e_i) = 0$

Quindi $(\forall i \in \mathbb{N})(1 \leq i \leq m-1 \rightarrow f(e_i) = 0) \xrightarrow{\text{E' Ogni } e_i \text{ è radice}} f \mid_{\mathbb{P}} m - 1$

Per ipotesi di induzione, allora abbiamo che:

$$f = h \cdot \prod_{i=1}^{m-1} (x - e_i), \quad \text{quindi } f = (x - e_m) \cdot g = h \cdot \prod_{i=1}^m (x - e_i)$$

PERCHE' g E' UN PRODOTTO DI $(x - e_i)$

(\leftarrow) Esiste $h \in A[x]$: $f = h \cdot \prod_{i=1}^m (x - e_i) \rightarrow$ ciascuna $(x - e_i)$ divide f

Quindi:

$f(e_j) = h(e_j) \cdot \prod_{i=1}^m (e_j - e_i) = 0$ perché, dato che $1 \leq j, i \leq m$, uno di questi i del prodotto è proprio j , quindi otterremo -ed avere nel prodotto un fattore uguale a 0.

ESEMPIO:

Si sono e_1, e_2, e_3 radici di f .

Allora il polinomio $(x - e_1)(x - e_2)(x - e_3) \mid f$ è sicuramente.

TEOREMA

Se A è un dominio di integrità, $f \in A[x] \setminus \{0_A\}$ e f ha m radici distinte, allora $m \leq \text{gr}(f)$

DIM

↪ NON POSSO AVERE PIÙ RADICI SEZ GRADO

Dieci e_1, e_2, \dots, e_m le m radici distinte di f e
dice $\prod_{i=1}^m (x-e_i) = f \rightarrow$ $\forall i \in \{1, \dots, m\}$ $(x-e_i)$

Per il teorema di Ruffini generalizzato, ho che
 $\exists h \in A[x]$ tale che $f = h \cdot g$

Se A è un dominio di integrità e $g \neq 0$, dunque
tale le formule di addizione dei gradi.

↪ $\text{gr}(f) = \text{gr}(g) + \text{gr}(h)$, ovviamente $\text{gr}(g) + \text{gr}(h) \geq \text{gr}(g)$.

Ma $\text{gr}(g)=m$ perché è il prodotto di m polinomi di
grado 1, quindi ho che $\text{gr}(f) \geq \text{gr}(g) \rightarrow m \leq \text{gr}(f)$

ATTENZIONE!

Se non siamo in un dominio di integrità, non vale.

• $f = [2]_4, x \in \mathbb{Z}_4(x)$, NON È UN DOMINIO
DI INTEGRITÀ

$f([0]_4) = [4]_4 = [0]_4$ e $f([2]_4) = [0]_4$, cioè f ha più radici
distinte anche se $\text{gr}(f)=1$ e ciò è causato dal
fatto che non siamo in un dominio di integrità

PRINCIPIO DI IDENTITÀ DEI POLINOMI

Sia A un dominio di integrità infinito.

Allora $(\forall f, g \in A[x])(f = g \Leftrightarrow \bar{f} = \bar{g})$

VEDERE LE APPLICAZIONI
POLINOMIALI
POLINOMI E' LA STESSA
COSA

PER QUESTO IN \mathbb{Z} DEFINISCE
TUTTI GLI APPLICATORI POLINOMIALI

DIM

\rightarrow E' ovvio per la definizione di applicazione polinomiale

(\Leftarrow) Definiamo $h = f - g$.

Poiché $\bar{f} = \bar{g}$, cioè $(\forall e \in A)[h(e) = \bar{h}(e) = \overline{f-g}(e) = \overline{f(e)} - \overline{g(e)} = 0]$

Poiché A è infinito, h ha infinite radici. Per il teorema precedente, allora, $h = 0$. Infatti, tenendoli in un dominio di integrità, se non fosse 0 dovrebbe avere il grado maggiore delle radici. Quindi $f = g$.

Sei ce'
INFINITE

ESEMPIO:

$$\bullet f = x^3 - x \in \mathbb{Z}_3[x]$$

$$\bar{f}([0]_3) = [0]_3^3 - [0]_3 = [0]_3$$

$$\bar{f}([1]_3) = [1]_3^3 - [1]_3 = [0]_3$$

$$\bar{f}([2]_3) = [2]_3^3 - [2]_3 = [2]_3 - [2]_3 = [0]_3$$

Quindi $\bar{f} = 0$, questo perché essendo \mathbb{Z}_3 finito qualche applicazione polinomiale deve coincidere, anche se i polinomi sono infiniti \hookrightarrow VA DA $\mathbb{Z}_3 \rightarrow \mathbb{Z}_3$

$$5) \text{ a. } x \in \text{ASSOC}(y) \Leftrightarrow x \in \text{DIV}(y) \wedge y \in \text{DIV}(x)$$

Se x è cancellabile, allora

$$\text{ASSOC}(x) = \{ u x \mid u \in U(\alpha) \}$$

ESISTONO DUE
ELEMENTI NON
NULLI CHE
SI DIVIDONO DA SOLO

$$\begin{cases} x = k y \\ y = b x \end{cases} \quad x = k b x$$

\mathbb{Z}_3 è integro? No

$$\hookrightarrow [3], [3] = [0],$$

Quindi \mathbb{Z}_3 non è integro

$$f = \bar{2}x^3 + \bar{2}x^2 \in \mathbb{Z}_5[x] \rightarrow \begin{array}{l} \text{BISOGNA TROVARE} \\ \text{UN POLINOMIO} \\ \text{MONICO E DIVISIBILE} \end{array}$$

con m INDICO $[m]$

$$\hookrightarrow f = \bar{2}(x^3 + x^2)$$

Se $\text{cd}(f)$ è cancellabile $\rightarrow f$ è cancellabile \rightarrow Allora f è ASSOC

$\downarrow \bar{2}$ è cancellabile perché invertibile ($\bar{2} \cdot \bar{5} = \bar{10} = \bar{1}$)

del tipo
 $\{ux \mid u \in U(\alpha)\}$

4 e 5 sono coprime con 9

QUINDI C'E'
ANCHE QUELLO
MONICO SE
TONGO N=1

$$\bullet \text{ Se ho } x^3 + x^2, (x^3 + x^2) \cdot \bar{2} = f \rightarrow \text{Quindi } x^3 + x^2 \in \text{DIV}(f)$$

$$\bullet \text{ Se faccio } f \cdot \bar{5} = x^3 + x^2 \rightarrow \text{Quindi } f \in \text{DIV}(x^3 + x^2)$$

Si inverso di $\bar{2}$ è $\bar{5}$

Quindi $x^3 + x^2$ è un polinomio monico ed è un associato di f perché si dividono reciprocamente

$$b. \bar{4}x^2 + \bar{8} \rightarrow \text{Anche } 4 \text{ è invertibile perché cancellabile}$$

\hookrightarrow l'inverso di 4 è $\bar{7}$ dato che:

$$\bar{7} \cdot \bar{4} = \bar{28} = \bar{1}$$

$$\bar{7}(\bar{4}x^2 + \bar{8}) = x^2 + \bar{1} \rightarrow \begin{array}{l} \text{Se moltiplico il polinomio} \\ \text{con l'inverso del coefficiente} \\ \text{direttore trovo il polinomio} \\ \text{monico associato a quel} \\ \text{polinomio} \end{array}$$

Per trovare l'inverso di $[4]_9$ avrei potuto fare le divisioni Euclidee

$$\hookrightarrow DE(4, 9) \rightarrow 9 = 2 \cdot 4 + 1$$

$$\hookrightarrow 9 - 2 \cdot 4 = 1 \rightarrow [9 - 2 \cdot 4]_9 = [1]_9 \rightarrow [-2]_9 \cdot [4]_9 = [1]_9$$

$$[-2+9]_9 \cdot [4]_9 = [1]_9 \rightarrow [\bar{7}]_9 \cdot [4]_9 = [1]_9$$

AFFIDABILITÀ IN UN ANELLO DI POLINOMI

Sappiamo che i divisori non nulli di \mathbb{Z} sono gli invertibili e gli associati di \mathbb{Z} .

