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	$(p \wedge (p \Rightarrow q)) \Longrightarrow q$	(legge dell'inferenza)
2.2	$(p \Rightarrow q) \iff ((\neg q) \Rightarrow (\neg p))$	(legge di contrapposizione)
2.3	$(p \Rightarrow q) \Longrightarrow ((p \Rightarrow \neg q) \Rightarrow \neg p)$	(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	$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Longrightarrow (p \Rightarrow r)$	(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	$((p \Rightarrow q) \Rightarrow p) \Longrightarrow p$	(legge di Peirce)
3.1	$p \Longrightarrow p$	(legge dell'identità)
3.2	$p \Longrightarrow (q \Rightarrow p)$	(legge dell'affermazione del conseguente)
3.3	$(\neg p) \Longrightarrow (p \Rightarrow q)$	(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 → Usare delle formule in modo corretto
Bisogna scrivere delle cose sensate usando un alfabeto → I SIMBOLI

ESEMPIO:
$\forall x \, y \, \exists \forall$ → Non ha senso

PARADOSSO DI RUSSELL

$\exists x (\underbrace{\forall y \in x, y \notin y}_{\text{PREDICATO}})$ → E' formalmente corretto

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

Il paradosso è di tipo ortografico, sintattico

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

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

} c'è una CONTRADDIZIONE
↓
ANCHE LE FRASI 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

"Epimenide è un filosofo di Creta
Epimenide dice: "Tutti i cretesi sono bugiardi""

LA FRASE È VERA O FALSA? → PARADOSSO

Questo paradosso nasce dal senso che diamo alle cose
↳ Semantica

SINTASSI → Intrecciare insieme → Prendere parti staccate mettetele insieme e formare frasi sintatticamente corrette
σύνταξη
↳ Si parte da presupposti formali

SEMANTICA → Da segno → Significare → Il significato che diamo ai simboli
σημασιολογία

Bisogna definire la $\boxed{\text{logica}}$ in maniera rigorosa, matematica
↓
DEFINIRE COSA VIENE PRIMA E COSA VIENE DOPO

LOGICA PROPOSIZIONALE

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

$\mathcal{A}$ → ALFABETO

P → VARIABILI PROPOSIZIONALI

$\mathcal{C}$ → CONNETTIVI LOGICI

$\mathcal{B}$ → PARENTESI

Una terna ordinata → PARENTESI TONDE
↓
Un insieme in cui conta l'ordine
↓
$(A, B) \neq (B, A)$

(SE $A \neq B$)
$\{A, B\} = \{B, A\}$ → PARENTESI GRAFFE
↓
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
   → NON p
3) Se f e g sono FBF, allora anche $f \wedge g$, $f \vee g$, $f \to g$, $f \leftrightarrow g$ sono FBF
   $f \wedge g$ → f e g; $f \vee g$ → f o g; $f \to g$ → f implica g; $f \leftrightarrow g$ → f se e solo se g
4) Niente 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

- $(p \to \neg q) \neg \vee p$ 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

$$\mathcal{C} = \left\{ \underset{\substack{\text{NON}\\ \text{NOT}}}{\neg}, \underset{\substack{\text{E}\\ \text{AND}}}{\wedge}, \underset{\substack{\text{O}\\ \text{OR}}}{\vee}, \underset{\substack{\text{IMPLICA}\\ \text{IMPLIES}\\ \text{IF-THEN}}}{\longrightarrow}, \underset{\substack{\text{SE E SOLO SE}\\ \text{IF AND ONLY IF}}}{\longleftrightarrow} \right\} \rightarrow$$

QUESTO È ANCHE L'ORDINE DI PRECEDENZA DEI CONNETTIVI

Potrebbe essere ambiguo $\neg p \vee q$

↳ Andiamo a dare la precedenza con le parentesi:

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

Se non trovo 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

$$v : f \rightarrow \{ \underset{\text{VERO}}{V}, \underset{\text{FALSO}}{F} \}$$

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

Definiamo $\neg$:

$v(\neg p) = V$ SE $v(p) = F$

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

$v(\neg p) = F$ SE $v(p) = V$

Definiamo $\wedge$:

$v(p \wedge q) = V$ SE E SOLO SE $v(p) = V$ E $v(q) = V$

Definiamo $\vee$:

$v(p \vee q) = V$ SE E SOLO SE $v(p) = V$ OPPURE $v(q) = V$

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

Definiamo $\rightarrow$:

$v(p \rightarrow q) = V$ SE E SOLO SE $v(p) = F$ OPPURE $v(q) = V$

Possono anche essere entrambe vere o entrambe false, ma è importante che notiamo il caso in cui $v(p) = V$ e $v(q) = F$

↳ <u>Dal vero non può seguire il falso</u>

Definiamo $\leftrightarrow$:

$v(p \leftrightarrow q) = V$ SE E SOLO SE $v(p) = V$ SE E SOLO SE $v(q) = V$

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

Se le due funzioni sono discordi allora $v(p \leftrightarrow q) = F$

TAVOLE DI VERITÀ

ESEMPIO:

- $p \wedge p$

1) Do' a p ogni possibile valore di verità

- $p \wedge p$

V	V
F	F

2) Trovo il valore di verità dell'espressione

- $p \wedge p$

V	V	V
F	F	F

Se trovo le parentesi vado a definire i valori di verità di ciò che sta al suo interno prima delle altre cose:

- $(p \wedge p) \longleftrightarrow p$

V	V	V		V
F	F	F		F

Confronto i due termini come prima

$(p \wedge p) \longleftrightarrow p$

V	V	V	V	V
F	F	F	V	F

→ 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 ANDATO A ROMA → E' 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
V	V	F	V
F	V	V	F

→ TAUTOLOGIA DEL TERZO ESCLUSO

TAUTOLOGIA E CONTRADDIZIONE

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

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

$\neg$	p	$\wedge$	$\neg q$	
V	V	F	F	V
V	F	F	V	F

→ PRINCIPIO DI NON CONTRADDIZIONE

↓

CON UN "$\neg$" UNA TAUTOLOGIA DIVENTA CONTRADDIZIONE E VICEVERSA

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

TAVOLA DI VERITÀ DELL'AND

p	∧	q
V	V	V
V	F	F
F	F	V
F	F	F

TAVOLA DI VERITÀ DELL'OR

p	V	q
V	V	V
V	V	F
F	V	V
F	F	F

TAVOLA DI VERITÀ DEL SE E SOLO SE

p	<->	q
V	V	V
V	F	F
F	F	V
F	V	F

→ Se A <-> B è una tautologia, A e B si dicono logicamente equivalenti

TAVOLA DI VERITA' DELL' IMPLICAZIONE

p	→	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 → INSALATA
NON POSSO METTERE HAMBURGER SENZA INSALATA MA POSSO FARE QUALSIASI ALTRA COMBINAZIONE

TROVARE IL VALORE DI VERITA' DI UN'ESPRESSIONE CON PIU' CONNETTIVI

1) Assegnare tutti i possibili valori di verità alle variabili

(p	∧	q)	→	p
V		V		V
V		F		V
F		V		F
F		F		F

2) Eseguire secondo l'ordine di precedenza
(Prima le parentesi, poi "¬", "∧", "∨", "→" e "↔")

(p	∧	q)	→	p
V	V	V	V	V
V	F	F	V	V
F	F	V	V	F
F	F	F	V	F

Con n variabili (ESEMPIO: p, q, r) $\to n=3$, le possibili combinazioni dei valori di verità sono 2^n.
Per non confondersi con le combinazioni bisogna assegnare alla prima variabile 2^{n-1} vere e il resto false, poi alla seconda 2^{n-2} vere e 2^{n-2} false, per poi ripetere fino alla fine, con la terza 2^{n-3} ecc...

↳ $(p \wedge q) \wedge r$

	$(p \wedge q)$	r
$2^{3-1} = 4$	V	V
	V	F
	V	V
	V	F
	F	V
	F	V
	F	F
	F	F

QUANTI CONNETTIVI BINARI ESISTONO?
Esistono 2^4 connettivi binari (16)
↳ AD ESEMPIO, $\wedge$ È SIA $p \wedge q$ (V F F) CHE $p \wedge q$ (V V V), $p \wedge q$ (F F V), $p \wedge q$ (F F F)

↳

$p \wedge q$	$p \vee q$
V	V
F	V
F	V
F	F

$p \to q$	$p \leftrightarrow q$
V	V
F	F
V	F
V	V

QUANTI CONNETTIVI UNARI ESISTONO?
Esistono 2^1 connettivi unari (2)

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

ALTRI CONNETTIVI: XOR

p	$\dot{\vee}$	q
V	F	V
V	V	F
F	V	V
F	F	F

→ POSSO ANCHE USARE "XOR" OPPURE "$\veebar$" AL POSTO DI "$\dot{\vee}$"

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

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

XOR
AUT
O DISGIUNTIVO

ALTRE TAUTOLOGIE

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

→ È CHIAMATA CONTRAPPOSIZIONE

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

→ NEGAZIONE DI →

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

ESEMPIO:

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

ma $\neg(\neg(p \to q)) \leftrightarrow \neg(p \wedge (\neg q))$ è una tautologia

↳ è la negazione della negazione di $\to$ di prima

posso unire le due espressioni che sono logicamente equivalenti

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

Se tolgo la parte al centro, otterrò una tautologia

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

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

Ne segue che anche il se è solo se è semanticamente superfluo perché viene definito a partire dall' "$\to$"

2. $(p \leftrightarrow q) \leftrightarrow ((p \to q) \wedge (q \to p))$ (NEGLI ESERCIZI 29/09/2021)

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

$$(p \leftrightarrow q) \overset{2.}{\leftrightarrow} ((p \overset{1.}{\to} q) \wedge (q \overset{1.}{\to} p)) \leftrightarrow (\neg(p \wedge (\neg q))) \wedge (\neg(q \wedge (\neg p)))$$

↳ VALGO A SOSTITUIRE

TOLGO LA PARTE AL CENTRO

$$(p \leftrightarrow q) \leftrightarrow (\neg(p \wedge (\neg q))) \wedge (\neg q \wedge (\neg p))$$ (NEGLI ESERCIZI 03/10/2021)

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

→ O ANCHE $p \mid q$

Esiste anche il NOR (not-or)

- Viene indicato con "NOR" oppure "↓"

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

NOR, NAND e NOT sono logicamente equivalenti:

p	$\mid$	p	$\longleftrightarrow$	$\neg$	p
V	F	V	V	F	V
F	V	F	V	V	F

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

$$\boxed{p \mid p \longleftrightarrow \neg p \longleftrightarrow p \downarrow p}$$

- $p \wedge q \longleftrightarrow \neg(p \mid q)$
- $p \vee q \longleftrightarrow \neg(p \downarrow q)$

STESSA COSA PER $\wedge$ USANDO $\mid$

↳ E' possibile definire $\vee$ usando solo $\downarrow$

↳ $p \vee q \longleftrightarrow \neg(p \downarrow q) \longleftrightarrow (p \downarrow q) \downarrow (p \downarrow q)$

$\downarrow$

$(p$	$\vee$	$q)$	$\longleftrightarrow$	$(p$	$\downarrow$	$q)$	$\downarrow$	$(p$	$\downarrow$	$q)$
V	V	V	V	F	V	V	V	F	V	F
V	V	F	V	F	V	F	V	F	V	F
V	F	V	V	F	V	V	V	F	V	F
F	F	F	V	V	F	F	F	V	F	V

[E' possibile dare alla macchina un solo connettivo e da lì creare gli altri → OTTIMIZZAZIONE]

	CONNETTIVI					
PROPRIETÀ	$\neg$	$\wedge$	$\vee$	$\rightarrow$	$\longleftrightarrow$	XOR
IDEMPOTENZA		✓	✓			
COMMUTATIVITÀ				✗	✓	✓
TRANSITIVA				✓		
ASSOCIATIVA		✓	✓		✓	✓
DISTRIBUTIVA		DI AND RISPETTO A OR ✓	DI OR RISPETTO A AND ✓			

ESERCIZI DEL 01/10/2021

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 → Andremo a vedere concretamente il valore di verità dei predicati

Per esempio, consideriamo:

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

$S(0)=1$ $S(S(0))=2$
$S(S(S(0)))=3$ ecc...

- $\mathbb{N}$ → INSIEME DEI NUMERI NATURALI
- $+$ → SOMMA
- $\cdot$ → PRODOTTO
- $\{0\}$ → COSTANTE
- S → FUNZIONE SUCCESSIVO
- $<$ → PREDICATO (IL MAGGIORE STRETTO)

UN ESEMPIO DI LINGUAGGIO DEL PRIMO ORDINE

ARITMETICA DEL PRIMO ORDINE

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

$x < y$ oppure $(x = y) \rightarrow \forall z (x+z = y)$ SE x E y SONO UGUALI, PER OGNI z, $x+z=y$

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

LOGICA DEL PRIMO ORDINE
DEFINIZIONE SINTATTICA

→ ALFABETO

$\mathcal{A} = (V, CON, P, F, B, CONN, Q)$ ← le frasi dovranno comunque essere i connettori, le parentesi, ma anche qualcos altro

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

↳ VARIABILI INDIVIDUALI

$CON = \{c_1, c_2, \dots\}$ → COSTANTI INDIVIDUALI → come "0"

m-arietà → IL NUMERO DI ARGOMENTI CHE IL PREDICATO COINVOLGE

$P = \{p_1^{i_1}, p_2^{i_2}, \dots\}$ → LETTERE PREDICATIVE con m-arietà

↳ ci dicono qualcosa, come il "<". → AD ESEMPIO: $5(0) < 0$

[Invece, 1+2 non è un predicato

UN ALTRO NUMERO COME LE COSTANTI ← perché è qualcosa di concreto, una funzione

↳ Il "<" è una lettera predicativa 2-aria (binaria) perché si riferisce a due termini

LE LETTERE PREDICATIVE CI DICONO QUALCOSA SULLE COSTANTI O TERMINI

$F = \{f_1^{i_1}, f_2^{i_2}, \dots\}$ → LETTERE FUNZIONALI con m-arietà

↳ Sono qualcosa di concreto, come un numero

↳ Ad esempio: 5(0) è una lettera funzionale 1-aria

+ è una lettera funzionale 2-aria

ASSOCIA A DUE NUMERI UN ALTRO NUMERO → 2+3 NON È VERO o FALSO

· è una lettera funzionale 2-aria

$B = \{(,)\} \cup \{,\}$ → ACCESSORI

$CONN = \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ → CONNETTIVI

QUANTIFICATORE UNIVERSALE → SI TROVA SCRITTO COME $\forall(x)$

$Q = \{\forall\}$ → QUANTIFICATORI

PARTI LOGICHE INVARIABILI

↳ SONO IMPLICITE IN OGNI LINGUAGGIO DEL I ORDINE

Ora che abbiamo definito l'alfabeto del linguaggio del primo ordine bisogna dire come usare questo linguaggio → S CON CHI POSSO USARLO?
S(0)? S(S(0))? S(X=Y)?

TERMINI

CIÒ A CUI POSSO APPLICARE UNA FUNZIONE

1) Ogni variabile individuale è un termine
2) Ogni costante individuale è un termine
3) Se f è una lettera funzionale n-aria e $t_1, t_2, \dots, t_n$ sono termini, allora $f(t_1, t_2, \dots, t_n)$ è un termine
4) Nient'altro è un termine

↳ 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 n-aria e $t_1, t_2, \dots, t_n$ sono termini, allora $p(t_1, t_2, \dots, t_n)$ è una FBF

AD ESEMPIO: • $\underset{t_1}{X} \underset{\text{LETTERA PREDICATIVA}}{<} \underset{t_2}{S(0)+0}$ è una FBF

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

2) Se a e b sono FBF, allora lo sono anche ¬a, a ∧ b, a ∨ b, a → b, a ↔ b, $\underbrace{(\forall X)(a)}_{\text{SI LEGGE: PER OGNI X, a}}$

AD ESEMPIO: $(\forall X)(S(0) < 0)$ è una FBF

ANCHE SE IN "a" NON C'È X VA BENE LO STESSO PERCHÉ È 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: $(S(0) < 0) = 0$ NON HA SENSO

(Arbitrario)

L'uguaglianza può essere considerato un predicato

↳ DI SOLITO VIENE ONESSO PERCHÈ IMPLICITO C'È SEMPRE

4) Niente altro è una FBF

ESEMPIO:

$$\underbrace{(X = Y)} \rightarrow (\underbrace{\forall Z\ (X + Z = Y)}) \text{ è una FBF?}$$

È UNA FBF PERCHÈ X e Y SONO TERMINI, QUINDI È UNA FBF PER LA 3

- $\forall Z$ È UNA FBF SE LO È $(X+Z=Y)$
- $X+Z$ È UNA FBF PER LA 1
- $X+Z=Y$ È UNA FBF PER LA 3

Sì, l'espressione è una FBF

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

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

PER OGNI X VALE a DOVE a È UNA FBF ← $(\forall X)(a) \longleftrightarrow a(t)$ per ogni termine t

EQUIVALE A DIRE

$(\forall X)(X < 0) \longleftrightarrow <(X, 0)$

↳ È COME DIRE $<(0,0)$
$<(1,0)$
$<(2,0)$

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

QUANTIFICATORE DI ESISTENZA (o esistenziale)

$\boxed{\neg(\forall x(\neg a)) \text{ lo definisco come } (\exists x)(a)}$

USUALE PER DEFINIZIONE

$\neg(\forall x(\neg a)) := (\exists x)(a)$ -> Si legge: esiste x tale che a

↳ uso $(\exists x)(a)$ AL POSTO DI UNA FRASE PIÙ LUNGA PER ABBREVIARE

↓ È UN'AFFERMAZ. SU a

È COME DIRE:

ESISTE UN GATTO BIANCO? ← uso $(\exists x)(a)$ al posto di una frase più lunga per abbreviare

NON TUTTI I GATTI SONO NON BIANCHI

a(x) È UNA -> FBF

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

↳ Esiste un solo x tale che a di x

ESISTE UN X E QUALUNQUE ALTRO TERMINE CHE SODDISFA a È PROPRIO X

LA FORMULA NON È PIÙ VERA SE DO A Y VALORE X

In cui x e y sono variabili distinte e y $\boxed{\text{non appare}}$ in a

VOGLIO UN UNICO X CHE FA LE COSE CHE FA X

↓

LE COSE CHE FA X LE FA SOLO X

↳ Se ad esempio ho: $\exists! x((x = y) \to \forall z(x + z = y))$ se vado a sostituire "$\exists! x$" con la sua definizione, la y della definizione va in conflitto con la y di a

↳ 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 apporti al valore di verità.