Esempio:

- $f = 2x \in \mathbb{Z}[x]$, è invertibile?

$$\text{BDIV}(f) = \text{U}(\mathbb{Z}[x]) \cup \text{Assoc}(f)$$

essendo \mathbb{Z} un campo, gli invertibili sono tutti tranne lo 0

$$\{\bar{1}, \bar{2}\}$$

$$\{\bar{1}, \bar{2}, \bar{8}\}$$

Ora che $\bar{2}$ è invertibile, $\bar{2}^{-1}$ è cancellabile. L'insieme $\{f\} = \{u \cdot x \mid u \in \mathbb{Z} \setminus \{0\}\}$

Quindi $\text{BDIV}(f) = \{\bar{1}, \bar{2}, \bar{8}, \bar{2}f\} \rightarrow$ Il m. polinomio è invertibile se non è invertibile e ha solo divisori triviali (nessun divisore di f)

Presto $f = h(\bar{8})$, per la formula di addizione dei gradi abbiamo che: $1 = g^2(f) = g^2(g) + g^2(h) \rightsquigarrow g^2(h) = 0$ perché $g^2(g) > 0$

$\text{Im } \geq_i$
polinomi:

- DI GRADO 1: $x, \bar{2}x, x+\bar{1}, x+\bar{2}, \bar{2}x+\bar{1}, \bar{2}x+\bar{2}$

- DI GRADO 0: $\bar{1}, \bar{2}$, questi sono divisori di f

Infatti sono frazioni associate a $\text{BDIV}(f)$

Questi non possono essere divisori di f se non c'è il termine noto in f

TEOREMA

Se $(\mathbb{Q}, +, \cdot)$ è un campo e $x \in \mathbb{Q}$ è cancellabile,

allora

$$\text{Assoc}(x) = \{u \cdot x \mid u \in \mathbb{Q} \setminus \{0\}\} \rightarrow$$

INOLTRE, OTTO CHE
VOLGE QUESTA COSA IN
 \mathbb{Q} SONO TUTTI INVERTIBILI
TRAMMENTO LO 0

COROLLARIO

Se $(\mathbb{Q}, +, \cdot)$ è un campo, ogni polinomio non nullo di $\mathbb{Q}[x]$ è associato ad un unico polinomio monico.

Questo polinomio si dice detto rappresentante monico delle classi di f .

UNICO
DATO
PER
L'INVERSO

SAPPIAMO CHE QUESTO POLINOMIO ESISTE PERCHÉ, ESSENDO $(\mathbb{Q}, +, \cdot)$ UN CAMPO, ALLORA IL $\text{cd}(f)$ È SICURAMENTE INVERTIBILE. MOLTIPLICANDO f PER L'INVERSO DI $\text{cd}(f)$ OTTERO UNICO POLINOMIO MONICO E ASSOCIAZIONE A

TEOREMA

(A $\neq \mathbb{F}$)

Sia A un campo e sia $f \in A[X] \setminus \{0\}$, allora esistono $c \in A$ e $g_1, g_2, \dots, g_m \in A[X]$ tali che $f = c \cdot g_1 \cdots g_m$; g_1, g_2, \dots, g_m sono monici e irriducibili e la decomposizione è unica a meno dell'ordine.

DIM

→ ESSENDO UN CAMPO, QUINDI TUTTI GLI ELEMENTI SONO DIVISIBILI

A è fattoriale, allora $A[X]$ è fattoriale.

Di conseguenza l'unicità della decomposizione deriva dall'unicità della decomposizione negli omelli fattoriali e dall'unicità del polinomio monico assunto dal COROLARIO DI PRIMA.

Dobbiamo dimostrare l'esistenza DELLA DECOMPOSIZIONE per induzione di prima parola su $g_1(f)$ (che chiamiamo m).

- Se $g_1(f) = 0$, è ovvio che f si decomponga come un 0 e $c \in A$
- Suppongo $m > 0$ e vero l'esistenza per $m-1$

ESSERE FATTORIALE → HO POCO FATTORIALE
A $[X]$ è fattoriale, quindi premetto una decomposizione irriducibile di f , avendo $f = h_1 \cdot h_2 \cdots h_m$ irriducibili

Scritto:

$$\left. \begin{array}{l} g_i := cd(h_i) \cdot h_i \\ c := \prod_{i=0}^m cd(h_i) \end{array} \right\} \begin{array}{l} \text{HO FATTO DIRENTARE TUTTI GLI} \\ h_1 \cdot h_2 \cdots h_m \text{ MONICI E HO MGRUPPATO} \\ \text{TUTTI I LORO COEFFICIENTI DIRETTORI} \\ \text{IN } c, \text{ CHE E' IL PRODOTTO DI TUTTI I} \\ cd(h_1), cd(h_2), \dots, cd(h_m) \rightarrow \text{cioè LI HO MESSI} \\ \text{IN EVIDENZA} \end{array}$$

Ho così scritto f come: $f = c \cdot g_1 \cdot g_2 \cdots g_m$ con g_1, g_2, \dots, g_m monici e irriducibili.

Quindi per induzione l'assunto è vero $\forall m \in \mathbb{N}$

SEMPIO:

$$f = (\bar{2}x + 1)(\bar{3}x + \bar{2}) \in (\mathbb{Z}_5)[x]$$

E' UN CAMPO \rightarrow APPLICA
L'HOTESI

$$\cdot (\bar{2}x + \bar{1}) = \bar{2}(x + \bar{3}) \rightarrow \text{METTO IN EVIDENZA IL } \bar{2} \rightarrow \bar{2} := [\bar{2}]_5$$

$$\cdot (\bar{3}x + \bar{2}) = \bar{3}(x + \bar{4}) \rightarrow \text{METTO IN EVIDENZA IL } \bar{3} \rightarrow \bar{3} := [\bar{3}]_5 \rightarrow$$

Quindi posso scrivere $f = \bar{2} \cdot \bar{3} \cdot (x + \bar{3})(x + \bar{4}) = \bar{1} \cdot (x + \bar{3})(x + \bar{4}) = (x + \bar{3})(x + \bar{4})$

SINTESI DI COMPOSIZIONE
IN POLINOMI MONICI
E ZEROCUEBILU

TEOREMA

Sia A un campo, $f \in A[x] \setminus \{0\}$ e consideriamo $m = \text{gr}(f)$.

f è irriducibile se e solo se $m > 0$ e vale:

- | | |
|---|-----------------------------------|
| 1) $(\forall g, h \in A[x]) (f = g \cdot h \rightarrow \text{gr}(g) = m \text{ XOR } \text{gr}(h) = m)$ | } EQUIVALENTE |
| 2) $(\forall g, h \in A[x]) (f = g \cdot h \rightarrow \text{gr}(g) = 0 \text{ XOR } \text{gr}(h) = 0)$ | } PERE ALLE
ZEROCUEBILI
DUE |

DIM

\leftarrow Se $\text{gr}(f) > 0$, allora $f \notin U(A[x])$. Infatti, se A è un campo gli invertibili di $A[x]$ sono tutti gli invertibili di A .

Se $f = g \cdot h$, dato che vale 1), posso supporre $\text{gr}(g) = m$ e,

cioè di conseguenza, per la formula di addizione dei gradi,

$\text{gr}(h) = 0 \rightarrow$ MA IN UN CAMPO, LE COSTANTI SONO QUELLI INVERTIBILI,
cioè proprio quelli con gr uguale a 0.