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

↳ In che senso $x < y$? Essendo variabili possiamo prendere il valore che vogliamo e il valore di verità dipenderà dalle costanti (o termini) che andremo a sostituire

↳ Si deve cercare di bloccare le variabili

↓

$\forall x (\forall y (x < y))$ → 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 → Delle FBF vere in ogni condizione

↳ AD ESEMPIO:

Sia p lettera predicativa 1-aria e c una costante

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

O ANCHE CON UNA VARIABILE

È una tautologia, sarà vera in ogni condizione

↳ Si possono costruire teoremi grazie alle tautologie

Formule vere in ogni interpretazione si dicono formule VALIDE → le formule che vengono da tautologie sono sempre valide

VARIABILI CON OCCORRENZA LIBERA ED OCCORRENZA VINCOLATA

DOVE STA X DENTRO f, DOVE SI TROVA

- Sia f una FBF, l'$\boxed{\text{occorrenza}}$ di una variabile x in f si dice vincolata se appare nella forma "$\forall x$" oppure se è presente nello scopo di un quantificatore "$\forall x$"

X È VINCOLATA

Se ho $\forall x(a)$, a si dice scopo del quantificatore

↳ DI CHE PARLA QUESTO $\forall x$? DI a

AD ESEMPIO: $(x = y) \rightarrow \forall z (x + z = y)$

- LA VARIABILE z È VINCOLATA?
- QUANTE OCCORRENZE DI z CI SONO? → 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 $\forall y$ NÉ IN UN SUO SCOPO

- Occorrenze di variabili non vincolate si dicono libere. → Posso andare a sostituire con una costante

↳ NON HA SENSO DIRE $\forall 0$

AD ESEMPIO:

$\exists x (0 < x \rightarrow 0 < y)$ → ANCHE CON $\exists x$, x È VINCOLATA PERCHÉ NON È ALTRO CHE $\neg(\forall x(\neg a))$

x → VINCOLATA, y → LIBERA

$(x = z) \rightarrow \forall z (x + z = y)$

z → LIBERA, z → VINCOLATA

Sia f una FBF ~~senza~~ variabili con occorrenze libere, si dice formula chiusa

TUTTE OCCORRENZE VARIABILI VINCOLATE

NEGLIO DIRE OCCORRENZE DI VARIABILI CHE VARIAB.

AD ESEMPIO:

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

È UNA FORMULA CHIUSA

x È NELLO SCOPO DI $\exists x$ E
y È NELLO SCOPO DI $\forall y$

ALTRI MODI DI SCRIVERE

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

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

SIGNIFICANO LA STESSA COSA

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

AD ESEMPIO:

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

POSSO SCRIVERE $f(x)$ PERCHÈ x È UNA VARIABILE LIBERA, NON POSSO SCRIVERE $f(x,z)$ PERCHÈ z NON È UNA VARIABILE LIBERA

POSSO ANCHE SCRIVERE $f(x,y)$ PERCHÈ y È LIBERA

BASTA CHE SOLO UN'OCCORRENZA È LIBERA PER SCRIVERLA

ATTENZIONE!

POSSONO ESSERCENE ANCHE ALTRE

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

Se f è una FBF con almeno n variabili libere $\to f(x_1, \dots, x_n)$ e $t_1, \dots, t_n$ sono termini, posso scrivere $f(t_1, \dots, t_n)$ dove in f: t_1 sostituisce le occorrenze libere di x_1, t_2 di x_2, ..., t_n di x_n

AD ESEMPIO:

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

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

- QUESTA FORMULA PUO' ESSERE SODDISFATTA?
  - ↳ LA PRIMA PARTE E' FALSA PERCHE $0=1$ E' FALSO E $\underset{F}{\neg}(\underset{V}{0=0})$ E' FALSO
  - ↳ LA SECONDA PARTE E' VERA PERCHE' z PUO' ESSERE UGUALE A 1
- VISTO CHE C'E' $\vee$, LA FORMULA E' VERA

NEGARE I QUANTIFICATORI

Già sappiamo come negare i connettivi, ma come negare i quantificatori?

Supponiamo di avere $B(x)$ = ESSERE BIANCO, x = GATTO } INSIEME DEI GATTI

NEGARE "PER OGNI" ↳ $\forall x(B(x))$ → OGNI GATTO E' BIANCO

↳ NEGHIAMO

↳ $\neg(\forall x(B(x)))$ → VUOL DIRE CHE C'E' UN GATTO CHE NON E' BIANCO

↳ LA NEGAZIONE NON E' "NESSUN GATTO E' BIANCO"

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

NEGARE "ESISTE" ↳ $\boxed{\neg(\exists x(\alpha)) \leftrightarrow \neg(\neg\forall x(\neg\alpha)) \leftrightarrow \forall x(\neg\alpha)}$

QUANTIFICATORI RISTRETTI

Possiamo trovare, ad esempio, una forma del tipo:

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

↳ Questa 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 2-aria p, una variabile x, un termine t ed f una FBF

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

AD ESEMPIO:

- $(\forall x<0)(x \neq x) := \overbrace{\forall x(x<0 \rightarrow x \neq x)}^{\text{È UNA FBF}}$

  ↳ È UN MODO PER ABBREVIARE → NON È UNA FBF UNA FBF

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

↳ C'È L'$\wedge$ INVECE DI $\rightarrow$

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

AD ESEMPIO:

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

INTRODUZIONE ALLA TEORIA DEGLI INSIEMI

COS'È UN INSIEME?

Sia x = variabile e φ = formula

Un insieme è: $\{x \mid \varphi\}$

TUTTI GLI x TALI CHE φ

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

↳ $\{x \mid x \notin x\}$

Partiamo dalla teoria del I ordine

↳ ci sono le variabili, quantificatori, connettivi, parentesi, virgole

L'insieme delle formule è vuoto e abbiamo $(I, \in)$ dove:

- I è una collezione di insiemi
  ↳ UNA COSA CONCRETA, COME I NUMERI IN $\mathbb{N}$
- $\in$ è appartiene
  ↳ 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 E 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 scrivo:

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

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
↳ o singoletto

È l'insieme che ha come unico elemento x

4) Scriveremo: $\varphi(x)$ È UNA FBF CON VARIABILE LIBERA x

$$\boxed{S = \{x \mid \varphi(x)\} :\longleftrightarrow \forall x (x \in S \longleftrightarrow \varphi(x))}$$ → DEFINIZIONE DI INSIEME

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

Utilizzando questo linguaggio qui, mi segue che

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

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

↳ NON USO DIRETTAMENTE x PERCHÉ NON POSSO USARE LA STESSA VARIABILE DEL QUANTIFICATORE

TEORIA DEGLI INSIEMI

$(I, \in)$

POSSO AVERE $x \in y \in z \in w$ → NON ESISTONO ELEMENTI PERCHE' OGNI ELEMENTO PUÒ ESSERE INSIEME DI QUALCOS'ALTRO

↑

$a \in \{a, b\}$ → CONCETTO PRIMITIVO DI APPARTENENZA
↳ SE ABBIAMO L'INSIEME $\{a, b\}$, ALLORA a APPARTIENE ALL'INSIEME

La teoria degli insiemi si basa su una serie di assiomi che ci dicono cos'è e cosa non è un insieme

ASSIOMI DELLA TEORIA DEGLI INSIEMI

La prima domanda da porci è: c'è qualche insieme?
↳ Esiste almeno l'insieme vuoto → l'insieme che non ha elementi

1) ASSIOMA DELL'INSIEME VUOTO

$\underbrace{\exists x}_{\text{L'INSIEME VUOTO}} \forall y (\neg (y \in x))$ → ESISTE UN x TALE CHE TUTTI GLI ALTRI INSIEMI NON SONO SUOI ELEMENTI

Insieme vuoto $= \emptyset$ → POSSO DARE UN NOME QUANDO SONO SICURO CHE L'INSIEME E' UNICO

Esiste un solo insieme vuoto? Cosa conta di un insieme?
↳ Ciò che è importante sono solo i suoi elementi

2) ASSIOMA DELL'ESTENSIONALITÀ

$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \leftrightarrow x = y)$ → PER OGNI COPPIA DI INSIEMI, QUESTI SONO UGUALI SE E SOLO SE HANNO GLI STESSI ELEMENTI

QUINDI L'INSIEME VUOTO E' UNICO ←

3) ASSIOMA DI SEPARAZIONE (O COMPRENSIONE)

Se S è un insieme e f è un predicato unario, allora $\{x \mid x \in S \wedge f(x)\}$ è un insieme
→ MEGLIO NON SCRIVERE IN QUESTA FORMA

$\{x \mid x \in S \wedge f(x)\} :\overset{DEF}{=} \{x \in S \mid f(x)\}$ → PER BREVITÀ

LA COLLEZIONE DI TUTTI GLI X TALI CHE APPARTENGONO AD S E SODDISFANO $f(x)$ → DEVE STARE PRIMA IN UN ALTRO INSIEME E NON PUO' ANCHE L'INSIEME → ENTRA CONTRADDIZIONE COME IL PARADOSSO DI RUSSELL

Dato che è impossibile scrivere l'assioma per ogni predicato, devo scrivere l'assioma in modo informale → E' UNO SCHEMA DI ASSIOMI

Questo assioma ci dice cosa non è un insieme
↳ Per trovare gli insiemi dobbiamo vedere dentro altri insiemi

• Meglio scrivere: Sia f un predicato unario, allora:

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

Oltre l'insieme vuoto, per ora, non abbiamo altri insiemi
↳ Dobbiamo trovare altri insiemi e un modo per farlo è con l'insieme delle parti

4) ASSIOMA DELLE PARTI

$\forall x \exists y \forall z (z \in y \leftrightarrow z \subseteq x)$ → PER OGNI INSIEME ESISTE UN INSIEME DELLE PARTI TALE CHE TUTTI GLI ELEMENTI DI QUESTO NUOVO INSIEME SONO TUTTI E SOLO I SOTTOINSIEME 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 assioma possiamo dire che esiste un insieme di tutti i sottoinsiemi → INOLTRE, POSSIAMO PARLARE DI INSIEME PRENDENDO UNA PARTE DELL'INSIEME

Per ogni insieme, esiste un solo insieme delle parti per x a causa dell'assioma dell'estensionalità → DUE INSIEMI DELLE PARTI HANNO COME ELEMENTI GLI STESSI ELEMENTI

Insieme delle parti di $x := \mathcal{P}(x)$

5) ASSIOMA DELLA COPPIA

$\forall x \forall y \underset{\text{INSIEME COPPIA}}{\exists z} \forall u (u \in z \longleftrightarrow (u = x \ \vee \ u = y))$ → ESISTE UN INSIEME CHE PER OGNI COPPIA DI INSIEMI CHE HO, SE U È UGUALE A X OPPURE È UGUALE A Y ALLORA U APPARTIENE A Z

↓

$\underbrace{x \in z \text{ e } y \in z}_{\text{TUTTI GLI ELEMENTI SONO O X O Y}}$

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

L'insieme coppia è unico per estensionalità

6) ASSIOMA DELL'UNIONE

$\forall f \underset{\text{INSIEME UNIONE DI } f}{\exists a} \forall y \forall x ((x \in y \wedge y \in f) \longleftrightarrow x \in a)$ → GLI ELEMENTI DI a SONO GLI ELEMENTI DEGLI ELEMENTI DI f

a insieme famiglia

Insieme unione di $f := \bigcup f$

L'insieme unione di f è unico per estensionalità

L'unione è unaria (o generalizzata) 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 vuoto X e Y e mostro che sono uguali

Siano X e Y insiemi vuoti $\rightarrow \forall z(\neg(z \in X))$ → VALE ANCHE PER Y

Sia $z \in X \rightarrow$ QUESTA COSA 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

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

entrambe che $z \in X \leftrightarrow z \in Y$

↳ Di conseguenza, per l'assioma dell'estensionalità,

$\boxed{X = Y}$

Visto che l'insieme vuoto è unico, allora per definizione

di 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 $Y \subseteq X$

Abbiamo dimostrato che $\emptyset \subseteq \emptyset$

Consideriamo, invece: $\forall x \forall z(z \in \emptyset \rightarrow z \in X)$ → SE PRENDO QUALUNQUE ELEMENTO z, SE z APPARTIENE A $\emptyset$ ALLORA APPARTIENE ANCHE A X

- PER DIRE SE È VALIDA ALLORA LA FORMULA DEVE ESSERE CHIUSA → ALTRIMENTI VALIDA O MENO NON VUOL 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):

$\forall z (z \in U \leftrightarrow z \subseteq X)$

$\forall z (z \in W \leftrightarrow z \subseteq X)$

$\underbrace{(z \in U \leftrightarrow z \subseteq X \leftrightarrow z \in W)}$

$\leftrightarrow \forall z (z \in U \leftrightarrow z \in W)$

$\downarrow$

Quindi, per l'assioma dell'estensionalità $\boxed{U = W}$

Insieme delle parti di $X := \mathcal{P}(X)$

PARTI DEL VUOTO

Dobbiamo scoprire che elementi ha $\mathcal{P}(\emptyset)$ → POSSO PARLARE DI INSIEME PER ASSIOMA 4

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

Per definizione: $X \subseteq \emptyset \overset{def}{\leftrightarrow} \forall z (z \in X \rightarrow z \in \emptyset)$

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

↳ Dobbiamo dimostrare che X non ha elementi → $X = \emptyset$

Sappiamo (dall'unicità del vuoto) che $\emptyset \overset{\text{È PARTE}}{\subseteq} \emptyset$ e sappiamo (dall'unicità del sottoinsieme delle parti) che questa è l'unica parte del vuoto

↳ Di conseguenza $\mathcal{P}(\emptyset)$ è il singleton del vuoto:

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

↳ È UN INSIEME CHE HA COME UNICO ELEMENTO IL VUOTO

↓

IL VUOTO, INVECE, NON HA ELEMENTI

ESEMPI:

- Costruiamo l'insieme delle parti delle parti del vuoto

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

↳ 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

Prendo $X \subseteq \{\emptyset\}$. Per definizione di sottoinsieme:

$\forall z (z \in X \rightarrow z \in \{\emptyset\})$ → Dobbiamo vedere quando questa frase è valida

Ci sono due possibilità:

- X potrebbe non avere elementi → $X = \emptyset$ → LA FRASE RISULTA VALIDA PERCHÉ $z \in X$ RISULTA ESSERE FALSO
- X e il $\{\emptyset\}$ hanno gli stessi elementi → $X = \{\emptyset\}$ per estensionalità
  ↳ IN QUESTO MODO SI HA $z \in \{\emptyset\} \rightarrow z \in \{\emptyset\}$, QUINDI LA FRASE È VALIDA ANCHE SE $z \in \{\emptyset\}$ È VERO

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

↳ IL NUMERO DI ELEMENTI DELLE PARTI DELLE PARTI È ESPONENZIALE: 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 → L'INSIEME COPPIA È UNICO

$\{\emptyset, \{\emptyset\}\} = \{\{\emptyset\}, \emptyset\}$ → Hanno gli stessi elementi

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

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

Per trovare l'insieme famiglia di $\mathcal{F}$, devo prendere gli elementi degli elementi di $\mathcal{F}$

$\bigcup \mathcal{F} = \{a,b,c,d,e\}$

↳ INSIEME FAMIGLIA

- PARADOSSO DI RUSSELL

Consideriamo il paradosso di Russell:

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

è un insieme?

Per assurdo, consideriamo che lo sia.

↳ $r = \{x \mid \neg(x \in x)\}$ → È 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 assurdo, quindi quella cosa non è un insieme

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

Consideriamo la condizione affinché due insiemi siano uguali per estensionalità
↳ $z \in x \rightarrow z \in y$

Chiamiamo $x = \{a\}$

$y = \{a, a, a, a\}$

Dividiamo due casi:

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

2) $z \neq a \rightarrow$ Anche in questo caso la formula è valida perché $z \in x$ è falsa $\begin{pmatrix} F \rightarrow V \\ F \rightarrow F \end{pmatrix} = V$

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

ALCUNE TAUTOLOGIE

- $\forall x (p(x) \wedge q(x)) \leftrightarrow \forall x (p(x)) \wedge \forall x (q(x))$
  ↳ Questa tautologia non vale se al posto di $\forall$ mettiamo $\exists$
  ↳ Non è detto che la x che verifica $\exists x (p(x))$ e $\exists x (q(x))$ sia la stessa, quindi non vale il $\leftrightarrow$

- $p \text{ XOR } q \leftrightarrow (p \wedge \neg q) \vee (q \wedge \neg p) \overset{\text{PROPRIETÀ DISTRIBUTIVA}}{\leftrightarrow} (p \vee q) \wedge (\neg (p \wedge q))$
  ↳ ESPLICITAZIONE DI XOR

SEPARAZIONE: Sia f un predicato unario, allora

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:

C'È UN SOLO ELEMENTO $\Rightarrow$ IL SINGLETON DI a

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

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

$a \in \{a\}$

$a \nsubseteq \{a\}$

Preso l'insieme a, a ha sicuramente il vuoto e l'insieme a come sottoinsieme

IL SINGLETON DI QUELL'UNICO ELEMENTO

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

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

LE PARTI DELLE PARTI È DATO DAI SINGLETON DEI SINGOLI ELEMENTI, GLI INSIEMI VUOTO E STESSO E LE VARIE COMBINAZIONI

$\Rightarrow 2^n$ DOVE n SONO GLI ELEMENTI

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

2 CONNETTIVI LOGICI

OPERATORI INSIEMISTICI

↳ Traduco il $\leftrightarrow$ con l' $=$ → Grazie a estensionalità

↳ Traduco l' $\rightarrow$ con $\subseteq$ → Grazie alla definizione di $\subseteq$

Siano X e Y due insiemi qualunque

- $X \cap Y = \{z \mid z \in X \wedge z \in Y\} = \{z \in X \mid \underbrace{z \in Y}_{\varphi(z)}\}$

CI TROVIAMO DENTRO X

↳ QUESTO È UN INSIEME PER L'ASSIOMA DI SEPARAZIONE → PRENDO TUTTI GLI ELEMENTI CHE SODDISFANO QUEL PREDICATO

- $X \cup Y = \{z \mid z \in X \vee z \in Y\}$ → QUESTA DEFINIZIONE NON VA BENE PERCHÉ DOBBIAMO DEFINIRE L'AMBIENTE IN CUI PRENDIAMO GLI ELEMENTI

↓

LA DEFINIZIONE NON VA BENE

↓

$X \cup Y := \bigcup\{X, Y\}$ → IN QUESTO CASO L'AMBIENTE È TUTTI GLI ELEMENTI DEGLI ELEMENTI DI QUESTA COPPIA

↳ USO ASSIOMI DELLA COPPIA E DELL'UNIONE

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

↳ È DETTO IN MODO INFORMALE, NON È LA DEFINIZIONE

- $X \Delta Y := \{z \in X \cup Y \mid z \in X \text{ XOR } z \in Y\}$ → È UN INSIEME PERCHÉ STANNO GIÀ DENTRO L'UNIONE CHE È UN INSIEME

↓

USIAMO L'ASSIOMA DI SEPARAZIONE

↓

DIFFERENZA SIMMETRICA

↓

TUTTI GLI ELEMENTI CHE O STANNO IN X O STANNO IN Y MA NON IN ENTRAMBI

• $\neg X := \{z \mid \neg(z \in X)\}$

SIMILE AL PARADOSSO DI RUSSELL

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

↓

Non è un insieme per nessun assioma

• 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 $\Omega := \{x \in I \mid f(x)\}$ → Per separazione, Ω è un insieme

ma Ω non è un insieme → Si è giunti ad un assurdo

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

↯ ASSURDO

Quindi l'insieme I non esiste → L'INSIEME UNIVERSALE DI REALTÀ È QUO UN INSIEME CHE PER CONTENERE UN TUTTO ETÀ DI CUI ABBIAMO BISOGNO PER FARE LA MATEMATICA

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

↓

• Da questo segue che, dato un insieme X

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

DIMOSTRAZIONE:

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

→ ASSIOMA DELL'UNIONE → $\{x, y\}$ È UN INSIEME PERCHÉ x E y LO SONO

Di conseguenza anche $\bigcup\{x, y\}$ è un insieme

Ma $\bigcup\{x, y\}$ sono tutti gli insiemi che stanno in x o in y CIOÈ ANCHE x E y

↳ Quindi sono tutti gli insiemi → $\bigcup\{x, y\}$ = INSIEME DI TUTTI GLI INSIEMI ↯

Quindi, l'unico modo per tradurre il $\neg$ è che prendo tutti gli elementi da un altro insieme

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

SETTRAZIONE INSIEMISTICA

↳ QUESTO VA BENE PER CLASSICA DI SEPARAZIONE

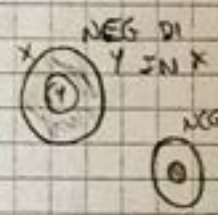
Si legge Y meno X

OPERAZIONI INSIEMISTICHE DALLE TAUTOLOGIE

Visto che c'è una corrispondenza tra linguaggio insiemistico e linguaggio logico proviamo a trasportare delle tautologie

DOPPIA NEGAZIONE

TH: $\forall X, Y (Y \subseteq X \rightarrow X \setminus (X \setminus Y) = Y)$



Dimostrazione:

Per definizione, $X \setminus (X \setminus Y) = \{z \in X \mid z \notin X \setminus Y\} =$

$= \{z \in X \mid z \notin X \setminus Y\} \overset{DEF}{=} \{z \in X \mid \neg(z \in X \wedge z \notin Y)\} =$ USO DE MORGAN

$= \{z \in X \mid z \notin X \vee z \in Y\} \overset{DEF}{=} \{z \mid (z \in X) \wedge (z \notin X \vee z \in Y)\} =$ DISTRIBUTIVA DI $\wedge$ RISPETTO A $\vee$

$= \{z \mid \underbrace{(z \in X \wedge z \notin X)}_{\text{SEMPRE FALSA}} \vee (z \in X \wedge z \in Y)\} =$ AFFINCHÈ LA FORMULA SIA VERA È NECESSARIO CHE $(z \in X \wedge z \in Y)$ SIA VERA

↳ SE È FALSA, ALLORA TUTTO È FALSO

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

↳ QUESTO È L'INSIEME DI TUTTI GLI INSIEMI CHE APPARTENGONO A X E APPARTENGONO A Y

$z \in X$ È SUPERFLUO

↳ 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. $\forall x, y\ (y \subseteq x \rightarrow \underbrace{y \cup (x \setminus y)}_{\text{UN INSIEME CHE APPARTENGANO A ALMENO UN DI QUESTI}} = x)$

Dimostrazione

TUTTI GLI Z TALI CHE

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

DISTRIBUTIVITÀ DI $\vee$ RISPETTO A $\wedge$ → COME FOSSE UNA MOLTIPLICAZIONE

TAUTOLOGIA DEL TERZO ESCLUSO $(p = z \in y)$

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

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

PER ESTENSIONALITÀ

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

DATO CHE $y \subseteq x$ SE $z \in y$, z DOVE PER FORZA APPARTIENE ANCHE AD x → $z \in y$ SUPERFLUO

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

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

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

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

SONO PROPRIO LA DEFINIZIONE DI INCLUSIONE

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

NON CONTRADDIZIONE $\neg(p \vee \neg q)$ DIMOSTRAZION NEGLI ESERCIZI DEL 13\10\2021

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

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

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

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

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

IDEMPOTENZA DI Δ

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

ASSOCIATIVITÀ DI $\cap$ $(p \wedge q) \wedge r \leftrightarrow p \wedge (q \wedge r)$

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

ASSOCIATIVITÀ DI $\cup$ $(p \vee q) \vee r \leftrightarrow p \vee (q \vee r)$

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

ASSOCIATIVITÀ DI Δ $(p \text{ XOR } q) \text{ XOR } r \leftrightarrow p \text{ XOR } (q \text{ XOR } r)$

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

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

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

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

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

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

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

ESPLICITAZIONE DI Δ

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

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

LEGGI DI DE MORGAN

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

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

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

L'assioma dell'unione è:

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

$\forall y \forall x$ non può essere riscritto come $\forall x \forall y$ perché non esiste una commutatività del $\forall$ → SE INVECE DI PRENDERE X CHE STA DENTRO Y CHE STA DENTRO f PRENDO Y CHE STA DENTRO X E Y CHE STA DENTRO f STO PRENDENDO QUALCOSA DI SIMILE ALL'INTERSEZIONE

↓

È possibile scrivere l'assioma dell'unione con $\exists$ in modo che sia un po' più agile e chiaro da capire → SCRITTURA LOGICAMENTE EQUIVALENTE

$$f = \{\underbrace{\{1,2,3\}}_{y}, \underbrace{\{4\}}_{y}\}$$

↓

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

↳ POSSO SCRIVERE PER ESTENSIONALITÀ → $\bigcup f := \{x \in a \mid \exists y (x \in y \wedge y \in f)\}$

↳ HO UNA FORMULA CHIUSA PER L'UNIONE UNARIA

INTERSEZIONE UNARIA

Sia f un insieme,

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

→ È SEMPRE PIÙ GRANDE DELL'$\bigcap f$ TUTTI GLI X CHE APPARTENGONO ALL'UNIONE UNARIA TALI CHE SE Y APPARTIENE AD f ALLORA X APPARTIENE A Y

↓

LA DEFINIZIONE DI INTERSEZIONE UNARIA È COMPLICE A QUELLA DELL'UNIONE UNARIA

ESEMPIO:

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

NESSUN X SODDISFA TUTTE LE CONDIZIONI

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

↳ AD ESEMPIO, PRENDIAMO 1 → È VERO CHE PER OGNI Y (CIOÈ $\{1,2,3\}$) SE $y \in f$ ALLORA $1 \in y$? SÌ → QUESTO RAGIONAMENTO DEVE ESSERE VERO PER OGNI Y, ANCHE $\{4\}$ E $\{3\}$ → PER $\{4\} \in \{3\}$, $1 \notin y$, QUINDI 1 NON FA PARTE DI $\bigcap f$ → STESSO RAGIONAMENTO PER TUTTI GLI X

- $f = \{\{1,2\},\{1\}\}$

  $\cap f = \{1\}$

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

  $\cup \emptyset = \emptyset$

  Quindi $\cap \emptyset = \emptyset$

- $\cap \{x, y\} = x \cap y$ → l'intersezione unaria della coppia 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
↳ È un modo informare per verificare le proprietà degli insiemi

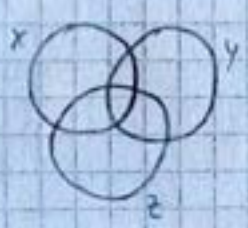
Per disegnare gli insiemi (consideriamo n insiemi) dovremo disegnare n cerchi in modo da rappresentare tutte le intersezioni possibili
↳ I DIAGRAMMI DI EULERO-VENN COMPRENDONO ANCHE GLI INSIEMI CHE NON FANNO PARTE DELLE INTERSEZIONI ↳ DIAGRAMMI ESTERNI

AD ESEMPIO:

- Un insieme

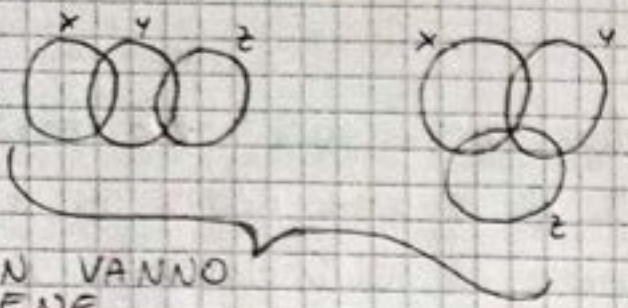
- Due insiemi

- Tre insiemi



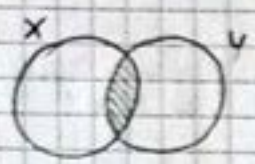
Non è detto che ci sia qualcosa nell'intersezione, ma devo comunque contemplarla

↳



NON VANNO BENE

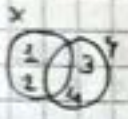
$X \cap Y$



AD ESEMPIO:

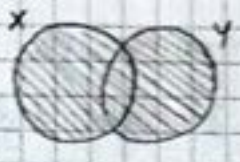
$X = \{1,2\}$

$Y = \{3,4\}$

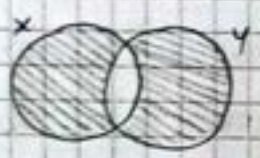


$X \subseteq Y$

$X \cup Y$



$X \Delta Y$

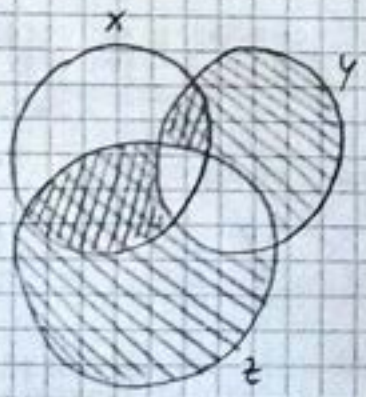


LA DIFFERENZA SIMMETRICA È L'UNIONE MENO L'INTERSEZIONE

$X \setminus Y$

ESEMPIO:

• $X \cap (Y \Delta Z)$



= $Y \Delta Z$

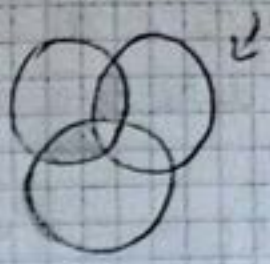
= $X \cap (Y \Delta Z)$

• $(X \cap Y) \Delta (X \cap Z)$

$\backslash\backslash\backslash = X \cap Y$

$/// = X \cap Z$

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



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

↳ PIÙ IMMEDIATO DA VEDERE

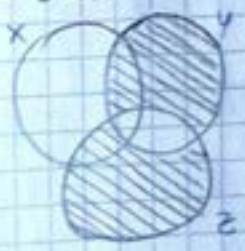
• Proviamo provare a vedere se vale la distributività di unione rispetto a differenza simmetrica

↳ Se è vero avrò questa dimostrazione grafica

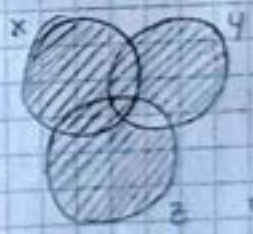
↳ Se non è vero allora posso fornire un controesempio

$X \cup (Y \Delta Z)$

$Y \Delta Z$



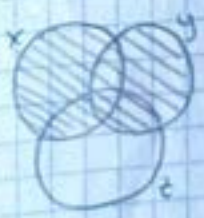
$X \cup (Y \Delta Z)$



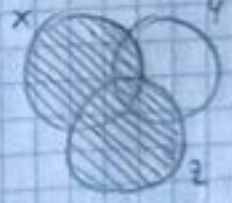
SONO DIVERSI

$(X \cup Y) \Delta (X \cup Z)$

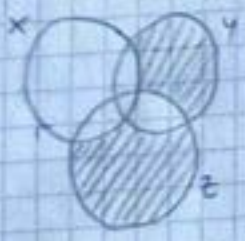
$X \cup Y$



$X \cup Z$



$(X \cup Y) \Delta (X \cup Z)$



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

↳ Posso dare un esempio di tre insiemi che mostrano ciò

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

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

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

Questo metodo sarebbe lunghissimo per trovare insiemi concreti per dimostrare che non vale un'uguaglianza

↳ È un modo informale

CONTINUO DELLA TEORIA DEGLI INSIEMI

DEFINIZIONE DELLA COPPIA ORDINATA

Siano x, y insiemi

$$\boxed{(x,y) \overset{DEF}{=} \{\{x\},\{x,y\}\}}$$ → NON SAPPIAMO CHE VALGA L'ORDINE

↓

Ciò che vogliamo dalla coppia ordinata è che valga l'ordine → Cioè (x,y) è diverso da (y,x)

↳ Per dire ciò scriveremo:

$$\boxed{x \neq y \rightarrow (x,y) \neq (y,x)}$$ → DOBBIAMO SPECIFICARE CHE $x \neq y$ PERCHÉ È NORMALE CHE $(x,x) = (x,x)$

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

↓

Posso dimostrare equivalentemente che:

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

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

Posso spezzare la tautologia della doppia implicazione e dimostrare l'uguaglianza prima in un senso e poi nell'altro

LA PRIMA CONDIZIONE SI CHIAMA NECESSARIA ← $(\rightarrow)$

↓

IMPLICAZIONE NECESSARIA

IPOTESI

Sia $x = y$ →

$$(x,y) \overset{DEF}{=} \{\{x\},\{x,x\}\} \overset{CONG}{=} \{\{x\},\{x\}\}$$

$$(y,x) = \{\{x\},\{x\}\}$$ → SONO UGUALI

($\Leftarrow$) Per ipotesi:

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

SONO UGUALI (CIOÈ HANNO GLI STESSI ELEMENTI)

Devono essere gli stessi elementi, quindi ho due ipotesi:

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

CHE POI È UGUALE A $\{x,y\}$ PERCHÉ È UNA COPPIA NON ORDINATA

Dato che questi due insiemi sono uguali devono 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

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

↳ LA QUARTERNA ORDINATA SARÀ $\rightarrow (x,y,z,T):=((x,y,z),T)$ E COSÌ VIA

PRODOTTO CARTESIANO

Il prodotto cartesiano è l'insieme di tutte le coppie 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

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

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

↳ TUTTI GLI z SI TROVANO NELLE PARTI DELLE PARTI → $a \cup b$

z è composto degli elementi di a e b

AD ESEMPIO: Se ho:

$a = \{0,1\}$

$b = \{1,2\}$

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

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

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

- Se a ha m elementi e b ha n elementi, $a \times b$ avrà $m \cdot n$ elementi

- $\underbrace{a \times b \times c}_{\text{FORMA LE TERNE ORDINATE}} = (a \times b) \times c$

(LEZIONE 09)

Correzione esercizi 15/10/2021

3) $\bigcap\{x\} = \{ z \in \bigcup\{x\} \mid \forall y (y \in \{x\} \to z \in y) \} =$

QUESTO È X — AFFINCHÉ SI HAGA QUESTO ALLORA Y DEVE ESSERE PROPRIO X

QUANTE Y CI SONO CHE SONO PROPRIO X → SOLO X

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

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

$\bigcup\{x\} = \{ z \mid \exists y (z \in y \wedge y \in \{x\}) \} =$ → Y DEVE ESSERE PROPRIO X PERCHÉ C'È SOLO X NEL $\{x\}$

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

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

Sia $x = x_1 \wedge y = y_1 \wedge z = z_1$

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

$\overset{DEF}{=} \{\{\{\{x\},\{x,y\}\}\}, \{\{\{x\},\{x,y\}\}, z\}\}$

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

$\overset{DEF}{=} \{\{\{\{x_1\},\{x_1,y_1\}\}\}, \{\{\{x_1\},\{x_1,y_1\}\}, z_1\}\}$

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

$(x_1, y_1, z_1) = \{\{\{\{x\},\{x,y\}\}\}, \{\{\{x\},\{x,y\}\}, z\}\}$ che per 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 $\{\{x\},\{x,y\}\} = \{\{x_1\},\{x_1,y_1\}\}$ cioè quando $x = x_1 \wedge y = y_1$

DALLA DIMOSTRAZIONE DELLA PROPRIETÀ CARATTERISTICA DELLE COPPIE ORDINATE

Corrispondenza tra insiemi

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

↳ $g \subseteq a \times b$

La coppia $(a \times b, g)$ si dice <u>corrispondenza</u> tra a e b con grafico g → VOGLIAMO COLLEGARE GLI ELEMENTI DI a E GLI ELEMENTI DI b IN QUALCHE MODO

CHIAMIAMO LA CORRISPONDENZA "PO"

$\underset{\to PO}{P} = (a \times b, g)$ e siano $c \in a$ e $d \in b$

Per definizione:

$\boxed{c\,p\,d :\Longleftrightarrow (c, d) \in g}$ → LA COPPIA c, d APPARTIENE AL GRAFICO DI p

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

↳ UN ESEMPIO DI CORRISPONDENZA È "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 $g \subseteq a \times b$)

↳ EE NE SONO ALCUNI SPECIALI

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

↳ g RICORDA IL GRAFICO DEL $\leq$, QUINDI È COME SE MI STESSI CHIEDENDO: $1 \leq 1$? SÌ

- $a = \{0, 3\}$ $\quad b = \{1\}$

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

$0\,P_1\,1$? Sì

$3\,P_1\,1$? No

→ STO CONSIDERANDO ANCORA LA RELAZIONE $\leq$

Quindi, ad esempio:

$\leq = (\mathbb{N} \times \mathbb{N}, g)$ → ORA g È INFINITO

→ IL PRIMO È SEMPRE MINORE O UGUALE DEL SECONDO

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

3 è in relazione "minore uguale" con 2?

↳ $3 \leq 2$? No

VISUALIZZIAMO LA RELAZIONE

Posso descrivere una relazione in vari modi, elencando il grafico

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

↳ IN QUESTO CASO g È TUTTO IL PRODOTTO CARTESIANO

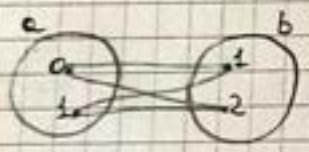
TABELLA

ELEMENTI DI b

P	1	2
0	x	x
1	x	x

ELEMENTI DI a

CON LE LINEE

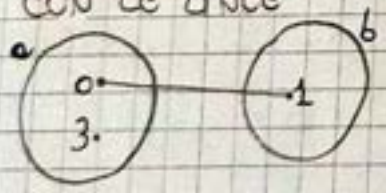


- $a = \{0,3\}$ $b = \{1\}$ $p_1 = (a \times b, g_1)$ $g_1 = \{(0,1)\}$

TABELLA

P_1	1
0	x
3	0

CON LE LINEE



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

↓

PUÒ ESSERE UTILE QUANDO g È INFINITO O HA TANTI ELEMENTI

- $p = (\mathbb{N} \times \mathbb{N}, g)$ mpm

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

- $(0,5) \in g$? No

- $2 p 2$? Sì

RELAZIONE BINARIA → UNA CORRISPONDENZA INTERNA AD UN INSIEME

Una corrispondenza tra a e a (Sia a un insieme) si dice relazione binaria
↳ $(a \times a, g)$

COSA NON È UNA CORRISPONDENZA?