$\hookrightarrow h \in U(A[x]) \rightarrow$ Ci sono solo divisori banali \rightarrow f è INVERTIBILE

INFATTI f
E' INVERTIBILE
ASSOCIATO

DEFINIZIONE DI IRRIDUCIBILE

\rightarrow Se $f \in U(A[x]) = U(A) = A \setminus \{0\}$ e $\text{DIV}(f) = \text{BDIV}(f)$,

allora $\text{gr}(f) > 0$ dato che $f \in A \setminus \{0\}$ e NON È UNA COSTANTE

Sia $f = g \cdot h$. A è un campo, quindi f è cancellabile.

Di conseguenza, $\text{BDIV}(f) = \{u \cdot f \mid u \in A \setminus \{0\}\} \cup A \setminus \{0\}$

VALUTARE XAR
VERGHE
MISTICO
SARCOIDE
OD MILD
L'EPOZIA \rightarrow f NON È INVERTIBILE

TUTTI I DIVISORI SONO SOLO QUELLI BANALI PER
PAG

ASSOCIATI
INVERTIBILI

In questo caso, $\text{gr}(f) = 0 \vee \text{gr}(h) = 0 \iff \text{gr}(g) = m \vee \text{gr}(h) = m$

TEOREMA

Sia A un campo e $f \in A[x]$ $\Rightarrow f$ E UN POLINOMIO
 f ha radici in A se e solo se ha almeno un
divisore di grado l in $A[x]$

DIM

(\rightarrow) E' vero per il teorema di Ruffini

(\leftarrow) E' vero perché sappiamo che ogni polinomio di
grado l ha radici in un campo. Infatti
se ho $kx+h$, posso premoltiplicare:

$\hookrightarrow e = -hk^{-2}$ che è radice del polinomio.

$\rightarrow f = g(kx+h)$ ha radice perché $kx+h$ c'ha

PER L'IRRIDUCIBILITA' DI UN POLINOMIO ANDIAMO A VEDERE
TEOREMA \rightarrow SE HA RADICI, PERCHÉ PERCORSI TUTTI I BON(f) PUÒ
RISULTARE MOLTO DIFFICILE

Se A è un dominio di integrità e $f \in A[x]$, se ho
 $gr(f) > 1$ e f ha radici, allora f non è irriducibile

DIM Se $gr(f) > 1$ ed ha radici, f si può dividere
per un certo $x-c$ PER RUFFINI, e sicuramente $(x-c) \in \text{BDIV}(f)$ perché
nella formula di addizione dei gradi.

TEOREMA

Un polinomio di grado 2 o 3 su un campo è
irriducibile se e solo se non ha radici in A

DIM

(\rightarrow) Se ha delle radici allora per il teorema di prima
non è irriducibile

(\leftarrow) Se f non è irriducibile allora è divisibile da qualcosa RUFFINI, ma
per le FAG è un divisore di grado 1 o 2, cioè non lese

TEOREMA

Se un polinomio di grado maggiore di 3 su un campo A è irriducibile, allora non ha radici in A

DIM

Se avesse radici, per Ruffini si sarebbe riducibile e per la FAG il grado sarebbe minore di 3?

ESEMPIO:

$$f = (x^2 + 1)(x^2 + 1) \in \mathbb{Q}[x]$$

NON È DETTO CHE SE UN POLINOMIO NON HA RADICI ALLORA È IRRIDUCIBILE

PERCHÉ HA DUE DIVISORI $(x^2 + 1)$ E $(x^2 + 1)$
CHE NON SONO ZERI

↳ f non è irriducibile e non ha radici in \mathbb{Q}

• $2 \in \mathbb{Z}[x] \rightarrow \mathbb{Z}[x]$ NON È UN CAMPO, QUINDI $2x$ PUR AVENDO GRADO 1
NON È IRRIDUCIBILE → QUASI IRRIDUCIBILE SOLO I PRIMI E X

$2 \in U(\mathbb{Z}[x])$ perché 2 non è invertibile in \mathbb{Z}

2 è irriducibile in $\mathbb{Z}[x]$ perché non invertibile e ha solo divisori

$2x$ ha grado 1 e non è irriducibile perché è un prodotto di irriducibili

TEOREMA FONDAMENTALE DELLA ALGEBRA

NOTA: Ogni polinomio non costante di $\mathbb{C}[x]$ ha radici

↳ I NUMERI COMPLESSI

COROLLARIO

In $\mathbb{C}[x]$ gli unici irriducibili sono i polinomi di grado 1 → UN POLINOMIO NON COSTANTE DI GRADO 3 SI SCOMPONE PER RUFFINI, DATO CHE HA RADICI

↳ QUESTO SI RIPETE FINO A CHE NON HANNO TUTTI GRADO 1

TEOREMA → NO DIM

Ogni polinomio irriducibile di $\mathbb{R}[x]$ ha grado minore di 3

COROLLARIO

I polinomi irriducibili di $\mathbb{R}[x]$ sono esattamente quelli di grado 1 e quelli di grado 2 senza radici
↳ ESEMPIO: $f = x^2 + 1$ NON HA RADICI IN $\mathbb{R}[x]$

TEOREMA

Ogni polinomio su $\mathbb{R}[x]$ di grado dispari ha una radice in $\mathbb{R}[x]$

DIM

Dal teorema di Bolzano

TEOREMA \rightarrow NO DIH

I polinomi di grado 2 su \mathbb{R} hanno radici in \mathbb{R} se e solo se $\Delta \geq 0$

ESEMPIO:

$$ax^2 + bx + c$$

$$\Delta = b^2 - 4ac \rightarrow \text{Se } \Delta \geq 0 \quad x_{1,2} = \frac{-b \pm \sqrt{\Delta}}{2a}$$

RADICI IN $\mathbb{Q}[x]$

ESEMPIO.

$$\cdot 3x^4 + \frac{1}{50}x + \frac{3}{4} = \frac{1}{180}(540x^4 + 2x + 135)$$

Moltiplicando tutto per il mcm dei denominatori ho un polinomio in \mathbb{Z} , che avrà le stesse radici

↪ ogni polinomio in $\mathbb{Q}[x]$ è associato a un polinomio in $\mathbb{Z}[x]$

CRITERIO DI IRRIDUCIBILITÀ DI EISENSTEIN \rightarrow NO DIM

Sia $f = a_0 + a_1x + a_2x^2 + \dots + a_mx^m \in \mathbb{Z}[x]$ con $a_m \neq 0$

Se esiste un numero primo p :

- 1) p divide a_0, a_1, \dots, a_{m-1}
- 2) $p \nmid a_m$
- 3) $p^2 \nmid a_0$.

↓
cioè, per
trovare una
radice in

• Moltiplico
il polinomio per
il massimo comune
denominatore e
trovo un polinomio
in $\mathbb{Z}[x]$

• I COEFFICIENTI
S'ESTRAGGONO

Allora f è irriducibile in $\mathbb{Q}[x]$

ESEMPIO:

$$\cdot \frac{1}{10}x^4 + \frac{3}{50} = f$$

f ha radici in $\mathbb{Q}[x] \leftrightarrow 10 \cdot f$ ha radice in $\mathbb{Q}[x]$

$x^4 + 3 = 10f \in \mathbb{Z}[x]$ e trovo il primo p :

$$p=3 \rightarrow a_0=3, a_1=0, a_2=0, a_3=0, a_4=1 \xrightarrow{3 \nmid a_0}$$

Per il criterio di Eisenstein, f è irriducibile.

• $x^n - p$ sono tutti irriducibili in $\mathbb{Q}[x]$ per il criterio di irriducibilità di Eisenstein

↪ Questo è una differenza con $\mathbb{R}[x]$, perché in $\mathbb{R}[x]$ non ci sono irriducibili di grado superiore al terzo, invece in $\mathbb{Q}[x]$ ci sono irriducibili di qualunque grado.