Ad esempio:

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

non è una corrispondenza perché $g_1 \nsubseteq a \times b$

L'INSIEME DELLE CORRISPONDENZE

- $CORR(a,b)$ è l'insieme delle corrispondenze tra a e b
- $REL(a) = CORR(a,a)$ è l'insieme delle relazioni binarie

LE FUNZIONI → LE FUNZIONI SONO PARTICOLARI CORRISPONDENZE

Siano a e b insiemi e sia $f = (a \times b, g)$ con $g \subseteq a \times b$.
↳ f È UNA CORRISPONDENZA DI a PER b

f si dice funzione o applicazione tra a e b se: $\boxed{(\forall x \in a)(\exists! y \in b)(x f y)}$

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

↳ SE IN a C'È UN SOLO ELEMENTO NON ASSOCIATO ALLORA f NON È UNA FUNZIONE → UN ELEMENTO DI b PUÒ ESSERE ASSOCIATO A PIÙ DI UN ELEMENTO DI a MA UN ELEMENTO DI a NON PUÒ ESSERE ASSOCIATO A PIÙ ELEMENTI DI b

$f : a \to b$
↳ f È UNA FUNZIONE CHE VA DA a A b

ATTENZIONE:
g non è la funzione, è il grafico della funzione

a si dice dominio di f

b si dice codominio di f

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

↳ DEVO PRIMA DIRE CHE E' UN SOTTOINSIEME DI a×b

IMMAGINE DI f

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

↳ E' UN SOTTOINSIEME DEL CODOMINIO

↓ ESISTE UN CERTO X TALE CHE LA COPPIA x,y STA NEL GRAFICO

↑ NOTAZIONE ALTERNATIVA

↳ PER SCRIVERE PIU' VELOCEMENTE

↳ SOTTINTENDO CHE $f(x) \in b$

DESCRIZIONE ESPLICITA DI UNA FUNZIONE f

$$f : x \in a \overset{\text{MAPS TO, ASSOCIA}}{\longmapsto} f(x) \in b$$

↓ DESCRIZIONE ESPLICITA DI UNA FUNZIONE

↳ SI POSSONO SCRIVERE COSE MOLTO COMPLESSE IN MODO SEMPLICE → A VOLTE PUO' ESSERE DIFFICILE DA SCRIVERE MA COSI' LO CAPISCO SUBITO

↓ AD ESEMPIO:

$f : x \in \mathbb{N} \longmapsto x+1 \in \mathbb{N}$ ↳ g SARA' $\{(0,1),(1,2),(2,3),(3,4)\dots\}$

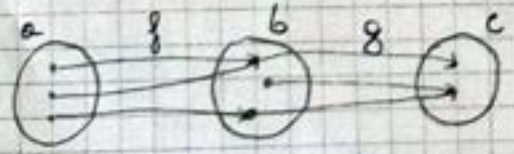
"Una corrispondenza tra due insiemi a e b si dice funzione ben posta se è una funzione"

↳ DEFINIZIONE INFORMALE, COLLOQUIALE

↳ Talvolta delle cose sembrano funzioni ma non lo sono

PRODOTTO RELAZIONALE (O TRA CORRISPONDENZE)

Se ho:



↳ CIOE' LA COMPOSIZIONE DA UN PUNTO DI VISTA DELLE RELAZIONI

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

Definisco $\rho\sigma = (a \times d, g_3)$ con g_3 definita con questa proprietà:

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

↳ C'È UN ELEMENTO IN MEZZO CHE COLLEGA LE DUE RELAZIONI

Z SI TROVA SIA IN b CHE IN c PERCHÈ DEVE APPARTENERE ALLA COPPIA $(x,z) \in g_1$ e $(z,y) \in g_2$

Il prodotto relazionale è associativo

ESEMPI:

- U = Insieme degli esseri umani

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

$x \rho y \leftrightarrow x$ è padre di y

↳ CIOÈ "LA COPPIA x, y STA NEL GRAFICO"

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

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

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

↳ $x \rho^2 y \leftrightarrow x$ è nonno di y

$\rho\sigma = \rho$ $\quad x \rho\sigma y \leftrightarrow \exists z (\underbrace{x \rho z \wedge z \sigma y}_{x \text{ È IL PADRE DEL FRATELLO DI } y})$

$\sigma\rho = x$ è lo zio di y

- $\subseteq$ su $\mathcal{P}(\mathbb{N})$ → $\subseteq$ È UNA RELAZIONE BINARIA QUINDI HO BISOGNO DELLE $\mathcal{P}(\mathbb{N})$

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

↳ L'INCLUSIONE QUADRA È UGUALE ALL'INCLUSIONE

• $p: m \in \mathbb{N} \to m+1 \in \mathbb{N}$ → QUESTA È PROPRIO UNA FUNZIONE

$\sigma = \leq$ su $\mathbb{N}$

$$m \, p\sigma \, n \leftrightarrow \exists z \big(\underbrace{m \, p \, z}_{\text{z È IL SUCCESSIVO DI m}} \wedge \underbrace{z \, \sigma \, n}_{\text{z È MINORE O UGUALE DI n}} \big) \leftrightarrow \underbrace{\exists z (m+1 = z \wedge z \leq n)}_{\text{È COME DIRE } m \leq n}$$

AD ESEMPIO:

3 pσ 4? Sì

2 pσ 4? Sì

4 pσ 4? No

Correzione esercizi 20/10/2021 (LEZIONE 10)

LE COPPIE DI DI CON DUE ELEMENTI IN OGNI ELEMENTO

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

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

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

STESSO INSIEME → $\{2,3\}\ P\ 8$? Sì

$\{3,2\}\ P\ 9$? Sì

Non è una funzione perché a uno stesso elemento ma associa due diversi

FUNZIONE COMPOSTA

LA FUNZIONE COMPOSTA → DA DUE FUNZIONI È ANCORA UNA FUNZIONE

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

Definisco $g \circ f = fg$ (COMPOSTA DI g E f) — PRODOTTO RELAZIONALE

VISTO CHE f È UNA FUNZIONE (DEL DOMINIO) E VISTO CHE g È UNA FUNZIONE (DEL CODOMINIO)

DESCRIZIONE ESPLICITA

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

FUNZIONE IMMERSIONE DI a IN b

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

↳ L'ELEMENTO x DI a → VAI A VEDERE DENTRO b MA È SEMPRE QUELL'ELEMENTO x

FUNZIONE IDENTITÀ DI a

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

↳ AD x ASSOCIO LO STESSO x ED È SCRITTO APPARTENENTE AD a

FUNZIONE RESTRIZIONE DI f AD S

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

RESTRINGO IL DOMINIO → VIENE TRASPORTATA L'INIETTIVITÀ

ESEMPIO:

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

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

FUNZIONE PROLUNGAMENTO DI f

ALLARGA IL DOMINIO

$g: b \to c$ si dice prolungamento di f se:

↳ È IL CONTRARIO DELLA RESTRIZIONE

↓

ALLARGHIAMO IL DOMINIO

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

FUNZIONE SURIETTIVA

Se $Im f = b$, f si dice suriettiva → QUANDO OGNI ELEMENTO DEL CODOMINIO È IMMAGINE DI ALMENO UN ELEMENTO DEL DOMINIO

↳ Dalla definizione di immagine, si deduce che:

f è suriettiva $\Longleftrightarrow (\forall y \in b)(\exists x \in a(f(x) = y))$

↳ letto per y quando è suriettiva → NELLA DEFINIZIONE DI $Im f$ PRENDIAMO IN MODO GENERICO "LE Y", ORA LE Y DEVONO ESSERE TUTTE

FUNZIONE NON SURIETTIVA

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

↳ NEGARE LA SURIETTIVITÀ

FUNZIONE RIDOTTA DI f AD S

Se $S \subseteq b$, $Im f \subseteq S$

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

↓

RESTRINGO IL CODOMINIO A QUALCOSA DI PIÙ VICINO ALL'IMMAGINE

↓

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

ESEMPIO:

$f: x \in \mathbb{N} \mapsto x+1 \in \mathbb{Q}$

$g: x \in \mathbb{N} \mapsto x+1 \in \mathbb{Z}$

FUNZIONE COSTANTE

Sia $\bar{y} \in b$

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

UNA FUNZIONE COMPOSTA DA DUE FUNZIONI SURIETTIVE, È SURIETTIVA

Siano f e g suriettive, allora $g \circ f$ è suriettiva

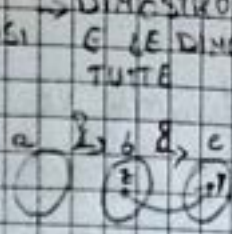
DIM

↳ BASTA CHE IO DIMOSTRO PER UNA Y PERCHÉ HO $\forall Y$ ↳ DEVE VALERE PER QUALSIASI → DIMOSTRO UNA E LE DIMOSTRO TUTTE

Sia $y \in c$

Poiché g è suriettiva, $\exists z \in b : g(z) = y$

Poiché f è suriettiva, $\exists w \in a : f(w) = z$ ↳ DATO CHE $z \in b$



Segue che $g \circ f(w) = \underbrace{g(f(w))}_{g(z)} = y$ ↳ HO TROVATO UN ELEMENTO IN a CHE HA, MEDIANTE $g(f(w))$, IMMAGINE Y

FUNZIONE INIETTIVA

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

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

DEFINIZIONE EQUIVALENTE

Per la tautologia della contrapposizione,

f è iniettiva $\leftrightarrow (\forall x, y \in a)(x \neq y \rightarrow f(x) \neq f(y))$ → PASSO METTERE EQUIVALENTEMENTE IL $\leftrightarrow$ PERCHÉ IL VERSO CONTRARIO DELLA FRECCIA È LA DEFINIZIONE DI FUNZIONE

↳ QUANDO ELEMENTI DISTINTI DEL DOMINIO HANNO IMMAGINI DISTINTE

FUNZIONE NON INIETTIVA

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

↳ NEGARE L'INIETTIVITÀ

ESEMPIO: QUANDO f È INIETTIVA O SURIETTIVA?

- $f: a \rightarrow b$ $\quad a = \{x\}$ ↳ DOMINIO DI UN SOLO DOMINIO $\quad f = (a \times b, G)$ $\quad G = \{(x, y)\}$ ↳ NON POSSO ESCLUDERE NIENT'ALTRO

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

Avendo un solo elemento, la funzione è per forza iniettiva. La funzione può essere suriettiva se anche b ha un solo elemento

- $f: x \in a \mapsto \{x\} \in \mathcal{P}(a)$ $\quad a = \{0, 1\}$ → NEL DOMINIO CI SONO 4 ELEMENTI → $\mathcal{P}(a) = \{\{0\}, \{1\}, \{0, 1\}, \emptyset\}$

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

La funzione è iniettiva ma non suriettiva perché ci sono degli elementi di $\mathcal{P}(a)$ che non sono associati → AD ESEMPIO: $\emptyset$

• $f: X \in \mathcal{P}(\mathbb{N}) \longmapsto X \cap (\mathbb{N} \setminus \{0\}) \in \mathcal{P}(\mathbb{N})$

P.A. → PER ASSURDO

Suppongo che $\exists X : f(X) = \{0\} \overset{\text{SIGNIFICA CHE}}{\longleftrightarrow} X \cap (\mathbb{N} \setminus \{0\}) = \{0\}$ FALSO

↳ L'INSIEME DI TUTTI GLI ELEMENTI CHE APPARTENGONO SIA A X CHE A $\mathbb{N} \setminus \{0\}$

↓

È FALSO PERCHÉ $\{0\}$ NON FA PARTE DI QUESTO INSIEME

Quindi la funzione non è suriettiva

↳ C'È UN ELEMENTO DEL CODOMINIO CHE NON È ASSOCIATO A NESSUN

È iniettiva?

→ IMMAGINI UGUALI → $f(x) = f(y)$

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

Supponiamo che $\bar{X} = \{0, 1\}$ $\bar{Y} = \{1\}$ → SUPPONIAMO CHE X E Y DIFFERISCANO SOLO PER LO ZERO

$f(\bar{X}) = \{1\} = f(\bar{Y})$

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

• $f: X \in \mathcal{P}(\mathbb{N}) \longmapsto \mathbb{N} \setminus X \in \mathcal{P}(\mathbb{N})$ → A UNA PARTE X DI $\mathbb{N}$ ASSOCIA IL COMPLEMENTO DI X IN $\mathbb{N}$

È iniettiva?

ELEMENTI GENERICI

Suppongo che $\mathbb{N} \setminus X = \mathbb{N} \setminus Y \Leftrightarrow \mathbb{N} \setminus (\mathbb{N} \setminus X) = \mathbb{N} \setminus (\mathbb{N} \setminus Y) \Leftrightarrow X = Y$

↳ PRESO LO STESSO INSIEME

La funzione è iniettiva

È suriettiva?

Prendo $Y \in \mathcal{P}(\mathbb{N})$

Sia $X = \mathbb{N} \setminus Y$ $f(X) \overset{\text{def}}{=} \mathbb{N} \setminus X = \mathbb{N} \setminus (\mathbb{N} \setminus Y) = Y$

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 INIETTIVE È 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

Siano $w, z \in a$: $\underbrace{g \circ f(w)}_{g(f(w))} = \underbrace{g \circ f(z)}_{g(f(z))}$ allora

Visto che:

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

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

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

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

DIM

Siano $z, w \in a$: $f(z) = f(w)$ allora; per la definizione di funzione di g, $g(f(z)) = g(f(w))$, $\overset{DEF}{\Rightarrow} g \circ f(z) = g \circ f(w)$; ma

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

↳ PER LA DEFINIZIONE DI FUNZIONE DI f

↳ Quindi f è iniettiva

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

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

DIM

$g(f(x)) \rightarrow f(x) \in b$, cioè il codominio di g

Sia $y \in c$ (→ codominio di g), poiché $g \circ f$ è suriettiva $\overset{def.}{\Rightarrow} \exists x \in a : g \circ f(x) = y$

allora g è suriettiva → ABBIAMO TROVATO $\forall y \in c$ UN ELEMENTO DEL DOMINIO DI g TALE CHE g FA QUELL'ELEMENTO DIA y → QUESTO ELEMENTO È $f(x)$

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:

$a = \{1\}$, $b = \{1, 2\}$ → È UN CONTROESEMPIO

$f: 1 \in a \mapsto 1 \in b$ (IMMERSIONE)

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

$g \circ f: x \in a \mapsto x \in a$ $\quad g \circ f = Id_a$

le identità sono sempre biettive → $g \circ f$ è biettiva

Ma g non è iniettiva e f non è suriettiva

Correzione esercizi 20/10/2021 (LEZIONE 11)

→ DEL 19/10/2021

9) II. $p: m \in \mathbb{N} \mapsto \{m\} \in \mathcal{P}(\mathbb{N})$ è una funzione

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

↳ cioè $\{m\} = \{n\}$ →

Quindi la funzione è iniettiva

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

VIII. $\{a, b\}\, p\, n \leftrightarrow a^b = n$

In g si ha che $(\{2,3\}, 8) \in g$ ma anche $(\{3,2\}, 9) \in g$

quindi questa non è una funzione

II. $(m,n) \in g \leftrightarrow m+n \in \mathbb{N}$ $\quad m\,p\,n \leftrightarrow m+n \in \mathbb{N}$

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

$(0,2) \in g$? Sì 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 e che due stessi elementi non siano associati associati a due diversi elementi

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

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

VII. $p: (l,m) \in \mathbb{N} \times \mathbb{N} \longmapsto l^m \in \mathbb{N}$ $\quad (l,m)\,p\,n \leftrightarrow l^m = n$

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

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

↳ Questa è una funzione perché ad ogni coppia viene associato uno ed un solo n

↳ DIPENDE DA COME DEFINIAMO 0^0 → POSSIAMO DEFINIRLO UGUALE A 1 PERCHÉ PER LA FUNZIONE $x \in \mathbb{R} \mapsto x^0 \in \mathbb{R}$ QUESTA È UNA FUNZIONE COSTANTE UGUALE A 1 TRANNE CHE A 0

$0^0 = 1$ PER CONTINUITÀ

$(0,0,n) \in g \leftrightarrow 0^0 = n$

La funzione è suriettiva?

Sia $n \in \mathbb{N}$

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

Sì, è suriettiva perché ogni coppia ha un'immagine

La funzione è iniettiva?

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

Non è iniettiva perché $p((0,1)) = p((0,2))$

5)

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

È una funzione

È iniettiva?

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

$f(-1) = 0 = f(0)$ → SE CONSIDERIAMO MINI

$f(-3) = -1 = f(2)$ → STESSA IMMAGINE

Quindi la funzione non è iniettiva

È suriettiva? → SE FOSSE STATO $m \in \mathbb{N}$ ALLORA SAREBBE STATO ANCHE SURIETTIVA

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

$f(-2m) = m$

Quindi la funzione è suriettiva

APPLICAZIONE (ANTI)IMMAGINE

Tutte le immagini degli elementi di questo X

Sia $f: a \to b$ $\quad \{y \in b \mid (\exists z \in x)(f(z) = y)\} \in \mathcal{P}(b)$

Definisco $\vec{f}: X \in \mathcal{P}(a) \mapsto \{f(z) \mid z \in X\} \in \mathcal{P}(b)$ → APPLICAZIONE IMMAGINE

$\overleftarrow{f}: Y \in \mathcal{P}(b) \mapsto \{x \in a \mid f(x) \in Y\} \in \mathcal{P}(a)$ → APPLICAZIONE ANTIIMMAGINE

Cioè, presa una parte del codominio, prendo tutti gli elementi del dominio che associano a quegli elementi del codominio

ESEMPI:

- $\vec{f}(\emptyset) = \emptyset$ → TUTTE LE IMMAGINI DEGLI ELEMENTI CHE STANNO NEL VUOTO

  $\overleftarrow{f}(\emptyset) = \emptyset$ ↳ TUTTI GLI x DEL DOMINIO TALI CHE $f(x) \in \emptyset$

- $\vec{f}(a) = \mathrm{Im} f$ → L'IMMAGINE DI a STESSO → SONO TUTTI GLI $f(z)$ CON $z \in a$

- $\vec{f}(\{x\}) = \{f(x)\}$ → SONO TUTTI GLI $f(z)$ TALI CHE $z \in \{x\}$, CIOÈ z È PROPRIO x → QUINDI PRENDO L'INSIEME DEGLI $f(z)$, CIOÈ, VISTO CHE CHE SOLO $f(x)$, SARÀ L'INSIEME CON SOLO $f(x)$ CIOÈ $\{f(x)\}$

- $\overleftarrow{f}(b) = a$ → TUTTI GLI ELEMENTI CHE SE CI FACCIO L'IMMAGINE STO IN b

  ↳ $\overleftarrow{f}(\mathrm{Im} f) = a$

- Se $y \in b \setminus \mathrm{Im} f$, allora $\overleftarrow{f}(\{y\}) = \emptyset$

- $f: n \in \mathbb{N} \mapsto \{n\} \in \mathcal{P}(\mathbb{N})$

  $\vec{f}(\{0,1\})$ = Tutte le immagini composte degli elementi di $\{0,1\}$ $= \{\overset{f(0)}{\{0\}}, \overset{f(1)}{\{1\}}\}$

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

  ↓ NON ESISTE UN ELEMENTO DI $\mathbb{N}$ CHE HA COME IMMAGINE $\{3,5\}$

  ↳ $f(3) = \{3\} \neq \{3,5\}$

CARATTERIZZAZIONI DI INIETTIVITÀ, SURIETTIVITÀ, BIETTIVITÀ A PARTIRE DA $\overleftarrow{f}$

- f è iniettiva se e solo se: $\forall y \in \mathcal{P}(b)$, $\overleftarrow{f}(y)$ o è $\emptyset$ o ha un solo elemento.

  ↳ $f \in In(a,b) \longleftrightarrow (\forall y \in \mathcal{P}(b))(\overleftarrow{f}(y) = \emptyset \vee ((\exists! x \in a)(\overleftarrow{f}(y) \ni x)))$

  È UN SOTTOINSIEME DI a — ESISTE UN UNICO ELEMENTO DI a CHE NE APPARTIENE

  → FUNZIONE INIETTIVA DI a IN b → TUTTE LE FUNZIONI INIETTIVE SONO LE FUNZIONI DELLE $\mathcal{P}(\mathcal{P}(a \times b))$

  DIM → VOGLIAMO DIMOSTRARE QUESTO SE E SOLO SE

  (→) Supponiamo che f sia iniettiva. Sia $y \in \mathcal{P}(b)$ e suppongo che $\overleftarrow{f}(y) \neq \emptyset$ → C'È L'ORA QUINDI SE DIMOSTRO CHE C'È UN SOLO ELEMENTO VA BENE LO STESSO

  È UN ALTRO ELEMENTO — Dalla definizione, $\exists x \in a : f(x) \in y$

  → DEVO DIMOSTRARE CHE SE LO PRENDO NEL NUOVO INSIEME HA UN SOLO ELEMENTO

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

  Dall'iniettività segue che z deve essere proprio uguale a x.

  Quindi, $z = x$, di conseguenza $\overleftarrow{f}(y) = \{x\}$

  (←) Prendo $x, y \in a$ e suppongo che $f(x) = f(y)$ → VOGLIO FAR VEDERE CHE $x = y$

  Prendo $\overleftarrow{f}(\{f(x)\})$ → QUINDI $\overleftarrow{f}(y)$ HA UN SOLO ELEMENTO → HO PRESO IL SOTTOINSIEME DI b CHE HA 0 ELEMENTI TALI CHE LA LORO IMMAGINE VALGA NEL SINGOLETTO DI $f(x)$, CHE PER COMPRENSIONE DI SINGOLETTO $f(x)$ VERRÀ $f(x) = f(x)$

  ↓

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

  ↳ Quindi la funzione è iniettiva perché abbiamo che se $f(x) = f(y)$ allora $x = y$

- f è suriettiva se e solo se $(\forall y \in \overbrace{\mathcal{P}(b) \setminus \{\emptyset\}}^{\text{PARTI NON VUOTE}})(\overleftarrow{f}(y) \neq \emptyset)$

  ↳ SE f È SURIETTIVA ALLORA È CHIARO CHE $\forall y \in \mathcal{P}(b)$ TUTTI GLI ELEMENTI DI b SONO ASSOCIATI AD ALMENO UN ELEMENTO DI a QUINDI $\overleftarrow{f}(y) \neq \emptyset$

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

- f è biettiva se e solo se $\forall y \in \mathcal{P}(b) \setminus \{\emptyset\}$ allora $\overleftarrow{f}(y)$ contiene esattamente un elemento → DEVE VALERE CHE $\overleftarrow{f}(y) \neq \emptyset$ E CHE ABBIA UN SOLO ELEMENTO

SEZIONE, RETRAZIONE E INVERSA DI f

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

- Se $f \circ g = id_b$, 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:

- $f: n \in \mathbb{N} \mapsto \{n\} \in \mathcal{P}(\mathbb{N})$

È una retrazione?

↳ Voglio che una volta applicata la composizione mi dia l'identità di a

$g: \mathcal{P}(\mathbb{N}) \to \mathbb{N}$

g, PER ESSERE UNA FUNZIONE DEVE ESSERE DEFINITA SU TUTTE LE PARTI DI $\mathbb{N}$

NON SERVE AFFINCHÉ g SIA UNA FUNZIONE → POTENDO PRENDERE MAGARI 1 E 3

$$g: p \in \mathcal{P}(\mathbb{N}) \mapsto \begin{cases} 0 & \text{SE } p \text{ HA 0 o PIÙ DI UN ELEMENTO} \\ n & \text{SE } (\exists n \in \mathbb{N})(p = \{n\}) \end{cases}$$

SE NON È UN SINGLETON.

↳ SCELGO, SE È UN SINGLETON DI UN ELEMENTO, ASSOCIA QUELL'ELEMENTO

È UNA RETRAZIONE? VEDIAMO

- $g \circ f(n) = g(f(n)) = g(\{n\}) = n \to g \circ f = Id_{\mathbb{N}} \to g$ È UNA RETRAZIONE DI f

È UNA SEZIONE?

- $f \circ g(\emptyset) = f(g(\emptyset)) = f(0) = \{0\} \to f \circ g \neq Id_{\mathcal{P}(\mathbb{N})} \to g$ NON È UNA SEZIONE DI f

PRENDO IL CASO IN CUI p NON È UN SINGLETON

DEL VUOTO SIAMO PARTITI AL SINGLETON DI ZERO

NON È DETTO CHE NON CI SIANO ALTRE g CHE SIANO SEZIONI

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 proprio

↓

COME SI VEDE SE ESISTONO SEZIONI (O RETRAZIONI)

↓

Ragioniamo per assurdo

P.A. c'è una sezione g di f.
Cioè $f \circ g = Id_b$ → l'identità di b è biettiva, quindi è ovviamente anche suriettiva

LA PRIMA FUNZIONE DI $f \circ g$ è f

Affinché $f \circ g$ sia suriettiva, è necessario che f sia suriettiva, ma questo è un assurdo ↯
perché f non è suriettiva → $f \circ g$ non può essere biettiva e quindi non si ha id

↓

NO ESEMPIO, f NON MANDA NULLA A $\emptyset$

TEOREMA SULL'INIETTIVITÀ

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

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

↓

DIM

- ($\Leftarrow$) Vogliamo vedere che se $a = \emptyset$ oppure esiste retrazione, f è iniettiva.

- Supponiamo che $a = \emptyset$
  ↳ la condizione di iniettività è banalmente verificata
  ↳ PER LA DEFINIZIONE DI INIETTIVITÀ, $\underbrace{(\forall x, y \in a)}_{\text{SEMPRE FALSO, QUINDI L'IMPLICAZIONE È SEMPRE VERA E LA FRASE È SEMPRE VERIFICATA}}(f(x) = f(y) \to x = y)$

↓

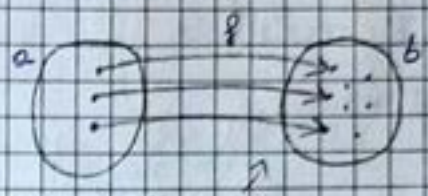
$\underbrace{(\forall x(\forall y(x \in a \wedge y \in a \to (f(x) = f(y) \to x = y))))}_{\text{FBF DI INIETTIVITÀ}}$

• Se $(\exists g : b \to a)(g \circ f = Id_a)$ allora, visto che Id_a è biettiva, anche $g \circ f$ è biettiva. In particolare $g \circ f$ è iniettiva e affinché ciò sia vero, f è iniettiva
↳ LA SECONDA FUNZIONE IN $g \circ f$

• $(\to)$ Sia f iniettiva.

Suppongo $a \neq \emptyset$, cioè che $\exists x \in a$ → SE DEVO FAR VEDERE CHE UNA COSA IMPLICA UNA DISGIUNZIONE POSSO NEGARE UNA DELLE DUE E FAR VEDERE CHE VALE L'ALTRA

Questo x lo chiamo $\bar{x}$



f è iniettiva ma freccia non vuol dire iniettiva

• GLI ELEMENTI DELL'IMMAGINE, CHE QUINDI VENGONO DA ELEMENTI DI a, LI RIMANDO A QUEGLI ELEMENTI DI a DA CUI VENGONO.
• GLI ELEMENTI CHE NON SONO $Im f$, LI RIMANDO ED $\bar{x}$

→ LA FUNZIONE DI RITORNO NON DEVE ESSERE PER FORZA INIETTIVA

Definisco $g : b \to a$

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

In particolare, dato che f è iniettiva, $\overleftarrow{f}(\{y\})$ ha un solo elemento che dipenderà da y → chiamo questo elemento x_y, quindi se $y \in Im f$, $\overleftarrow{f}(\{y\}) = \{x_y\}$

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

→ QUESTA PARTE CI SERVE PER DEFINIRE LA FUNZIONE g

→ Dobbiamo vedere se g è una retrazione, cioè:

QUESTO CASO NON CI SERVE PER VEDERE SE È UNA RETRAZIONE PERCHÉ TUTTI GLI ELEMENTI DI a VANNO PER FORZA NELL'IMMAGINE DI f

↳ $g \circ f(x) = Id_a$

$g \circ f(x) = g(f(x)) = x$ → POSSO SCRIVERE x PERCHÉ $f(x) \in Im f$ SEMPRE, QUINDI x_y È PROPRIO x

↳ $f(x) \in Im f$? CERTO, PER DEFINIZIONE → SIAMO NEL PRIMO CASO → g ASSOCIA x_y, CIOÈ L'ELEMENTO DA CUI PROVIENE $f(x)$

TEOREMA SULLA SURIETTIVITÀ

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

DIM

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

$(\exists g: b \to a)(f \circ g = Id_b)$

Dato che $f \circ g$ è suriettiva, f è suriettiva (UN'ALTRA FUNZIONE DI $f \circ g$)

↳ $f \circ g$ È BIETTIVA PERCHÉ Id_b È BIETTIVA

STESSO RAGIONAMENTO 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

↳ Potrei avere un elemento in b che è associato a più di un elemento di a → Devo sceglierne uno ed escludere gli altri

È possibile costruire g grazie all'ASSIOMA DELLA SCELTA

Abbiamo visto qualche lezione fa che:

f è suriettiva se e solo se $(\forall y \in b)(f^{\leftarrow}(\{y\}) \neq \emptyset)$

→ C'È SEMPRE UN ELEMENTO DI a CHE MANDA IN y

↳ $f^{\leftarrow}(\{y\})$ È UN INSIEME

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

$\varphi_b: f^{\leftarrow}(\{y\}) \in \mathcal{P}(a) \mapsto x \in a\ (x \in f^{\leftarrow}(\{y\}))$

TALE CHE VALGA?

↳ SCELGO CON LA FUNZIONE DELLA SCELTA

QUESTA FUNZIONE QUA NON SI PUÒ DIMOSTRARE A PARTIRE DA ALTRI ASSIOMI, QUINDI SERVE UN ASSIOMA A PARTE

ASSIOMA DELLA SCELTA CI PERMETTE DI ORDINARE GLI INSIEMI IN MODO DA AVERE UN MODO

← NON È UN MODO PER SCEGLIERE x, PERCHÉ POSSO PRENDERE IL PRIMO DELL'INSIEME MA NON VUOLE DIRE CHE È POSSIBILE DETERMINARE QUALE È IL PRIMO

Grazie all'assioma della scelta posso definire g.

Definisco $g: y \in b \mapsto \varphi(\overleftarrow{f}(\{y\})) \in a$ → AD y ASSOCIO UN CERTO ELEMENTO CHE STA NELL'ANTIIMMAGINE DEL SINGLETON DI y

→ Voglio vedere se g è una sezione di f.

$$\left(f \circ g(y) = f(g(y)) = f(\varphi(\overleftarrow{f}(\{y\}))) = y\right)$$

↳ PER DEFINIZIONE, $\varphi(\overleftarrow{f}(\{y\}))$ È UN CERTO x CHE APPARTIENE A $\overleftarrow{f}(\{y\})$, MA $f(x)$ È PROPRIO y, QUINDI:

g NON DEVE ESSERE PER FORZA SURIETTIVA, CI POSSONO ESSERE DEGLI ELEMENTI DI a NON ASSOCIATI

Quindi $f \circ g = Id_b$

TEOREMA (COROLLARIO)

$f: a \to b$ è biettiva se e solo se ha un'inversa

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

1) f è biettiva
2) f ha un'inversa
3) f ha sezioni e retrazioni
4) f ha una e una sola sezione
5) $(\forall y \in b)((\exists! x \in a)(y = f(x)))$

5) E 1) SONO LA STESSA COSA, QUINDI 5) ⟺ 1)

3) → 4)

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

DIM

Partiamo con il dimostrare una delle tre.

r è una retrazione?

↳ $r \circ f = Id_a$, quindi $(r \circ f) \circ s = Id_a \circ s$

Ma $Id_a \circ s = s$ dato che Id_a non fa nulla agli elementi, li lascia così come sono.

Per associatività, $(r \circ f) \circ s = r \circ (f \circ s) = r \circ Id_b$ (DEFINIZIONE DI SEZIONE)

Dato che Id_b non cambia nulla nella relazione,

$r \circ Id_b = r$ → $(r \circ Id_b)(y) = r(Id_b(y)) = r(y)$ → È STESSA COSA FA ANCHE $Id_b \circ s$

Di conseguenza $r = s$

→ SE CI SONO DUE INVERSE, COINCIDONO PERCHÉ ENTRAMBE SONO SIA SEZIONE CHE RETRAZIONE

4) → 5)

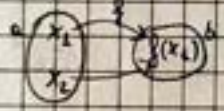
DIM

Suppongo che $(\exists x_1, x_2 \in a)(x_1 \neq x_2 \wedge f(x_1) = f(x_2))$ → SUPPONIAMO CHE LA 5) NON VALGA

f è suriettiva perché già sappiamo che esiste una sezione per ipotesi (da nostra ipotesi è l'affermazione 4)

f NON È BIETTIVA PERCHÉ NON INIETTIVA

Se suppongo che f non è iniettiva, vuol dire che esistono più sezioni



UNA SEZIONE MANDA $f(x_1)$ IN x_1, L'ALTRA MANDA $f(x_1)$ IN x_2

Prendo una sezione g: $g(f(x_1)) = x_1$

DUE SEZIONI DIVERSE

E prendo un'altra sezione $\bar{g}$ tale che: $y \in b \longmapsto \begin{cases} g(y) & \text{se } y \neq f(x_1) \\ x_2 & \text{se } y = f(x_1) \end{cases}$

Ho dimostrato 4) → 5) con non 1) → non 4) → CONTRAPPOSIZIONE

COME TROVARE L'INVERSA DI f? → PUÒ ESSERE UTILE PER VEDERE SE UNA FUNZIONE È BIETTIVA

ESEMPIO:

Prendo $f: m \in \mathbb{Z} \mapsto m-1 \in \mathbb{Z}$

$y = m-1 \rightarrow y+1 = m$ → VOGLIO UNA FUNZIONE CHE AD y ASSEGNI DI NUOVO m

Definisco $g: m \in \mathbb{Z} \longmapsto m+1 \in \mathbb{Z}$ → È L'INVERSA? VEDIAMO

$(f \circ g)(m) = f(g(m)) = f(m+1) = m$ → g È SEZIONE?

$(g \circ f)(m) = g(f(m)) = g(m-1) = m$ → g È RETRAZIONE

g È INVERSA

Correzione esercizi 26/10/2023 (LEZIONE 13)

2.II) $g: n \in \mathbb{N} \longmapsto 3n-2 \in \mathbb{Q}$

$f: m \in \mathbb{Q} \longmapsto 3m+2 \in \mathbb{N}$ Non è una versione perché $f \circ g(n) = 6n$ → Non è un'identità di b

Se prendo $x = \frac{m+2}{3}$

$g(x) = \cancel{3}\left(\frac{m+2}{\cancel{3}}\right) - 2 = m$

$\begin{cases} y = 3n-2 \\ n = \frac{y+2}{3} \end{cases}$

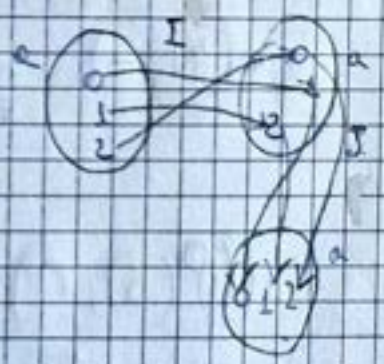
$\rightarrow f: m \in \mathbb{Q} \longmapsto \frac{m+2}{3} \in \mathbb{N}$ → SE PRENDO $m = -3$ PERÒ $f(-3) = -\frac{1}{3}$ → NON APPARTIENE AD $\mathbb{N}$ → QUINDI f NON È UNA FUNZIONE

$f \circ g(n) = f(g(n)) = f(3n-2) = \frac{3n-2+2}{3} = n$

$g \circ f(m) = g(f(m)) = g\left(\frac{m+2}{3}\right) = 3\left(\frac{m+2}{3}\right) - 2 = m$

g non è invertibile

2.IV) $Q = \{0,1,2\}$



$I: Q \to Q$

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

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

$J: Q \to Q$ → PER TROVARE L'INVERSA BASTA INVERTIRE IL GRAFICO

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

$I \circ J(0) = I(J(0)) = I(2) = 0$ ecc.

OPERAZIONI SU INSIEMI
STRUTTURE ALGEBRICHE

- Sia S un insieme non vuoto ($S \neq \emptyset$) e sia $*: S \times S \to S$ (è una funzione che va da $S \times S$ a S)

  $*$ viene detta <u>operazione</u> <u>interna</u> di S (BINARIA)
  ↳ applicabile a due elementi alla volta
  ↓
  il dominio è il prodotto cartesiano

- 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 $\mathbb{N}$
  ↳ $2 - 3 = -1 \notin \mathbb{N}$

  il "$-$" non va da $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$
  ↓
  non è una funzione
- $((\mathcal{P}(S), \cap)$ è una struttura algebrica

PROPRIETÀ COMMUTATIVA

Se $S \neq \emptyset$ e $*$ è un'operazione di S, $*$ si dice commutativa se:

$(\forall x, y \in S)(x * y = y * x)$

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: $(\mathbb{N}, +) \rightarrow$ IL $+$ È ASSOCIATIVO

ELEMENTO NEUTRO A DESTRA

$d \in S$ si dice elemento neutro a destra (di $(S, *)$) se:

$$(\forall x \in S)(x * d = x)$$

↳ d STA A DESTRA

↳ SE È COMMUTATIVA NON BISOGNA SPECIFICARE A DESTRA O A SINISTRA

ELEMENTO NEUTRO A SINISTRA

$l \in S$ si dice elemento neutro a sinistra (di $(S, *)$) se:

$$(\forall x \in S)(l * x = x)$$

ESEMPIO:

- In $(\mathbb{Z}, -)$, 0 è un elemento neutro a destra ma non a sinistra

$(1) - 0 = 1$ ma $0 - (1) = -1 \neq 1$

ELEMENTO NEUTRO O UNITÀ

L'ELEMENTO NEUTRO DI SOLITO VIENE CHIAMATO "UNITÀ"

$u \in S$ si dice elemento neutro se è neutro a destra e a sinistra → ESEMPIO: IN $(\mathbb{N}, *)$, 1 È ELEMENTO NEUTRO

TEOREMA (DELL'UNICITÀ 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 $\underbrace{l * d = l}_{\text{PER DEFINIZIONE}}$, ma $\underbrace{l * d = d}_{\text{PER DEFINIZIONE}}$, quindi $l = d$

↳ 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

MONOIDE

- Un semigruppo con elemento neutro si dice monoide

↳ ESEMPIO:

- $(\mathbb{N}, +)$ è un monoide perché 0 è un elemento neutro

- Un'altra notazione del monoide è: $(S, *, u)$ dove u è l'elemento neutro → CI VIENE DATO ESPLICITAMENTE L'ELEMENTO NEUTRO

↳ ESEMPIO:

- $(\mathbb{N}, +, 0)$
- $(\mathbb{Z}, +, 0)$
- $(\mathbb{N}, \cdot, 0)$
- $(\mathcal{P}(S), \cap, S)$ Perché $(\forall x \in \mathcal{P}(S))(S \cap X = X)$ → CON $X \subseteq S$ PERCHÉ $X \in \mathcal{P}(S)$
- $(\mathcal{P}(S), \cup, \emptyset)$

ESEMPIO:

· Monoide delle parole su un alfabeto.