TEOREMA - ~~NO DIT~~ \$f \in \mathbb{Z}[x]\$ NON NULLO

Sia \$f \in \mathbb{Z}[x] \setminus \{0\}\$, \$\deg(f) = q_m\$, \$f(0) = q_0\$ \$\rightarrow\$ ~~DOVE~~ ~~NON E' DO~~ TEOREMA

Se \$e \in \mathbb{Q}\$ e \$f(e) = 0\$, allora \$e = \frac{u}{v}\$ dove \$N | q_m\$ e
\$u | q_0\$ con \$q_0 \neq q_m\$. Esprimi

COROLARIO

Sia \$f \in \mathbb{Z}[x] \setminus \{0\}\$ monico. Allora tutte le radici razionali di \$f\$ sono intere.

PERCHE'?

\$e = \frac{u}{v}\$ per il Teorema precedente. Dato che in un polinomio monico \$q_m = 1\$, allora \$N | 1 \rightarrow e = \pm 1\$
 $\hookrightarrow N = \pm 1$

ESEMPIO:

• \$f = x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{R}[x] \rightarrow\$ Seomporre in polinomi irriducibili su \$\mathbb{R}[x]\$ e su \$\mathbb{C}[x]
So che \$(x^3 + 1) | f\$

Faccio la divisione lunga:

$$\begin{array}{r}
 \begin{array}{c} x^5 + x^4 + x^3 + x^2 + x + 1 \\ \hline \text{sottraggo} \quad x^5 + 0 + 0 + x^2 + 0 + 0 \\ \hline \rightarrow \quad x^4 + x^3 + 0 + x + 1 \\ \hline \text{sottraggo} \quad x^4 + 0 + 0 + x + 0 \\ \hline \quad x^3 + 0 + 0 + 1 \\ \hline \quad x^3 + 0 + 0 + 1 \\ \hline \quad 0 \end{array} \quad \begin{array}{c} x^3 + 1 \\ \hline x^2 + x + 1 \end{array} \\
 \end{array}$$

IN EFFETTI
\$(x^3 + 1) | f\$

Quindi, \$f = (x^2 + x + 1)(x^3 + 1)\$ SU \$\mathbb{R}[x]\$ NON ESISTONO POLINOMI IRREDUCIBILI DI GRADO SUPERIORE AL SECONDO

Noto che \$(-1)^3 + 1 = 0\$, quindi posso scomporre \$(x^3 + 1)\$ dato che ha radice \$-1 \rightarrow x+1 | x^3 + 1\$

$$(x^3 + 1) = (x+1)(x^2 - x + 1) \text{ per Ruffini}$$

posso → $x^3 + 0x^2 + 0x + 1$

FREQUENTAMENTE CON LA DIVISIONE LUNGA

$x^3 + x^2$	$x^2 - x + 1$
$-x^2$	$+1$
$-x^2 - x$	$\underline{x + 1}$

Quindi ho che:

$$f = (x^2 + x + 1)(x+1)(x^2 - x + 1)$$

Noto che Δ di $x^2 - x + 1$

è -3 e Δ di $x^2 + x + 1$

è -3

PER LA REGOLA INFATTI NON HA INFATTO DEL DISCRIMINANTE → RADICI IN REALI

↳ Quindi questi due polinomi sono irriducibili in $\mathbb{R}[x]$



$f = (x^2 + x + 1)(x+1)(x^2 - x + 1)$ è irriducibile in $\mathbb{R}[x]$

↳ $x+1 \in \mathbb{R}$ IRREDUCIBILE PERCHE' DI GRADO 1 E GLI ALTRI FATTORI SONO IRREDUCIBILI

• Scomporre f su $\mathbb{C}[x]$

Per il teorema fondamentale dell'algebra trovo

$x+1 \in \mathbb{C}$ IRREDUCIBILE

c_1 radice di $x^2 - x + 1$ e c_2 radice di $x^2 + x + 1$

Quindi posso dividere e scrivere che

$$x^2 - x + 1 = (x - c_1)(x - d_1)$$

IN REALTA' NON C'È IMPORTA CHI SANO

C'È IMPORTA CHE SAPPIANO CHE ESISTONO

Inoltre, similmente,

$$x^2 + x + 1 = (x - c_2)(x - d_2)$$



Quindi $f = (x+1)(x - c_1)(x - d_1)(x - c_2)(x - d_2)$ è

irriducibile su $\mathbb{C}[x]$ perché tutti di grado 1

POSSO ANCHE TROVARE LE SOLUZIONI DI c_1, c_2, d_1, d_2

$$c_1 = \frac{1+i\sqrt{3}}{2} \in d_1 = \frac{1-i\sqrt{3}}{2}$$

DATO CHE NEI NUMERI COMPLESSI $i = \sqrt{-1}$ $i^2 = -1$

$$c_1 = \frac{1+i\sqrt{3}}{2} \in d_1 = \frac{1-i\sqrt{3}}{2}$$

ESERCIZI + SPIEGAZIONE

LEZIONE 31

5) Esiste $n \in \mathbb{Z}$ tale che $3 | 2n - 1$?

$3 | 2n - 1 \Leftrightarrow (\exists k \in \mathbb{Z})(2n - 1 = 3k) \rightarrow$ Quando $n=2$ è soluzione.

Inoltre, $3 | 2n - 1 \Leftrightarrow [2]_3, [n]_3 = [1]_3 \rightarrow$ E' UN'EQUAZIONE CONGRUENZIALE
 \downarrow $[2]_3, [n]_3 - [2]_3 = [0]_3$

La scrittura delle classi di equivalenza è, ad esempio,

$$[2]_3 = \{y \in \mathbb{Z} | 2 \equiv_3 y\} \Leftrightarrow [2]_3 = \{y \in \mathbb{Z} | (\exists k \in \mathbb{Z})(2 - y = 3k)\}$$

Quindi $[2]_3$ sono tutte e sole le soluzioni perché 2 è una soluzione di $2n - 1 = 3k$ in \mathbb{Z} .

6) Esiste $n \in \mathbb{Z}$ tale che $23 | 79n - 1$?

Cioè $(\exists k \in \mathbb{Z})(79n - 1 = 23k)$?

$$\downarrow 79n - 1 = 23k \text{ CON } k \in \mathbb{Z}$$

Potrei applicare il teorema
di Bezout \rightarrow DEVO VEDERE I MCD TRA
 $79 \in 23$

↳ Già so che il MCD tra 79 e 23 è uno dei divisori comuni di 23 (dato che 23 è primo)

↳ Provo lo stesso con l'algoritmo delle divisioni successive

$$\hookrightarrow 79 = 23 \cdot 3 + 10$$

$$23 = 10 \cdot 2 + 3$$

$$10 = 3 \cdot 3 + 1 \leftarrow \text{MCD}$$

$$3 = 1 \cdot 1 + 0$$

Benso d|79 e d|23 \rightarrow d|10 \rightarrow d|13 \rightarrow d|1

↳ Per Bezout esistono $n, k \in \mathbb{Z}$: $1 = 79n + 23k$, quindi la risposta all'esercizio è sì. IL MCD

Di conseguenza, per trovare u e k :

$$\begin{aligned} 1 &= 10 - 3 \cdot 3 = 10 - (23 + 10 \cdot 2) \cdot 3 = 10 + 10 \cdot 6 - 23 \cdot 3 = \\ &= 10 \cdot 7 - 23 \cdot 3 = (79 - 23 \cdot 3) \cdot 7 - 23 \cdot 3 = 79 \cdot 7 - 23 \cdot 29 \end{aligned}$$

Quindi $u = 7$ e $k = -29$, PER THOVRE $u \in K$ POTREI ANCHE FAIRE UNA EQUAZIONE DIOFANTEA O DUE EQUAZIONI CONGRUENTI

$$\text{infatti } 1 = 79 \cdot 7 - 23 \cdot 29 = 553 - 552$$

$$\begin{matrix} [79]_{23} \cdot [u]_{23} = [1]_{23} \\ \times [23]_{23} \cdot [u]_{23} = [1]_{23} \end{matrix}$$