Prendo $A = \{ \dots \}$ (ALFABETO, INSIEME DI CARATTERI) → AD ESEMPIO: $A = \{a, b, c, d, e, \dots, z\}$ (GLI ELEMENTI DI A SI DICONO LETTERE)

$$S = \{ x \mid (\exists m \in \mathbb{N})((\exists x_1, \dots, x_m \in A)(x = x_1 x_2 \dots x_m)) \}$$

METTO UN CARATTERE VICINO ALL'ALTRO

↳ S è l'insieme delle parole (finite) su A

Esiste la <u>parola vuota</u> (con $m = 0$) che dico $\emptyset$

COME FORMO IL MONOIDE?

$* = ((S \times S) \times S, g)$ → CON FUNZIONE SENSO CHE:

METTERE UNA VICINO ALL'ALTRA

$$(\forall x_1, x_2, x_3 \in S)((x_1, x_2), x_3) \in g \leftrightarrow x_3 = x_1 x_2)$$

$$*: (x_1, x_2) \in S \times S \longmapsto x_1 x_2 \in S$$

↳ ESEMPIO:

· $CA * SA = CASA$

$(S, *, \emptyset)$ è un monoide

$*$ si dice giustapposizione o concatenazione

↳ Operazione non commutativa ma associativa.

Correzione esercizi 27/10/2023 (LEZIONE 19)

- $\alpha: (x,y) \in \mathbb{Z} \times \mathbb{Z} \longmapsto x+y+1 \in \mathbb{Z}$

α È COMMUTATIVA? CIOÈ $x \alpha y = y \alpha x$
Sì, è commutativa perché $x+y+1$ è commutativa

α È ASSOCIATIVA? CIOÈ $(x \alpha y) \alpha z = x \alpha (y \alpha z)$
Sì, è associativa

ELEMENTO NEUTRO DI α? CIOÈ $u \in \mathbb{Z} : (\forall x \; x \alpha u = x)$
L'ELEMENTO NEUTRO È -1 PERCHÉ $x-1+1=x$
↳ $u=-1$ $\quad -1 \alpha x = x \iff x \alpha -1 = x$

- $\beta: (x,y) \in \mathbb{Z} \times \mathbb{Z} \longmapsto -x \cdot y \in \mathbb{Z}$

COMMUTATIVITÀ? Sì
ASSOCIATIVITÀ? Sì
ELEMENTO NEUTRO? $(\forall x \in \mathbb{Z})(-1 \beta x = x)$
↳ L'ELEMENTO NEUTRO È -1

- $\delta: (x,y) \in \mathbb{Z} \times \mathbb{Z} \longmapsto 2 \cdot x \cdot y \in \mathbb{Z}$

COMMUTATIVITÀ? Sì
ASSOCIATIVITÀ? Sì
ELEMENTO NEUTRO? No perché y non appartiene a $\mathbb{Q}$ ma a $\mathbb{Z}$, quindi non posso assegnare $\frac{1}{2}$

- $\zeta: (x,y) \in \mathbb{N} \times \mathbb{N} \longmapsto x \cdot 10^y \in \mathbb{N}$

COMMUTATIVITÀ? No, perché $(1 \zeta 2 = 100 \neq 2 \zeta 1 = 20)$
ASSOCIATIVITÀ? No
ELEMENTO NEUTRO? A sinistra non esiste, a destra è 0

OPERAZIONE OPPOSTA

Sia data $\alpha : (x,y) \in S \times S \mapsto x \alpha y \in S$

l'operazione opposta di α sarà $\bar{\alpha}$:

$$\bar{\alpha} : (x,y) \in S \times S \mapsto y \alpha x \in S$$

DEFINIZIONE DI OPERAZIONE OPPOSTA

Sia (S, α) una struttura algebrica ed una operazione binaria.

L'operazione $\bar{\alpha} : (x,y) \in S \times S \mapsto \alpha(y,x) \in S$ si dice operazione opposta di α

L'operazione opposta è una operazione di operazioni (o anche, operazione di relazioni).

↳ In particolare, l'operazione opposta è duale, infatti fatta due volte ci viene data la stessa cosa di partenza → Infatti, l'operazione opposta è chiamata operazione duale

↓

$$(\bar{\bar{\alpha}}) \quad (x,y) \in S \times S \mapsto y \bar{\alpha} x = x \alpha y \in S$$

Per verificare che le funzioni α e $(\bar{\bar{\alpha}})$ sono la stessa funzione, è necessario verificare che siano la stessa coppia:

$$\alpha = ((S \times S) \times S, g) \qquad (\bar{\bar{\alpha}}) = ((S \times S) \times S, (\bar{\bar{g}}))$$

Due funzioni sono uguali se hanno lo stesso dominio lo stesso codominio e lo stesso grafico.

Quindi $\alpha = (\bar{\bar{\alpha}})$ dato che hanno anche lo stesso grafico? PER LA

• Se α è commutativa, allora $\alpha = \bar{\alpha}$
↳ $y \alpha x = x \bar{\alpha} y = y \bar{\alpha} x = x \alpha y$

• Gli elementi neutri di α, in $\bar{\alpha}$ si scambiano
↳ AD ESEMPIO:
Se d è un elemento neutro a DX di (S, α), 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 CAPIAMO CHE È INUTILE DIMOSTRARE UNA LEGGE ANCHE PER LE OPERAZIONI OPPOSTE DATO CHE POI TUTTO SI RIFLETTE

• L'operazione opposta può essere definita come operazione unaria sull'insieme delle operazioni su S.
↳ È UN SOTTOINSIEME DELLE $\mathcal{P}(\mathcal{P}(\mathcal{P}(S \times S \times S)))$

↓

INSIEME DELLE OPERAZIONI DI $S \times S$ IN S

L'insieme delle operazioni di $S \times S$ in S lo chiamo
$MAP(S \times S, S)$ → È UN INSIEME PERCHÈ LE OPERAZIONI SONO DELLE FUNZIONI CON COPPIE APPARTENENTI ALLE $\mathcal{P}(\mathcal{P}(\mathcal{P}(S \times S)))$
↓ SONO TUTTI GLI $x \in \mathcal{P}(\mathcal{P}(\mathcal{P}(S \times S)))$ TALI CHE SODDISFANO QUELLA COSA
↓ INSIEME DELLE OPERAZIONI BINARIE INTERNE IN S

OPERAZIONE "SEGNATO"

Definisco l'operazione segnato → LE FUNZIONI SONO SEMPRE INSIEMI E IN QUANTO TALI POSSONO ESSERE MANDATI DA ALTRE PARTI

$^- : \alpha \in MAP(S \times S, S) \longmapsto \bar{\alpha} \in MAP(S \times S, S)$ → SONO SEMPRE OPERAZIONI
↳ OPERAZIONE UNARIA

La dualità del segnato si esprime dicendo
che $^{-1} = ^-$ → SEGNATO ALLA MENO 1 È UGUALE A SEGNATO → L'INVERSA DEL SEGNATO È ANCORA SEGNATO

Visto che $^-$ ha un'inversa, allora è biettiva.

PARTI STABILI

Data 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 parte chiusa (o stabile) di $(S,*)$ se l'immagine di $*_{|t \times t}$ appartiene ancora a t

NON È DETTO CHE VADA IN t

Quindi se: $\forall x,y \in t$, $*_{|t \times t}(x,y) \in t$

LA RESTRIZIONE DI $*$ A $t \times t$ → POSSO FARE 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 parte stabile di $(\mathbb{N},+)$? Vediamo

$Im +_{|\{0\} \times \{0\}} \subseteq \{0\}$?

Sì, perché la somma di $0+0$ è sempre $0 \in \{0\}$

$\boxed{\text{Quando abbiamo un monoide, il singleton dell'unità è sempre una parte stabile}}$

L'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 $(\mathbb{N},+)$

La somma dei numeri pari è ancora pari, quindi i numeri pari sono una parte chiusa in $(\mathbb{N},+)$

→ SEMPRE DI $(S,*)$

· Se t è una parte stabile, allora posso scrivere:

$(t,*)$ → È UN ABUSO DI NOTAZIONE PERCHE QUESTO $*$ IN REALTÀ È UNA RESTRIZIONE DI $*$ USATO IN $(S,*)$

· Se t è una parte stabile, $*_{|t\times t}$ è un'operazione di t.

$*_{|t\times t} = ((t\times t)\times t, g)$ dove g è:

$g = \{(x,y,z) \in t^3 \mid *(x,y) = z \in t\}$ → g SONO TUTTE LE TERNE ORDINATE TALI CHE L'IMMAGINE DELLE PRIME DUE È UGUALE ALLA TERZA COORDINATA

t^3 → $t\times t\times t$ → TERNE ORDINATE

· $*_{|t\times t}$ si dice operazione indotta da $*$ su t

ESEMPIO:

· Chi è $+_{|\{0\}\times\{0\}}$?

$+_{|\{0\}\times\{0\}} = (((\{0\}\times\{0\})\times\{0\}, \{(0,0,0)\})$

SCRITTO ESPLICITAMENTE

g SONO TUTTI GLI $(x,y,z) \in \{0\}\times\{0\}\times\{0\}$ TALI CHE $+(0,0)$ SIA UGUALE A 0

· Consideriamo un certo $m \in \mathbb{N}$ e:

$m\cdot\mathbb{N} = \{n \in \mathbb{N} \mid (\exists k \in \mathbb{N})(n = k\cdot m)\}$ → HO PRESO TUTTI GLI n CHE SONO MULTIPLI DI m

SE m È 2, $m\cdot\mathbb{N}$ SONO I NUMERI PARI

$m\cdot\mathbb{N}$ è una parte stabile qualunque sia m?

↳ Devo mostrare che la somma di due elementi che si trovano in $m\cdot\mathbb{N}$ siano ancora in $m\cdot\mathbb{N}$

Siano $x, y \in m \cdot \mathbb{N}$

Per definizione $(\exists k_1, k_2 \in \mathbb{N})(x = k_1 \cdot m \wedge y = k_2 \cdot m)$.

$x + y = k_1 m + k_2 m = (k_1 + k_2) \cdot m$

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 quanti sono i numeri naturali

Anche $\{0\}$ rientra in $m \cdot \mathbb{N}$ perché $\text{Im } 0 \cdot \mathbb{N} = 0 \in \{0\}$

Si può dimostrare che $m \cdot \mathbb{N}$ sono tutte e sole le parti stabili del monoide $(\mathbb{N}, +)$

PERCHÈ 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 È UNA SOTTO(STRUTTURA)

Se S è una struttura algebrica e t è una sua parte chiusa, allora posso scrivere

$t \leqslant S$ → SI LEGGE: t È UNA SOTTO(STRUTTURA) DI S

ESEMPIO:

- $(\mathbb{N}, +)$ è un monoide, quindi $m \cdot \mathbb{N}$ è un sottomonoide
- $(\mathbb{N} \setminus \{0\}, +)$ è un semigruppo, quindi $m \cdot \mathbb{N} \setminus \{0\}$ è un sottosemigruppo

PROPRIETÀ CONSERVATE NELLE PARTI STABILI

- La proprietà commutativa è conservata per le parti stabili → L'OPERAZIONE SU T ALLA FINE È LA STESSA CHE HO IN S
- La proprietà associativa è conservata per le parti stabili
- L'elemento neutro non è una proprietà conservata perché potrebbe non conservarsi
  ↳ ESEMPIO:
  $(\mathbb{N}, +)$ è un semigruppo che ha un elemento neutro, ma in $\mathbb{N} \setminus \{0\}$ è un sottosemigruppo senza elemento neutro → I sottosemigruppi possono perdere degli elementi

INVERTIBILITÀ

Sia $(S, *)$ una struttura algebrica con elemento neutro u.

- Se $x \in S$ e $(\exists y \in S)(x * y = u)$, y si dice inverso destro di x. x si dice invertibile a destra.
- Se $x \in S$ e $(\exists y \in S)(y * x = u)$, y si dice inverso sinistro di x. x si dice invertibile a sinistra.
- Se $x \in S$ e $(\exists y \in S)(x * y = u = y * x)$, 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'UNICITÀ DELL'INVERSA)

T.H: Sia $(S, *)$ una struttura algebrica con elemento neutro u, 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 inverso sinistro di x e d inverso destro di x.

$l * x = u \rightarrow (l * x) * d = u * d = d$

Per l'associatività, (TUTTE LE STRUTTURE ALGEBRICHE CHE FAREMO SONO ASSOCIATIVE)

$l * (x * d) = l * u = l$

Quindi $l = d$

$\boxed{\text{Visto che l'inverso è unico, lo indichiamo con } x^{-1}}$.

↳ 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 monoide $(m, *)$ si dice gruppo se tutti gli elementi di m sono invertibili → ESEMPIO: $(\mathbb{N}, +)$ NON È UN GRUPPO

ELEMENTO SIMMETRICO, INVERSO E OPPOSTO

Un elemento invertibile si dice anche simmetrizzabile.

Solitamente, l'<u>inverso</u> di un elemento (o, anche, il <u>simmetrico</u> di quell'elemento), viene chiamato "<u>opposto</u>" se ci troviamo in un monoide in notazione 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

↓

Solitamente, dire che un numero è l'inverso di un altro si ha quando ci troviamo in una notazione moltiplicativa

COSA CI INDICA IL FATTO CHE ABBIAMO UN INVERSO?

L'avere un inverso ci indica che se faccio il prodotto di qualcosa allora posso anche tornare indietro.

↓

Avrò una struttura con delle simmetrie.

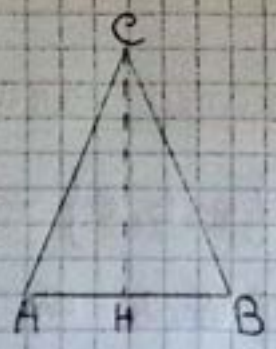
↳ Posso applicare delle funzioni a questa "cosa" (UNA FIGURA, UNO STATO ecc...) per lasciare lo stato così com'è (ad esempio lo stato di una figura)

↓

ESEMPIO:

Prendo un triangolo isoscele ABC, quindi con $AH = HB$

Vogliamo trovare tutti i movimenti del piano che lasciano il triangolo ABC, uguale a se stesso. (CIOÈ LA FIGURA "TRIANGOLO")



↳ 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'altezza 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 STESSO

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 → la composizione è associativa e si ha un'identità, quindi l'insieme delle simmetrie è un monoide

↳ Ogni simmetria ha quella inversa (AD ESEMPIO, la riflessione ha come inversa la riflessione stessa) → RIFLETTO UNA VOLTA E HO IL TRIANGOLO CON A E B INVERTITI, RIFLETTO DI NUOVO E HO A E B AL LORO POSTO

Sto dicendo che la struttura con tutte le funzioni che sono simmetrie, con la composizione, è un gruppo. In particolare, è un gruppo abeliano, infatti riflessione composta identità sarà uguale a identità composta riflessione ecc...

Correzione esercizi 29/10/2021 (LEZIONE 15)

2. $A = \{a, b, c\}$ → L'OPERAZIONE È LA GIUSTAPOSIZIONE

- I_1 = "Parole che contengono una sola a"

I_1 non è una parte chiusa perché presi due elementi dall'insieme I_1, la loro giustapposizione non si trova in I_1

↳ $a \in I_1$ ma $aa \notin I_1$ → Parte non chiusa

↳ LA PAROLA "a" HA UNA SOLA a ↳ ANCHE "b" ECC.

↓ LA COMPOSIZIONE DI DUE PAROLE CON UNA SOLA a NON DÀ UNA PAROLA CON UNA SOLA 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 uno di questi x_m e di questi y_n è una a. Cioè:

SE DEVO DIMOSTRARE PER TUTTI A ALLORA DEVO ESSERE GENERICO

$$((\exists i, j \in \mathbb{N})(1 \leq i, j \leq m))(x_i = a = y_j)$$ → SIA X CHE Y HANNO ALMENO UNA A PERCHÉ APPARTENGONO A I_2

Faccio la giustapposizione xy. Quindi:

$xy = x_1 x_2 x_3 \dots x_m y_1 y_2 y_3 \dots y_n$ ma dato che almeno un elemento di x ha una "a" (cioè x_i) allora $xy \in I_2$

SE DEVO DIMOSTRARE CHE È UNO CHE NON VA ALLORA USO UN CONTROESEMPIO

Di conseguenza I_2 è una parte chiusa.

Inoltre, I_2 è anche un sottosemigruppo perché associativo, ma non un sottomonoide dato che non c'è l'elemento neutro (la parola vuota non appartiene ad A)

6. $(\mathcal{P}(\mathbb{N}), \Delta)$ è un gruppo? è abeliano?