- Chiedere se $(\exists k \in \mathbb{Z})(79u + 23k = 1)$ è come chiedere se $[79]_{23}$ è invertibile

$$\hookrightarrow (\exists k \in \mathbb{Z})(79u + 23k = 1) \leftrightarrow 79u \equiv_{23} 1 \leftrightarrow [79]_{23} [u]_{23} = [1]_{23}$$

$$79u - 1 = 23 \cdot k$$

$[79]_{23}$ è invertibile



$[10]_{23}$ è invertibile

$$\hookrightarrow 10 \cdot 7 = 70 = 23 \cdot 3 + 1 \rightarrow [10]_{23} \cdot [7]_{23} = [1]_{23}$$

LEZIONE 32

4) $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ SONO PROPRIO LE UNICHE CLASSI IN \mathbb{Z}_{23}

$$[\underline{\underline{3}}0]_3, [\underline{\underline{-8}}]_3, [\underline{\underline{1}}\underline{\underline{1}}]_3$$

$$0 \text{ ANCHE. } -8 + 3 \cdot 3 = 1$$

$[\underline{\underline{-8}}]_3 = [\underline{\underline{1}}]_3$ perché $-8 = 3 \cdot 2 + 2$, che facendo ai negativi sarà $-8 = -3 \cdot 2 - 2$, ma il resto deve essere $0 \leq r < 3$

Quindi $-8 = 3 \cdot (-2) - 3 + 3 - 2 \rightarrow \text{AGGIUNGO E SOTTRAGO 3}$

$$\text{e } -8 = 3 \cdot (-2) - 3 + (3 - 2) = 3 \cdot (-3) + 1$$

NETTO IN EVIDENZA

5) $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$

$$0 \equiv \underline{\underline{3}}0 \leftarrow [30]_5, [\underline{\underline{1}}]_5, [\underline{\underline{-8}}]_5$$

NO PERCHE' MANCA CLASSE, EIOE' $[4]_5$

$$\forall (a, b \in \mathbb{Z}) ((2 \times b) \rightarrow a * b = a + b) \wedge (2 \mid b \rightarrow a * b = a + \frac{b}{2})$$

$*: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ è un'operazione perché se fissiamo sempre qual è l'immagine di una coppia

$$\hookrightarrow 10 * 7 = 17$$

$$\hookrightarrow 11 * 8 = 15$$

le coppie sono quelle che a destra o hanno un numero pari o dispari

• Questa operazione non è commutativa, infatti

$$7 * 10 = 12 \text{ che è diverso da } 10 * 7 = 17$$

$(\forall a, b \in \mathbb{Z})(a \equiv_2 b \wedge c \equiv_2 d) \rightarrow (a * c \equiv_2 b * d)$ è un'operazione congruenziale

$$\begin{array}{l} (0 \equiv_2 0) \wedge (0 \equiv_2 2) \\ \hookrightarrow \text{DATO CHE * TOGlie UN 2} \\ \text{DAI FATTORI SE } b \text{ È IL PRIMO, QUINDI} \\ \text{PER TROVARE UN CONTROESEMPIO} \\ \text{USO } b \text{ CHE HA UN SOLO 2} \\ \text{NELLA SCOMPPOSIZIONE} \\ \hookrightarrow 0 * 0 = 0 + 0/2 = 0 \neq_2 0 * 2 = 0 + 2/2 = 1 \end{array}$$

SE AVESSI PROVATO CON $0 * 4 = 0 + 4 = 2$, QUINDI AVREI AVUTO CHE $2 \equiv_2 0$

No, non è un'operazione congruenziale perché ho trovato dei valori per cui non vale l'implicazione

LEZIONE 33

$$1) 12x \equiv_7 3$$

Notiamo che $5x \equiv_7 12x \equiv_7 3$, infatti $12 = 7 \cdot 1 + 5$

$$[5]_7 \div [x]_7 = [3]_7 \leftrightarrow 12x \equiv_7 3$$

$$\begin{array}{l} 5 \cdot 3 = 7 \cdot 2 + 1, \text{ quindi } [3]_7 \text{ è l'inverso di } [5]_7 \\ [5]_7 [3]_7 = [7 \cdot 2]_7 + [1]_7 \end{array}$$

$$[x]_7 = \underbrace{[3]_7 [5]_7}_1 \cdot [x]_7 = [3]_7 [3]_7 = [0]_7 = [2]_7$$

cioè ho mostrato $[5]_7 \cdot [x]_7 = [3]_7$ per $[3]_7$
le soluzioni sono

$$\{y \in \mathbb{Z} | (\exists k \in \mathbb{Z})(y = 2 + 7k)\} = [2]_7$$

GRAFI

Un grafo è un insieme di punti e di archi.

Ecco un problema che può essere rappresentato tramite un grafo:

STRADE KALININGRAD (RUSSIA)

La teoria dei grafi nasce a Königsberg (Germania).

Queste città è attraversata dal fiume Nevez. Ci sono dei ponti che collega i vari punti della città.

Cio' che ci si chiese fu: E' possibile attraversare tutti i ponti una sola volta camminando su tutti i percorsi di terra?

IN QUESTO CASO, I PONTI SONO RAPPRESENTATI DA PREMI E LA TERRA DA PUNTI



GRAFO SEMPLICE

Sia N un insieme tale che $N \neq \emptyset$ e p una relazione binaria simmetrica e antiriflessiva su N .
 (N, p) si dice grafo (semplice) \hookrightarrow NON E' UNA RELAZIONE D'ORDINE PERCHE' SIMMETRICA

Gli elementi di N si dicono vertici del grafo.
Le coppie $\{a, b\} \subseteq N$: $a p b$ si dicono archi o lati

\hookrightarrow SONO COPPIE NON ORDINATE PERCHE' $a p b = b p a$ (SIMETRIA)

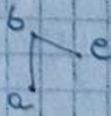
ALTRA DEFINIZIONE EQUIVALENTE DI GRAFO

Sia $N \neq \emptyset$ e sia $l \subseteq P_2(N) = \{\{x, y\} \in P(N) \mid x \neq y\}$.
 (N, l) lo dico grafo (semplice)

\hookrightarrow Posso arrivare dalla prima alla seconda definizione e viceversa. \rightarrow DALLA PRIMA ALLA SECONDA SI HA SE p E' LA RELAZIONE DI APPARTENENZA A l (E' IMM. E ANTIRIF.).
 \hookrightarrow L'INSIEME DEGLI PREMI E' UN SOTTOINSIEME DI $P_2(N)$

COME RAPPRESENTARLI?

Se $N = \{a, b, c\}$ e $l = \{\{a, b\}, \{b, c\}\}$, il grafo sarà così fatto:



MULTIGRAFO \rightarrow PIÙ ARCHI SUGLI STESSI VERTICI

Una terza di insiemi non vuoti (N, l, σ)
 si dice multigrafo se $\sigma: l \rightarrow P_2(N)$

UNA σ L'INSIEME
DEI LATI
 FUNZIONE

A l_1 ASSOCIA
 LA COPPIA
 $\{a, b\}$, A l_2
 ASSOCIA $\{b, c\}$
 ETC

ESEMPIO:

PONTI DI KÖNIGSBERG

$$N = \{a, b, c, d\}$$

$$l = \{l_1, l_2, l_3, l_4, l_5, l_6, l_7\}$$

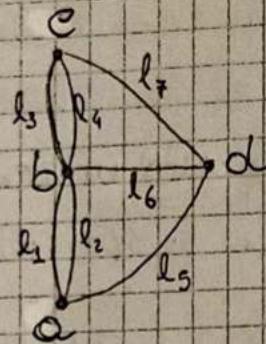
$$\sigma(l_1) = \{a, b\} = \sigma(l_2)$$

$$\sigma(l_3) = \{b, c\} = \sigma(l_4)$$

$$\sigma(l_5) = \{a, d\}$$

$$\sigma(l_6) = \{b, d\}$$

$$\sigma(l_7) = \{c, d\}$$



\hookrightarrow IL PROBLEMA STA
 NEL VOLER ATTRAVERSARE
 UNA VOLTA TUTTI
 GLI ARCHI

TERMINOLOGIA

Sia (N, l) un grafo.

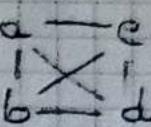
- Se $x, y \in N$ e $\{x, y\} \in l$, x e y si dicono estremi di $\{x, y\}$ e diremo che x e y sono adiacenti
 \downarrow
 e' UN PIANO TRA LORO
- Archи che hanno vertici in comune, cioè $\cap \neq \emptyset$, si dicono incidenti
- Se $x \in N$, si denota con $d(x)$ e si dice grado di x il numero di archi che contiene x \rightarrow NELL'ESEMPIO DI PRIMA, $d(a)=3$
- Se $d(x)$ è dispari (o pari), diremo che x è dispari (o pari) \rightarrow x È DISPARI

\hookrightarrow INTERSEZ
 TRA I DUE
 ARCHI

- Se $d(x)=0$, diremo che x è isolato

Un grafo si dice completo se tutti i suoi vertici sono a due a due adiacenti

↳ cioè se $\{v, P_2(v) \sim\}$, ogni vertice è collegato con tutti gli altri.
ESEMPIO:

Grafo completo a 4 vertici: 

- Un grafo completo su m vertici si denota con $K_m \rightarrow$ K DI COMPLETO (IN Tedesco)

- $(N, P_2(v) \setminus l)$ si dice grafo complementare a (N, l)
↳ HA GLI STESSI VERTICI MA GLI ARCHI SONO TUTTI SOTTRAENDO THOSE CHE NON C'ERANO PRIMA

- Se $N' \subseteq N$ e $l' \subseteq l$, allora (N', l') si dice sottografo di (N, l)
↳ ALCUNI VERTICI E ALCUNI ARCHI DI QUELLI DI PRIMA

- Se l'insieme N è finito, il (multi)grafo π dice finito

↳ Anche se si hanno una quantità infinita di archi, l'importante è che i vertici siano finiti.

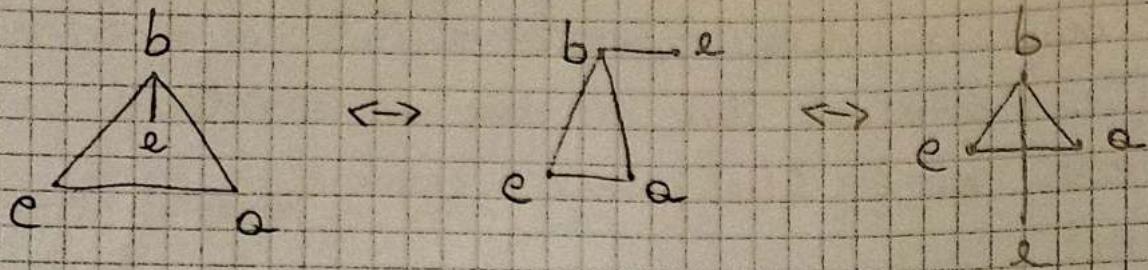
- Se (N, l) e (N', l') sono grafhi, una funzione $f: N \xrightarrow{\text{BIETTIVAMENTE}} N'$ si dice isomorfismo tra (N, l) e (N', l') se:

↳ LA FUNZIONE E BIETTIVAMENTE
UN VERTICE STA IN UN ARCO
PER E SOLO SE STA IN UN ARCO
ANCHE DELL'ALTRA PARTE
 $(\forall x, y \in N)(\{x, y\} \in l \Leftrightarrow \{f(x), f(y)\} \in l')$

↳ Si conserva il grado degli elementi di N , il numero di vertici e il numero di leti.
Per quanto riguarda le rappresentazioni grafiche, ci possono essere dei problemi perché due grafhi isomorfi possono essere rappresentati in più modi.

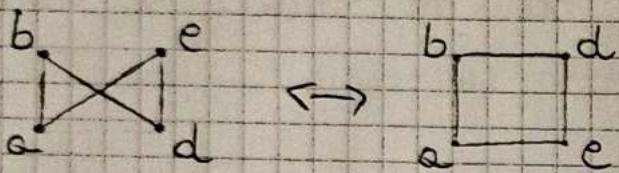
AUTOMORFISMO
SE $(N, l) = (N', l')$

MAPPRESENTAZIONE GRAFICA DI GRAFI ISO MOKI



Sono lo stesso grafo!

Ciò può essere anche più complesso, ad esempio:



GRAFO PLANARE

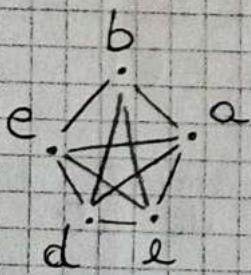
- Un grafo si dice piano o plenare se è rappresentabile su un piano senza archi che si intersecano.

Il problema dei grafi è che possiedono un grafo apparentemente non plenare ma che in realtà lo è, come nei due esempi sopra.

Se ho, ad esempio, questi due grafi:

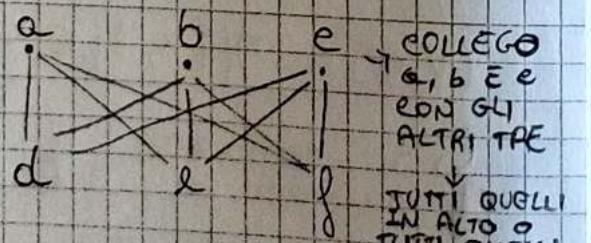
• K_5

\downarrow
GRAFO
COMPLETO
SU 5



• $K_{3,3}$

\downarrow
GRAFO
BIPARTITO



E' possibile riscrivere i grafi in modo da avere un grafo plenare? Come faccio a sapere?

↳ TEOREMA DI KURATOWSKI

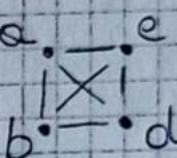
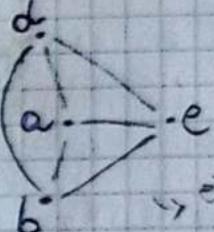
TEOREMA DI KURATOWSKI - DIM

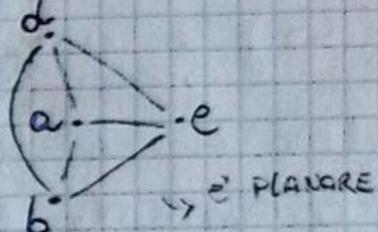
Un grafo finito è plamare se e solo se non contiene né K_5 né $K_{3,3}$ come sottografi

COROLLARIO:

K_5 e $K_{3,3}$ non sono plamari

Non è detto che un grafo completo non è plamare. → Solo i grafi completi da 5 in su non sono

ESEMPIO: K_4  \leftrightarrow 
SEMPRE NON PLANARE



TEOREMA SOMMA

Sia (v, l) un grafo finito. Allora $2|l|= \sum_{x \in v} d(x)$

SE CI SONO UN NUMERO FINITO DI VERTICI ALLORA CI SONO UN NUMERO FINITO DI LATI PERCHE' I LATI SONO UN SOTTOINSIEME DI $C_2(v)$

DIM

Sia t il numero di estremi di qualche lato.

Quindi $t=2|l| \rightarrow$ OGNI LATO HA DUE ESTREMI, QUINDI SE HO $|l|$ LATI, IL NUMERO DI ESTREMI TOTALI E' $2 \cdot |l|$

Ma ogni vertice x è estremo di $d(x)$ lati.