↳ Vediamo quale può essere l'elemento neutro.
È il vuoto → $X \Delta \emptyset = (X \cup \emptyset) \setminus (X \cap \emptyset) = X \setminus \emptyset = X$

Per l'esplicitazione della differenza simmetrica, $(\forall X, Y)(X \Delta Y = (X \cup Y) \setminus (X \cap Y))$. La differenza simmetrica è commutativa perché lo sono $X \cup Y$ e $X \cap Y$.
Inoltre, abbiamo già visto che è associativa.
↳ $(\forall X, Y, Z)((X \Delta Y) \Delta Z = X \Delta (Y \Delta Z))$

Quindi notiamo che $(\mathcal{P}(\mathbb{N}), \Delta)$ è un monoide commutativo.
↳ Bisogna vedere se ci sono gli elementi inversi, cioè, vogliamo trovare un Y che per ogni X dia l'insieme vuoto. Cioè: $X \Delta Y = \emptyset$
↓
Questo elemento è X stesso perché $(\forall X \in \mathbb{N})(X \Delta X = \emptyset)$
Inoltre, visto che Δ è commutativo, X è l'unico inverso perché è sia inverso destro che inverso sinistro.
↳ Quindi $(\mathcal{P}(\mathbb{N}), \Delta)$ è un gruppo abeliano perché ogni elemento X ha un inverso Y ed è un gruppo commutativo

9. $a = \{1, 2, 3\}$

$\boxed{MAP_{Bi}(a,a) := Sym(a)}$ → l'insieme simmetrico di a

l'insieme delle applicazioni biettive di a in a

Consideriamo l'insieme delle funzioni iniettive di a in a ($MAP_{In}(a,a)$)

↓

Prendo l'operazione "composizione", quindi:

CONDIZIONI DI FINITEZZA: INIETTIVA E ANCORA INIETTIVA ↓ A CHE APPLICAZIONI DI A SU A INIETTIVE POSSO COMPORRE RISPONDENDO DA A SU A

$(MAP_{In}(a,a), \circ)$ è una struttura algebrica

↳ Questo è un monoide perché l'elemento neutro è Id_a e vale l'associatività per la composizione di funzioni

In $MAP_{In}(a,a)$ ci sono anche tutte le applicazioni biettive, quindi $(MAP_{Bi}(a,a), \circ)$ è un sottomonoide di $(MAP_{In}(a,a), \circ)$

↓

Inoltre, sappiamo già che ogni applicazione biettiva ha l'inversa, quindi

$(Sym(a), \circ)$ è un gruppo ma non abeliano dato che $\circ$ non è commutativo

AD ESEMPIO: $\alpha: a \to a$

il gruppo di Sym

$\alpha(1) = 2$ $\quad \alpha^{-1}(1) = 3$
$\alpha(2) = 3$ $\quad \alpha^{-1}(2) = 1$
$\alpha(3) = 1$ $\quad \alpha^{-1}(3) = 2$

↓

Prendo poi $\beta: a \to a$

$\beta(1) = 2$
$\beta(2) = 1$
$\beta(3) = 3$

→ da loro composizione:

$(\alpha \circ \beta)(1) = (\alpha(\beta(1))) = \alpha(2) = 3$
$(\beta \circ \alpha)(1) = (\beta(\alpha(1))) = \beta(2) = 1$ $\Big\}\ \alpha \circ \beta \neq \beta \circ \alpha$

ELEMENTO NEUTRO E INVERSO NELLE SOTTOSTRUTTURE

Gli elementi neutri e gli inversi possono anche non trasportarsi nelle sottostrutture

AD ESEMPIO:

- Consideriamo la struttura:
  $(\mathbb{Z},+)$ che è un monoide

  La parte chiusa $(\mathbb{N}\setminus\{0\},+)$ è un sottosemigruppo di $(\mathbb{Z},+)$ ma non ha più l'elemento neutro → non è un sottomonoide

  $(\mathbb{N}\setminus\{0\},+) \leqslant (\mathbb{Z},+)$

L'INTERSEZIONE DI PARTI CHIUSE È ANCORA UNA PARTE CHIUSA

- Sia $(S,*)$ una struttura algebrica e sia t un sottoinsieme delle parti di S $(t \subseteq \mathcal{P}(S))$ 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 $\mathbb{N}$

Data la struttura algebrica $(\mathbb{N},+)$, posso prendere $t=\{2\mathbb{N},3\mathbb{N}\} \subset \mathcal{P}(\mathbb{N})$.

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 → Devo far vedere che $\forall x, y \in \cap t$, $x * y \in \cap t$

Prendiamo $x, y \in \cap t$ (GLI ELEMENTI DEGLI ELEMENTI DI t). Per definizione di $\cap t$, $(\forall z \in t)(x, y \in z)$ Ma ogni $z \in t$ è una parte chiusa, quindi $x * y \in z$ per la definizione di parte chiusa

PER IPOTESI

↳ $(\forall z \in t)(x * y \in z)$, quindi per definizione $x * y \in \cap t$

↓

$\cap t$ 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

↳ ESSERE UN SOTTOGRUPPO SIGNIFICA ESSERE UNA PARTE CHIUSA CHE HA ANCHE GLI INVERSI

SOTTOSTRUTTURE GENERATE

Abbiamo visto che all'interno di una struttura ci sono tante sottostrutture

↳ Voglio trovare le più piccole sottostrutture che contengano un certo sottoinsieme

AD ESEMPIO:

Prendo $(\mathbb{N}, +)$ in questo monoide.

Voglio il "più piccolo" $S \leq \mathbb{N}$ tale che $2 \in S$

↳ Visto che è un sottomonoide allora deve essere una parte stabile → Ci deve stare 2, 4, 6 ecc...
$2+2$ $2+2+2$

"Il più piccolo" lo codifico nel senso dell'intersezione

↳ Voglio l'intersezione di tutte le strutture che contengono 2 → IN QUESTO CASO IL SOTTOMONOIDE È "I NUMERI PARI"

SOTTOSTRUTTURA GENERATA DA t

Sia $(S, *)$ una struttura algebrica e prendo un sottoinsieme di S $(t \subseteq S)$. La sottostruttura generata da t (si scrive $\langle t \rangle$) è:

TUTTI GLI X INTERSECATI TRA DI LORO

GLI X SONO SOTTOSTRUTTURE E CONTENGONO T

UN'ALTRA NOTAZIONE

$$\langle t \rangle := \bigcap \{ X \in \mathcal{P}(S) \mid X \leq S \wedge t \subseteq X \} \quad \left(=: \bigcap_{X \leq S,\, t \subseteq \mathcal{P}(X)} X \right)$$

È UNA DEFINIZIONE

È UNA SOTTOSTRUTTURA DELLO STESSO TIPO DI S (SE S È UN MONOIDE X DEVE ESSERE UN MONOIDE E AVERE L'UNITÀ)

↳ Ora abbiamo definito cosa significa essere "il più piccolo", ma come facciamo a trovare tutte le sottostrutture 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, $\langle t \rangle$ È PROPRIO QUESTO IN QUESTI CASI

↳ STO DICENDO CHE $\langle t \rangle$, CIOÈ L'INTERSEZIONE UNARIA DI TUTTE LE PARTI DI S ACC. (DEFINIZIONE SOPRA) SONO TUTTI GLI ELEMENTI CHE APPARTENGONO A S TALI CHE SI SCRIVONO COME COMPOSIZIONE DI m ELEMENTI CHE APPARTENGONO A t

GRUPPI

$$\langle t \rangle = \{ x \in S \mid (\exists m \in \mathbb{N})(\exists \varepsilon_1, \dots, \varepsilon_m \in \{-1, 1\})((\exists x_1, \dots, x_m \in t)(x = x_1^{\varepsilon_1} * \dots * x_m^{\varepsilon_m})$$

$x = x_1^{-1} * x_2^{-1} * x_3^{-1} * x_4^{1} * \dots x_m^{1}$

↳ x^{-1} RAPPRESENTA L'INVERSA DI X

LA DIFFERENZA TRA MONOIDE E GRUPPO È CHE CI SONO O MENO LE INVERSE → NEL MONOIDE SI TOLGONO LE ε

DIMOSTRAZIONE DELLA CARATTERIZZAZIONE DEI MONOIDI

Per dimostrare che $\langle t \rangle = \{ x \in S \mid (\exists m \in \mathbb{N})(\exists x_1, \dots, x_m \in t)(x = x_1 * \dots * x_m) \}$ usiamo la doppia inclusione, dalla tautologia della doppia implicazione.

↳ Per far vedere che due insiemi sono uguali devo far vedere che $\langle t \rangle \subseteq \{ x \in S \mid (\exists m \in \mathbb{N})(\dots)(\dots) \}$ e viceversa, cioè che $\{ x \in S \mid (\exists m \in \mathbb{N})(\dots)(\dots) \} \subseteq \langle t \rangle$

($\subseteq$) Vediamo prima che $\langle t \rangle \subseteq \{x \in S \mid (\exists m \in \mathbb{N})(\ldots)(\ldots)\}$

↳ $\langle t \rangle$ è una $\mathcal{P}(S)$ perché è l'intersezione di certe $\mathcal{P}(S)$ che contengono t

Per comodità, chiamiamo:

$$b = \{x \in S \mid (\exists m \in \mathbb{N})(\exists x_1, \ldots, x_m \in t)(x = x_1 * \ldots * x_m)\}$$

faccio vedere che b è una parte chiusa di S che contiene t, che quindi partecipa all'intersez.

Prendo $x, y \in b$.

Per la definizione di b, $x * y \in b$ → b, quindi, è una parte chiusa

↳ Infatti, $(\exists m \in \mathbb{N})(x = x_1 * \ldots * x_m)$ ed $(\exists m \in \mathbb{N})(y = y_1 * \ldots * y_m)$, quindi $(\exists n \in \mathbb{N})(\exists m \in \mathbb{N})$ dove $x * y = x_1 * \ldots * x_n * y_1 * \ldots * y_m$, quindi questa cosa $(x * y)$ sta ancora in b.

di solito si aggiunge una definizione che ci stabilisce l'elemento neutro

↳ Posso anche definire il caso in cui $m = 0$, quindi avrò che $0 \in b$ e questo sarà l'elemento neutro.

Di conseguenza b è una sottostruttura 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 per definizione $(\exists x_1 \in t)(x = x_1)$, quindi $x \in t \to b$ diventa 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 facciamo l'intersezione.

($\supseteq$) Vogliamo dimostrare che $\{x \in S \mid (\exists m \in \mathbb{N})(\ldots)(\ldots)\} \subseteq \langle t \rangle$

Vogliamo quindi dimostrare che tutte le sottostrutture di S che contengono t, contengono anche b.

↳ Devo far vedere che $(\forall x \leq S)(t \subseteq x \to b \subseteq x)$, perché da ciò segue che $b \subseteq \langle t \rangle$ → dato che $x \in$ una sottostruttura di S e b fa parte di x

Sia X una parte di S e che contenga t
↳ $X \leq S \wedge t \subseteq X$ ↳ È UNA GENERICA SOTTOSTRUTTURA CHE CONTIENE t.

Prendo poi un generico elemento di b
↳ $Y = Y_1 * \ldots * Y_m : Y_1, \ldots, Y_m \in t$

Poiché X è una parte chiusa, allora $y \in X$.
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, dove abbiamo preso il monoide $(\mathbb{N}, +)$

$\langle 2 \rangle$ 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.
↳ $X_1, X_2, X_3, \ldots, X_m$ sono sempre 2.

$X = X_1 + X_2 + X_3 + \ldots + X_m = 2 + 2 + 2 + \ldots + 2$ m volte

NOTAZIONI DELLA SOTTOSTRUTTURA GENERATA

La sottostruttura generata da t si può indicare sia con che senza le "{}"

↳ t è UNA PARTE DI S → UN SOTTOINSIEME

ESEMPIO:

- Posso scrivere sia $\langle\{1\}\rangle$ che $\langle 1\rangle$
- Anche $\langle\{a,b,c\}\rangle$ che $\langle a,b,c\rangle$ sono equivalenti.

ESEMPI:

- Nel monoide $(\mathbb{N},+)$:

$\langle\{1\}\rangle = \mathbb{N}$ perché sono tutte le ripetizioni dell'operazione "+" con gli elementi che stanno in $\{1\}$ (cioè 1)

↳ È la somma di 1 per n volte con n che varia → ESEMPIO: $1 = 1$
$2 = 1+1$
$3 = 1+1+1$

$\langle 2\rangle = 2\cdot\mathbb{N}$ (Tutti i numeri pari)

- Nel monoide $(\mathbb{N},\cdot)$:

$\langle 1\rangle = \{1\}$ perché sono tutte le possibili ripetizioni di $1\cdot 1\cdot 1\cdot 1\cdot\ldots\cdot 1$

↳ Inoltre questo è un sottomonoide perché abbiamo anche l'elemento neutro

Correzione esercizi 02/11/2021 (LEZIONE 16)

3) $\langle t \rangle = \{ x \in g \mid (\exists m \in \mathbb{N})((\exists \varepsilon_1, \dots, \varepsilon_m \in \{-1,1\})((\exists x_1, \dots, x_m \in t)(x = x_1^{\varepsilon_1} * \dots * x_m^{\varepsilon_m})))\}$ T.H.

HP: $(g, *)$ è un gruppo; $t \neq \emptyset$

↳ se $\varepsilon = -1$, quell x^{-1} rappresenta l'inversa

Sappiamo che $\langle t \rangle \overset{DEF}{:=} \bigcap \{ x \in \mathcal{P}(g) \mid t \subseteq x \wedge x \leq g \}$

La dimostrazione è uguale a quella del caso del monoide con la differenza che ora $t \neq \emptyset$

Voglio far vedere che l'insieme $\langle t \rangle$ e $\{ x \in g \mid (\exists m \in \mathbb{N})(\dots) \}$ sono uguali

↳ lo vedo con la doppia inclusione

DIM

($\subseteq$) Devo far 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 sottostrutture di g, di cui $\langle t \rangle$ è l'intersezione tra tutte queste sottostrutture, è proprio l'insieme $\{ x \in g \mid (\exists m \in \mathbb{N})((\exists \varepsilon_1, \dots, \varepsilon_m \in \{-1,1\})(\dots))\}$

↳ Di fatti, ne segue che poi $\langle t \rangle \subseteq \{ x \in g \mid (\exists m \in \mathbb{N})(\dots)(\dots)(\dots)\}$

$b = \{ x \in g \mid (\exists m \in \mathbb{N})((\exists \varepsilon_1, \dots, \varepsilon_m \in \{-1,1\})((\exists x_1, \dots, x_m \in t)(x = x_1^{\varepsilon_1} * \dots * x_m^{\varepsilon_m})))\}$

dove:

- Essere una parte di g → È una cosa ovvia
- Contenere t → È ovvio perché se ho $m = 1$ ed $\varepsilon_1 = 1$, avrò che b sono tutti e solo gli elementi $x_1 \in t$, quindi $x = x_1$, quindi $x \in t$

POSSO AVERE ANCHE LE COMPOSIZIONI DI UN SOLO ELEM.

- È una sottostruttura di g → Stesso ragionamento della dimostrazione della caratterizzazione dei monoidi

Quindi $\langle t \rangle \subseteq b$

(2) Devo far vedere che $\bigcap_{x \in a} a \subseteq \bigcap g$, (un generico)

TUTTI GLI ELEMENTI DI a APPARTENGONO A TUTTI GLI ELEMENTI CHE SONO IN g

↓

SE $a \subseteq b \cap g$, TUTTI GLI ELEMENTI di a SONO SIA IN b CHE IN c

allora $(\forall x \in g)((\forall y \in a)(y \in x))$; quindi presa una qualunque parte chiusa di g che contiene t, questa contiene anche b.

b è una parte chiusa perché un qualunque elemento di b non è altro che la composizione di qualunque elemento di t elevati a 1 o -1

↳ Cioè sono o l'elemento stesso o il suo inverso, quindi per ogni sottogruppo di g, l'elemento (di) b c'è ancora dato che c'è la sua inversa.

↳ ESEMPIO:

$x, y, z \in S$ dove $S \leq g$ (S è un sottogruppo di g)

Quindi $x \in S$, ma anche $x^{-1} \in S$, ed anche $x^{-1}y \in S$

Quindi se ho degli elementi che appartengono a t, tutte le combinazioni di questi elementi appartengono ad S.

↳ b è contenuto in tutti i sottogruppi di g che contengono t

Quindi $b \subseteq \langle t \rangle$

ALTRIMENTI NON SAREBBE UN GRUPPO

Inoltre, sappiamo che $\langle t \rangle$ ha l'elemento neutro perché ci viene assicurato dal fatto che $t \neq \phi$

↳ Visto che $t \neq \phi$, $\exists x \in t$.

Esiste, di conseguenza, un certo $t * t^{-1} \in b$

↓

Ma questo $t * t^{-1}$ è proprio l'unità, quindi $t * t^{-1} = 1_g$

Visto che $\langle t \rangle$ è una parte chiusa, ha l'elemento neutro e ha gli inversi, è anche lui un gruppo

ELEMENTI SIMMETRIZZABILI

Denoto con $U_{(S)}$ (è un S) l'insieme degli elementi simmetrizzabili di S semigruppo → cioè tutti gli elementi della struttura che sono simmetrizzabili

$(U_{(S)}, *)$ è un gruppo? → • È il elemento neutro perché 1_S è simmetrizzabile

OPERAZIONE SIGNIFICANDO NELLA LOGICA → LA EQUIVALENZA DA PARTE SINGOLE

• l'associatività viene se $*$ è associativo → $*$ è associativo perché S è un semigruppo

• È una parte chiusa

Perché $U_{(S)}$ è una parte chiusa? → DIMOSTRIAMO DIMOSTRARE CHE PER OGNI COPPIA DI ELEMENTI SIMMETRIZZABILI, IL LORO PRODOTTO È SIMMETRIZZABILE

Prendiamo X e Y simmetrizzabili (cioè invertibili)

Per definizione: $(\exists w, z \in S)(X * w = 1_S \wedge Y * z = 1_S)$ → ELEMENTO NEUTRO

Esiste un certo elemento che composto con $X*Y$ dia l'unità? Sì, ed è $z*w$.

↳ $X*Y*(z*w) \overset{\text{ASSOCIATIVA}}{=} X*(Y*z)*w = (X*1_S)*w = X*w = 1_S$

Di conseguenza $X*Y \in U_{(S)}$, quindi $U_{(S)} \leq S$ → È 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

↳ $(U_{(S)}, *)$ è un gruppo

ESEMPI:

• $U((\mathbb{N},+)) = \{0\}$ → È L'UNICO ELEMENTO AD AVERE L'OPPOSTO

• $U((\mathbb{Z},+)) = \mathbb{Z}$ → TUTTI GLI ELEMENTI HANNO OPPOSTI

• $U((\mathbb{Z},\cdot)) = \{-1, 1\}$ → AD ESEMPIO, L'INVERSO DI 2 È 1/2 MA NON STA IN $\mathbb{Z}$, SOLO L'INVERSO DI 1 E -1 STA IN $\mathbb{Z}$

MOLTIPLICAZIONE

Sia g un gruppo del tipo "$(g, \cdot)$" → È UN ABUSO DI NOTAZIONE PERCHÉ g NON È IL GRUPPO, MA INDICO CON g IL GRUPPO $(g, \cdot)$

$XY := X \cdot Y$

UNITÀ DEL GRUPPO E DEL SOTTOGRUPPO

Sia h un sottogruppo di g ($h \leq g$)

↳ Di conseguenza, $(h, \cdot)$ è un gruppo e avrà 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

Prendo l'unità di g e la moltiplico con l'unità di h

↳ $1_g \cdot 1_h = 1_h$ → DATO CHE 1_g È L'ELEMENTO NEUTRO DI g

Visto che 1_h è l'unità di h, posso scrivere che:

↳ $1_h \cdot 1_h = 1_h$

Quindi $\cancel{1_h} \cdot 1_h = 1_g \cdot \cancel{1_h}$ → $1_h = 1_g$

SONO CANCELLABILI

DIM (2) → UN ALTRO MODO PER VEDERLO

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

$\langle u \rangle = \{u\}$ di $(S, *, u)$

ESEMPIO:

In $(\mathbb{N}, +)$

$\langle 0 \rangle = \{0\}$ perché $0+0+0+\ldots+0=0$

SOTTOMONOIDE DA UN MONOIDE

ESEMPIO:

Consideriamo $(\mathbb{N}, \cdot)$ in quanto monoide.

Vogliamo trovare il sottomonoide generato da 0

↳ $\langle 0 \rangle$ deve comunque restare un monoide, quindi anche se $0 \cdot 0 \cdot 0 \cdot 0 \ldots \cdot 0 = 0$, non posso scrivere che $\langle 0 \rangle = \{0\}$ → Devo aggiungere l'elemento neutro all'insieme $\langle 0 \rangle$ affinché sia un monoide.