Di conseguenza $t=\sum_{x \in v} d(x) \rightarrow$ IL NUMERO DI ESTREMI DI QUALCHE LATO E' LA SOMMA, PER TUTTI GLI $x \in v$, DEL GRADO DI x

ALTRÉ DEFINIZIONI

Sia (v, l) un grafo.

cioè, v_1, v_2, \dots, v_n SONO VERTICI

• Siamo $v_1, v_2, \dots, v_m \in v$ tale che:

$(\forall i \in \mathbb{N}) ((1 \leq i \leq m-1) \rightarrow \{v_i, v_{i+1}\} \in l)$

TRA v_1 E v_2 C'E' UN ARCO, TRA v_2 E v_3 C'E' UN ALTRO ARCO ECC... TUTTI COLLEGATI

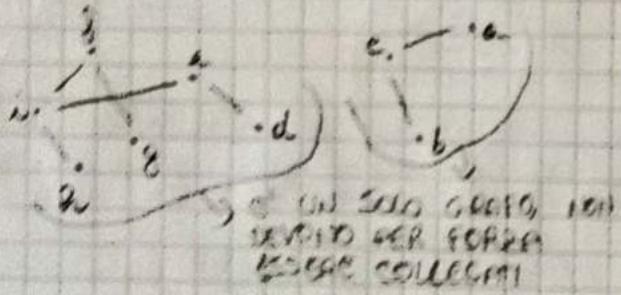
RIPETONO
e l'insieme $\{\{v_1, v_2\}, \{v_2, v_3\}, \dots, \{v_{m-1}, v_m\}\}$ ha ordine m , le m -uple $(\{v_1, v_2\}, \dots, \{v_{m-1}, v_m\})$ si dice

si dice cammino da N_1 a N_m di lunghezza m .

- Per ogni $X \in N$ aggiunge il cammino vuoto
 C_X da X a X di lunghezza 0
- Un cammino di lunghezza diversa da 0 da N_1 a N_m si dice circuito se $N_1 = N_m$
- Definisco $\gamma = (N \times N, g)$ con $g \subseteq N \times N : (N_1, N_2) \in g$
se e solo se esiste un cammino da N_1 a N_2 .
 $\hookrightarrow \gamma$ è una relazione di equivalenza su N
- Una classe di equivalenza di γ si dice componente连通子图 del grafo.

ESEMPIO:

Questo grafo ha due componenti connesse



- a, b, c sono in relazione tra di loro essendo cammini anche d, e, f, g, h, i sono in relazione tra di loro essendo cammini
- nessuno della classe dei primi 4 è in relazione con la classe di equivalenza dei ultimi 5
- quindi ci sono due componenti connesse

CAMMINO SU UN MULTIGRAFO

- Sia (V, E, O) un multigrafo, ovvero, insieme, insieme degli archi $N_1, N_2, \dots, N_m, N_{m+1} \in V$, insieme degli archi $l_1, l_2, \dots, l_m \in E$ tutti distinti: $O(l_i) = \{N_k, N_{k+1}\}$ per ogni $i \in \mathbb{N}$: $1 \leq i \leq m$. Allora (l_1, l_2, \dots, l_m) si dice cammino in questo caso nelle liste degli archi non ci sono passaggi che lo rappresentino
- Un cammino $(l_1, l_2, l_3, \dots, l_m)$ è detto euleriano se $E = \{l_1, l_2, l_3, \dots, l_m\}$ e, se esiste, segue ogni 2 passaggi EX. H.P.:

Un cammino assorbiante di due circuiti
essenziali x_1 , per x_1, x_2, \dots, x_n , fino a x_1 , che
ha che $N_x = 1$ e spiega come
essere corretto.

TEOREMA DI EULER

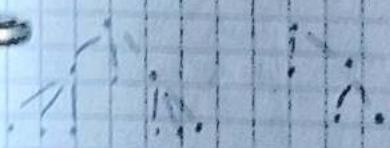
Sia G un multigrapfo aperto privo di nodi
isolati.

Allora se G non è connesso o è solo
e tutti i suoi vertici sono pari
allora non c'è un circuito assorbente con punto
di Königberg perché ogni vertice è disconnesso.

ALBERI E FORESTE

- Un grafo si dice foresta se non ha circuiti
- Un grafo si dice albero se è una foresta
ed è连通的

ESEMPIO:



È UNA FORESTA



È UN ALBERO

ogni albero ha
solamente un
vertice radice

TEOREMA

Un grafo finito (n, k) è una foresta se e solo se per ogni coppia $(x, y) \in \{1, \dots, n\}^2$ e $x \neq y$ esiste al più un cammino da x a y
ma non necessariamente un cammino

DIMOSTRAZIONE PRENDERA PAGINA

COPPIARAI ALL'ULTIMA PAGINA

se ho $x \neq y$ e ho due nodi per arrivare nel caso
che tra x e y c'è un
ciclo

DIM VOGLIO DIMOSTRARE CHE.

$$\rightarrow \exists i \rightarrow \forall n$$

(\rightarrow) • Siamo $(\{u_1, u_2\}, \{u_2, u_3\}, \dots, \{u_{m-1}, u_m\})$ e $(\{N_1, N_2\}, \{N_2, N_3\}, \dots, \{N_{m-1}, N_m\})$ due cammini distinti tra X e Y (cioè $u_1 = N_1 = X$ e $u_m = N_m = Y$)

PRENDIAMO TUTTI GLI INDICI DA 1 A m DOVE $u_i = N_i$ SI SEPARANO

• Sia $i = \{n \in \mathbb{N} \mid (\exists k \in \mathbb{N})(u_n = N_k \wedge \{u_n, u_{n+1}\} \neq \{N_k, N_{k+1}\})\}$

• Sia $\tau = \min(i)$ e sia k_τ il relativo k .

• Sia ora $j = \{n \in \mathbb{N}_0 \mid (\exists k \in \mathbb{N})(u_{n+1} = N_{k+1})\}$

PRENDIAMO TUTTI GLI INDICI DI m DOPO IL DOVE m E N SI ACCONGIUNGONO

• Sia $s = \max(j)$ e sia k_s il relativo k .

ALTRIMENTI NON POTRANNO DEFINIRE $i \in S$

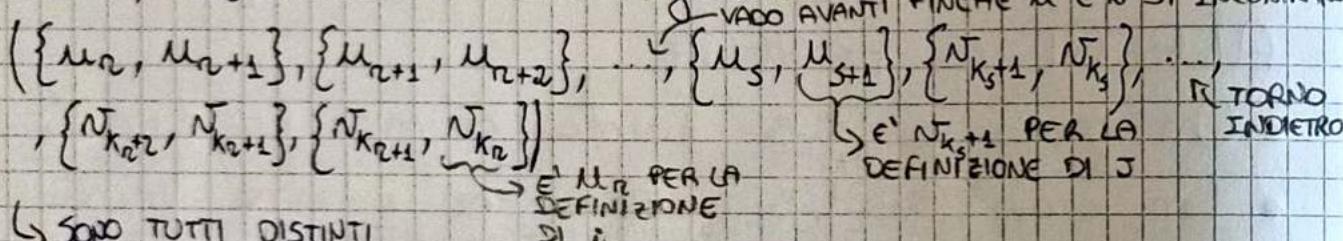
• Certo è che $k_\tau \neq k_s$

↓

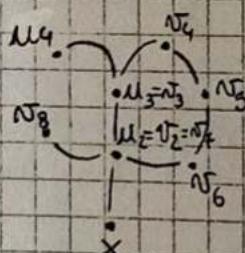
WLOG

Possò supporre, senza perdere la generalità, $k_\tau < k_s$.

Allora, il circuito \bar{i} è il seguente:



↳ SONO TUTTI DISTINTI
PERCHE' ABBIAMO PRESO I MINIMI DEI $\rightarrow \tau < s \in k_\tau < k_s$ RISPETTIVI INSIEMI



* Inizialmente ho che $u_1 = N_1 = X$, ma a un certo punto si sfidano, essendo due cammini distinti, quindi $i \neq \emptyset$

↳ Com τ prendo il primo punto in cui si sfidano, in questo

Così $i = 2$ perché il cammino \bar{i} sfidò prima a u_2 e poi a u_3 , \rightarrow IL MINIMO ESISTE FERCHÉ È UN INSIEME DI NUMERI NATURALI DIVERSO DAL VUOTO

A un certo punto i due cammini dovranno ricongiungersi dato che ho che $u_m = N_m = Y$, quindi di certo $j \neq \emptyset$

↳ Com s prendo il primo punto in cui i due cammini si ricongiungono

(\leftarrow) Per dimostrare, ci sia un circuito $(\{N_1, N_2\}, \{N_2, N_3\}, \dots, \{N_{m-1}, N_m\})$ con $N_1 = N_m$. Essendo un circuito, $m > 1 \rightarrow$ NON ESISTONO CIRCUITI SU UN SOLO ELEMENTO

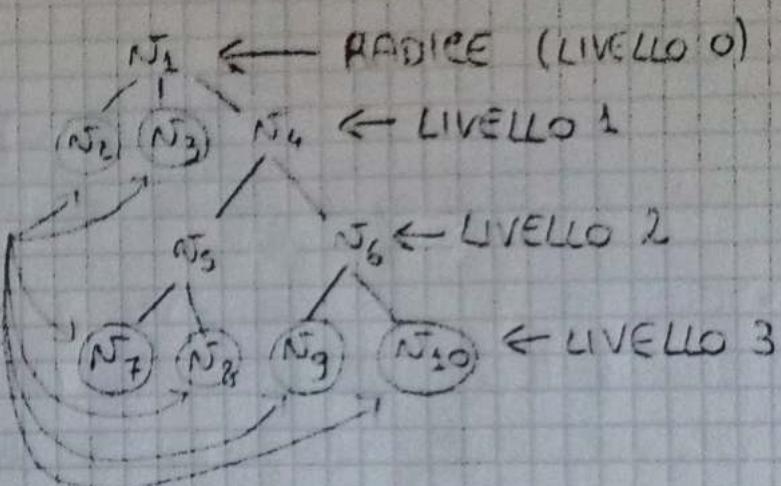
Allora $(\{N_1, N_2\})$ e $(\{N_2, N_3\}, \dots, \{N_{m-1}, N_m\}, \{N_m, N_1\})$ SONO DUE CAMMINI DISTINTI TRA $N_1 \in N_2$

APPRESENTAZIONE RADICALE DI UN ALBERO

Un esempio di rappresentazione radicale di un albero è:

- In un albero, un vertice di grado 1 si dice foglia

\hookrightarrow NON DIPENDE DAL LIVELLO



TEOREMA

Ogni albero finito con almeno due vertici ha almeno una foglia

DIM

Per Assurdo, considero l'albero privo di foglie.

Dico $N = \{N_1, N_2, \dots, N_m\}$ e sono che $|N| = m$

- Prendo $l_1 = \{N_1, N_2\}$ \Rightarrow L'ALBERO
E' FINITO

DATO CHE SE
L'ALBERO NON E' FINITO
TUTTI I VERTICI SONO CONNESSI

In questo modo sono che $d(N_1) > 2$

Essendo il grado maggiore di 2, posso trovare N_3 tale che $N_3 \notin \{N_1, N_2\}$ (dato che g è un albero \rightarrow quindi non è un circuito)

DATO CHE $N_3 \neq N_1$ E $N_3 \neq N_2$
DATO CHE N_3 DEVE ESSERE
CONNESSO A N_1 E NON HA CIRCUITI

- Dico, allora, $l_2 = \{N_1, N_3\}$, ma $d(N_1) > 2$ e così via.



Traò una successione l_1, \dots, l_m di letti distinti che collegano $m+1$ vertici distinti, ma ciò è un assurdo perché esce dall'insieme N .

TEOREMA (2)

Un albero di m vertici ha $m-1$ lati $\rightarrow |L| = m-1$

DIM

(Per induzione di I forma). • Se $m=1$ allora c'è 0 vertici, perché ci sarebbero 0 lati.

• Sia $m > 1$ e sia vero l'assunto per $m-1$

Per il teorema di prima (1) trovo una foglia X . Prendo il sottografo S di g in cui tolgo X e il suo unico ramo.

S ha $m-1$ vertici e $|L_S| = m-1$ lati.

• Per induzione, $|L_S| = m-1-1$, quindi c'è
che $|L| = m-1$

TEOREMA

Un albero finito con almeno due vertici ha almeno due foglie

DIM

Sia $|V| = m$.

IL NUMERO DI LATI DI g

Per il teorema (2), ho che $|L| = m-1$.

Per il teorema somma ho che $\sum_{x \in V} d(x) = 2(m-1)$.

Se per assurdo, ho meno di 2 foglie, allora ho almeno $m-1$ vertici di grado maggiore o

uguale a 2. \rightarrow CON m VERTICI HO SICURAMENTE ≥ 0 VERTICI HANNO GRADO MAGGIORI DI 2 QUINDI TUTTI GLI ALTRI VERTICI HANNO GRADO MAGGIORE DI 2

Ovvero $\sum_{x \in V} d(x) \geq 2(m-1) + 1$, che è un assurdo perché so che $\sum_{x \in V} d(x) = 2(m-1)$

GRADO DI $m-1$ VERTICI E 2 A CUI AGGIUNGO QUESTA UNICA FOGLIA, CHE HA GRADO 1

TEOREMA - ^{DIM}

Se $g = (V, E, \alpha)$ è un grafo finito con esattamente k componenti connesse,

allora $|E| \geq |V| - k$

↳ cioè, il numero di archi è sempre maggiore o uguale al numero di vertici meno il numero di componenti connesse

TEOREMA - ^{DIM}

Vale che, dato $g = (V, E, \alpha)$ grafo finito con k componenti connesse, $|E| = |V| - k$ se e solo se g è una foresta.

COROLLARIO

Sono equivalenti le seguenti:

- 1) g è un albero
- 2) g è un grafo connesso e $|V| = |E| + 1$
- 3) g è una foresta e $|V| = |E| + 1$

DIM

1) \rightarrow 2) Se g è un albero allora è connesso proprio per definizione di albero e per il teorema di prima vale l'uguaglianza $|E| = |V| - k$ (essendo un albero una particolare foresta).

2) \rightarrow 3) Se g è un grafo connesso allora le componenti connesse sono 1 sola, cioè, per il teorema di prima, $|E| = |V| - 1$, cioè $|V| = |E| + 1$.

Inoltre è una foresta dato che, essendoci una sola componente connessa e $|E| = |V| - 1$, allora non ci sono circuiti.

3) \rightarrow 1) Se N è una foresta e $|N| = |L| + 1$ allora per il teorema di prima abbiamo che c'è una sola componente connessa, cioè la foresta è un albero.

COROLLARI DI 5 PAGINE FA

Dal teorema secondo cui un grafo finito (N, L) è una foresta se e solo se per ogni coppia $(x, y) \in N \times N$ e $x \neq y$ (cioè di vertici distinti, dato che con uno stesso vertice non ci sarà mai un cammino) esiste al più un cammino da x a y , discendono dei corollari.

COROLLARIO

Un grafo finito g è un albero se e solo se per ogni coppia (x, y) di vertici distinti di g esiste uno e un solo cammino da x a y .

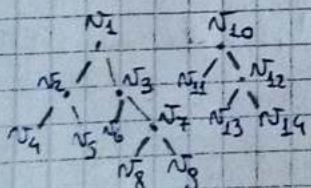
COROLLARIO

Ogni foresta finita è un grafo pomer.

DIM
La dimostrazione è una diretta conseguenza del teorema di Kuratowski, dato che sia K_5 che $K_{3,3}$ hanno dei circuiti e quindi non possono essere foreste.

ESEMPIO:

* Se ho le foreste:



Non esiste un cammino tra N_1 e N_{10} , ma il grafo è una foresta.