$\langle 0 \rangle = \{0, 1\}$

STRUTTURE CICLICHE

$(S, *)$ è una struttura ciclica se:

$(\exists x \in S)(S = \langle x \rangle)$ → SONO LE STRUTTURE 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 possibili combinazioni della somma di 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 $1 = 3+2^{-1}$ -> ANCHE $0 = 2+2+2+3^{-1}+3^{-1}$

↳ $1 \in \langle 2,3 \rangle$ e visto che $\langle 2,3 \rangle$ è una parte chiusa, 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 Bezout

↓

Se genero un sottogruppo di $\mathbb{Z}$ con due numeri coprimi allora genero tutto $\mathbb{Z}$

- $\langle 2,4 \rangle = 2\mathbb{Z}$ (sono ancora i numeri pari)

Quindi $\mathbb{Z}$ è un gruppo ciclico, $\mathbb{N}$ è un monoide ciclico.

CANCELLABILE A SINISTRA

Se S è un semigruppo e $x \in S$, x si dice cancellabile a sinistra se:

$$(\forall y, z \in S)(xy = xz \rightarrow y = z)$$ LA SEMIFACTORIZZAZIONE

CANCELLABILE A DESTRA

Se S è un semigruppo e $x \in S$, x si dice cancellabile a destra se:

$$(\forall y, z \in S)(yx = zx \rightarrow y = z)$$

CANCELLABILE

Se S è un semigruppo e $x \in S$, x si dice cancellabile se è cancellabile a destra e cancellabile a sinistra

NON CANCELLABILE A SINISTRA

x non è cancellabile a sinistra se:

$$(\exists y, z \in S)(xy = xz \wedge y \neq z)$$

NON CANCELLABILE A DESTRA

x non è cancellabile a destra se:

$$(\exists y, z \in S)(yx = zx \wedge y \neq z)$$

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

<u>DIM</u>

Dato che x è invertibile, allora, per definizione:

$$(\exists \bar{x} \in g)(x\bar{x} = 1_g \wedge \bar{x}x = 1_g)$$

Siano $y, z \in g$. $xy = xz$ → VOGLIO FAR VEDERE CHE x È CANCELLABILE, QUINDI CHE $y = z$

Avrò che: $y = 1_g y = \bar{x}xy = \bar{x}xz = 1_g z = z$

Con lo stesso procedimento si può dimostrare che vale la cancellabilità a destra

↳ Quindi x è cancellabile → 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:

$\sigma_x : z \in S \longmapsto xz \in S$ (TRASLAZIONE SINISTRA)

↳ SIGMA

$\delta_x : z \in S \longmapsto zx \in S$ (TRASLAZIONE DESTRA)

↳ DELTA

↳ SE C'È UN ELEMENTO $z \in S$, APPLICO x DALLA 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 $\sigma_x(Y)$ e XZ è proprio uguale a $\sigma_x(Z) \rightarrow \sigma_x(Y) = XY$ e $\sigma_x(Z) = XZ$

↳ Quindi, $(\forall Y, Z \in g)(\sigma_x(Y) = \sigma_x(Z) \rightarrow Y = Z)$

ma questa è proprio la definizione di funzione iniettiva. Ne segue che:

- X è cancellabile a sinistra se e solo se σ_x è iniettiva.
- X è cancellabile a destra se e solo se δ_x è iniettiva.

INVERSA DI σ_x E δ_x

Se $X \in U(S)$, posso trovare l'inversa di σ_x

↳ l'inversa di σ_x è $\sigma_{x^{-1}}$ → L'INVERSA DI σ_x È σ DELL'INVERSA DI X

$$\boxed{\sigma_{x^{-1}} = \sigma_x^{-1} \quad e \quad \delta_{x^{-1}} = \delta_x^{-1}}$$

DIM

Dato che X è invertibile, se faccio la composizione di $\sigma_{x^{-1}}$ e σ_x, ottengo l'identità

↳ $(\sigma_{x^{-1}} \circ \sigma_x)(Z) = \sigma_{x^{-1}}(\sigma_x(Z)) = \sigma_{x^{-1}}(X \cdot Z) = X^{-1} \cdot (X \cdot Z) = Z$

↳ $\sigma_{x^{-1}}$ È L'INVERSA SINISTRA → PER LO STESSO PROCEDIMENTO, $\sigma_{x^{-1}}$ È ANCHE L'INVERSA DESTRA

- Dato che σ_x e δ_x sono invertibili, allora sono biettive

RELAZIONE TRA ELEMENTI CANCELLABILI E INVERTIBILI

Abbiamo dimostrato (2 PAGINE PRIMA) 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 $m \neq 0$, sappiamo che:

$$(\forall x, y \in \mathbb{Z})(mx = my \longrightarrow x = y)$$ → DEFINIZIONE DI CANCELLABILE A SINISTRA

ma m, quasi sempre, non è invertibile

↳ ESEMPIO:

$\cdot\ 2x = 2y$ → 2 è cancellabile ma non è invertibile in $\mathbb{Z}$

TAVOLE DI CAYLEY

Ci permettono di visualizzare cosa succede nelle strutture algebriche con un'operazione.

↳ SONO BIDIMENSIONALI PERCHÉ L'OPERAZIONE È BINARIA

↓

Prendo $(S, *)$ con $S \neq \emptyset$

AD ESEMPIO:

- $S = \{a, b\}$
- la tavola di Cayley ci permette di definire l'operazione $*$

QUESTA È L'UNICA TAVOLA CON DUE SOLI ELEMENTI

*	a	b
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, resta uguale

Un elemento è neutro a destra se la colonna corrispondente resta uguale a quella degli elementi

↳ a è l'unità di $(S, *)$

↳ Inoltre, dato che $a * a = a$, a è l'inverso di se stesso

NEUTRO A DESTRA

NEUTRO A SINISTRA →

*	a	b
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

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

→ NON CI POSSONO ESSERE SPAZI VUOTI PERCHÉ ALTRIMENTI * NON SAREBBE UN'OPERAZIONE
↓
L'OPERAZIONE È DEFINITA SU TUTTE LE COPPIE DEL DOMINIO $S \times S$

- Affinché b sia invertibile a sinistra, allora:

$(\exists x \in S)(x \cdot b = 1)$

↳ Uno della colonna, per b, deve dare a ↳ $c*b=a$

↓

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, scambiando righe e colonne, la tavola resta uguale ↳ SE HO CHE $b*c=a$, VOGLIO ANCHE CHE $c*b=a$

↳ SO HO FATTO • TABELLA

↓

$*$ è commutativa se la tavola è simmetrica rispetto alla diagonale principale

- x è cancellabile a sinistra quando σ_x è iniettiva

↳ σ_x è la riga che sta su x → (CONSIDERIAMO $x=b$) $\sigma_b(a)=b$ $\sigma_b(c)=a$ $\sigma_b(b)=c$

↳ Dato che è iniettiva, tutti gli elementi della riga sono differenti

↓

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 = Cancellabili a sinistra

PER FAR VEDERE CHE C È UNA PARTE CHIUSA, $x*y$ DEVE APPARTENERE A C

Prendo $x, y \in C$. Voglio far vedere che anche la loro composizione appartiene a C. Cioè che $x*y \in C$, cioè:

↳ $(\forall w, z \in S)((x*y)*z = (x*y)*w \longrightarrow z = w)$ DEFINIZIONE DI CANCELLABILE A SINISTRA DI $x*y$

Dobbiamo vedere che C è parte chiusa di ogni gruppo abeliano

↳ Presi $w, z \in S$, so che per l'associatività $x*(y*z) = x*(y*w)$. 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 parte chiusa.

10. $S = \{x, y, u\}$

*	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, $(ux)*y$ È UGUALE A $(x*y)*u$

- u è l'elemento neutro → RIGA E COLONNA DI U SONO IDENTICHE
- $(S, *)$ è commutativo → PERCHÉ SIMMETRICA RISPETTO ALLA DIAGONALE
- Tutti gli elementi sono cancellabili → APPARONO UNA SOLA VOLTA IN OGNI RIGA E COLONNA
- $(S, *)$ è un gruppo abeliano → LO NOTIAMO PERCHÉ $x*y$ FA u E ANCHE $y*x$ FA u, QUINDI y È L'INVERSO DI x E VICEVERSA

9. $S = \{X, Y, u\}$ → la struttura $(S, *)$ non è un monoide, ma ha l'elemento neutro

*	u	X	Y
u	u	X	Y
X	X	u	X
Y	Y	Y	u

X si ripete nella riga di X e Y si ripete nella riga di Y

- u è l'elemento neutro
- Poiché $Y \neq u$, ma $X * Y = X = X * u$, X non è cancellabile a sinistra
  ↳ Anche Y non lo è dato che $Y * u = Y * X$
- Tutti gli elementi sono cancellabili a destra ↳ NIENTE SI RIPETE NELLA COLONNA

PERCHÉ NON È UN MONOIDE?

- Notiamo che:

$Y = u * Y = (X * X) * Y$
↳ $X * X = u$

Assumiamo per assurdo che sia associativa. Quindi:

$(X * X) * Y = X * (X * Y) = X * X = u$ ↯ $(X*X)*Y \neq X*(X*Y)$

→ Quindi $(S, *)$ non è un monoide perché non è associativa

POTENZE DI UN ELEMENTO → SI POSSONO DIMOSTRARE PER INDUZIONE

Sia $(S, *)$ un semigruppo

- $(\forall x \in S)(\forall m, n \in \mathbb{Z})(x^m \in S \wedge x^n \in S \rightarrow x^m \cdot x^n = x^{m+n})$
- $(\forall x \in S)(\forall m, n \in \mathbb{Z})(x^m \in S \wedge x^n \in S \rightarrow (x^m)^n = x^{m \cdot n})$

↳ Dato che $(S, *)$ è un semigruppo, x non è detto che abbia gli inversi → Devo specificare che:
$x^m \in S$ e che $x^n \in S$ → PER ESEMPIO, PER USARE $m = -2$, $x^{-2} \in S$
↳ Se S è un gruppo, questa parte posso anche toglierla perché gli inversi ci sono sicuramente

DEFINIZIONE DELLE POTENZE

- $\boxed{x^n := x * x * \ldots * x}$ per n volte → $\forall n \in \mathbb{N} \setminus \{0\}$
- $\boxed{x^0 := 1_S}$ se è l'elemento neutro → $n = 0$
- $\boxed{x^{-n} := (x^n)^{-1}}$ se abbiamo la inversa → $\forall n \in \mathbb{N} \setminus \{0\}$
  ↳ cioè se $(S, *)$ è un gruppo.

GENERALE PER OGNI STRUTTURA

- Se in notazione additiva, le potenze si dicono multipli.
- Vale anche la proprietà commutativa delle potenze perché:

$$x^m \cdot x^n = x^{m+n} = x^{n+m} = x^n \cdot x^m$$

↳ LE POTENZE COMMUTANO TRA DI LORO PERCHÉ COMMUTA LA SOMMA TRA GLI ESPONENTI

- Ogni semigruppo ciclico è commutativo.
  ↳ cioè che $(\exists x \in S)(S = \langle x \rangle)$

↳ IL SEMIGRUPPO CICLICO È GENERATO DA $x * x * x * \ldots * x$ PER n VOLTE, CHE NON È ALTRO CHE x^n, CHE È COMMUTATIVO

AD ESEMPIO:

- Il gruppo $(S, *)$ con $S = \{x, y, u\}$ è un gruppo ciclico di ordine 3

*	u	x	y
u	u	x	y
x	x	y	u
y	y	u	x

$x * x = y$ e $x * y = u$, quindi tutti gli elementi del gruppo erano potenze di x:

↳ $\cdot\, x = x^1$
$\cdot\, y = x * x = x^2$
$\cdot\, u = x * y = x * x * x = x^3$

• Sia $m \in \mathbb{Z}$ in $(\mathbb{Z},+)$

I MULTIPLI DI m IN Z

$m \cdot \mathbb{Z} = \{ m \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(m = k\,m) \} \leq \mathbb{Z}$

↳ $m \cdot \mathbb{Z}$ È UN SOTTOGRUPPO DI $\mathbb{Z}$

↳ • C'è l'unità quando $k=0$, $m \cdot 0 = 0$

• È una parte chiusa perché: $k_1 m + k_2 m = (k_1 + k_2) \cdot m \in m \cdot \mathbb{Z}$

• Ha gli inversi perché: Preso km, anche $-km \in m\mathbb{Z}$

↳ È SEMPRE UN MULTIPLO DI $\mathbb{Z}$

Alcuni esempi di sottogruppi di $\mathbb{Z}$ sono:

• $\{0\} = 0\mathbb{Z}$ ↳ TUTTI GLI m MULTIPLI DI ZERO

• $\mathbb{Z} = 1\mathbb{Z}$ → TUTTI I MULTIPLI DI 1

• $2\mathbb{Z}$ → I NUMERI PARI

• Si può dimostrare che i sottogruppi di $(\mathbb{Z},+)$ sono tutti e soli i <u>multipli di $\mathbb{Z}$</u>

OMOMORFISMI TRA STRUTTURE ALGEBRICHE

↳ È una operazione binaria

OMOMORFISMO → Stessa forma, o simile.

In matematica abbiamo tante cose diverse che sono praticamente la stessa cosa (o simili) → Tanti tipi di strutture algebriche che sono, bene o male, la stessa cosa

ESEMPIO:

• Consideriamo il gruppo fatto dalla parola Nuda e il gruppo formato dallo 0.

SONO GRUPPI PERCHÉ SONO CHIUSI, HANNO L'INVERSO E L'UNITÀ

↳ Questi due gruppi sono bene o male gli stessi perché hanno un solo elemento e la stessa operazione

↳ C'è un isomorfismo tra i due

DEFINIZIONE DI OMOMORFISMO

Prendo $(S,*)$ e $(\bar{S},\bar{*})$ → L'OPERATORE $*$ è SIMILE A $\bar{*}$

- Una funzione $\varphi: S \to \bar{S}$ si dice omomorfismo se

$$\boxed{(\forall x,y \in S)(\varphi(x*y) = \varphi(x) \bar{*} \varphi(y))}$$

→ POSSIAMO PASSARE DA UNA STRUTTURA ALL'ALTRA TRAMITE QUESTA FUNZIONE CHE RISPETTA L'OPERAZIONE $*$ E $\bar{*}$

TRA x E y PUO' STARCI SOLO $*$

ESEMPIO:

- EXP: $x \in \mathbb{R} \mapsto e^x \in \mathbb{R}$

è un omomorfismo tra la la somma e il prodotto perché $e^{x+y} = e^x \cdot e^y$ → È UN OMOMORFISMO PERCHE' STA PORTANDO LA SOMMA IN UN PRODOTTO TRA LE IMMAGINI e^x E e^y

$(\mathbb{R},+)$ e $(\mathbb{R}\setminus\{0\},\cdot)$ sono la struttura dell'omomorfismo

MONOMORFISMO

- Omomorfismo iniettivo si dice monomorfismo

EPIMORFISMO

- Omomorfismo suriettivo si dice epimorfismo

ISOMORFISMO

- Omomorfismo biettivo si dice isomorfismo

ESEMPIO:

- L'applicazione identità è un isomorfismo perché conserva la struttura e le sue caratteristiche

- Anche la funzione logaritmica è un isomorfismo perché è l'inversa della funzione esponenziale

L'INVERSA DI UN ISOMORFISMO È UN ISOMORFISMO?

Consideriamo $(S, *)$ e $(\bar{S}, \bar{*})$ e l'isomorfismo φ tra le due strutture.

Essendo φ biettiva, esiste φ^{-1} e sarà anch'essa un omomorfismo.

L'INVERSA

DIM Prendo $x, y \in \bar{S}$ (IL DOMINIO DELL'INVERSA) e considero:

$$\boxed{\varphi(\varphi^{-1}(x) * \varphi^{-1}(y))} = \varphi(\varphi^{-1}(x)) \bar{*} \varphi(\varphi^{-1}(y)) = \boxed{x \bar{*} y}$$

DALLA PROPRIETÀ DELL'ISOMORFISMO

Applico φ^{-1} $\boxed{\text{ambo}}$ i lati e avrò:

$$\varphi^{-1}(x) * \varphi^{-1}(y) = \varphi^{-1}(x \bar{*} y)$$

↳ Quindi anche φ^{-1} è un isomorfismo

PROPRIETÀ CONSERVATE DEGLI EPIMORFISMI

Gli epimorfismi "conservano":

- la commutatività
- l'associatività
- $\boxed{\text{Gli elementi neutri}}$ → QUELLI A DESTRA LI MANDA A DESTRA, QUELLI A SINISTRA LI MANDA A SINISTRA
- Gli inversi

DIM (CONSERVAZIONE DEGLI ELEMENTI NEUTRI) → ASSOCIA L'ELEMENTO NEUTRO DI UN GRUPPO NELL'ELEMENTO NEUTRO DELL'ALTRO

- Consideriamo $\varphi: S \xrightarrow{EPI} \bar{S}$ e $1_S \in S$
- Sia $y \in \bar{S}$, $y = y \bar{*} \overbrace{\varphi(1_S)}^{\text{UNITÀ DI } \bar{S}} = \varphi(x) \bar{*} \varphi(1_S)$ perché, visto che φ è suriettiva, $(\exists x \in S)(\varphi(x) = y)$ → DEFINIZIONE DI SURIETTIVITÀ
- Ma φ è un omomorfismo, quindi avrò che:

$$\varphi(x) \bar{*} \underbrace{\varphi(1_S)}_{\text{SI CONTRADDICE}} = \varphi(x * 1_S) = \varphi(x) = y$$

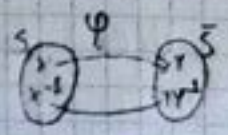
→ l'elemento neutro di $\bar{S}$ perché $\varphi(1_S)$ è l'unità di $\bar{S}$

ELEMENTO NEUTRO

DIM (CONSERVAZIONE DEGLI ELEMENTI INVERSI)

Per dimostrare che l'elemento inverso di x viene mandato 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 dimostro di avere l'identità.

In $\bar{S}$ abbiamo che, visto che φ è un omomorfismo,

$\varphi(x^{-1}) \bar{*} \varphi(x) = \varphi(x^{-1} * x) = \varphi(1_S) = 1_{\bar{S}}$ → SAPPIAMO CHE L'IDENTITÀ SI TRASPORTA

Inoltre, $(\varphi(x))^{-1} \bar{*} \varphi(x) = 1_{\bar{S}}$, quindi $\varphi(x^{-1}) = (\varphi(x))^{-1}$ e sono la stessa inversa sinistra di $\varphi(x)$

Ripetendo lo stesso procedimento considerando $\varphi(x^{-1})$ e $(\varphi(x))^{-1}$ le inverse destre otterremmo lo stesso risultato, quindi $\varphi(x^{-1}) = (\varphi(x))^{-1}$ e sono la stessa inversa

DIM (CONSERVAZIONE DELLA COMMUTATIVITÀ)

Prendo $x, y \in \bar{S}$ e considero $(S, *)$ commutativo.

Dato che φ è suriettiva, $\exists (\exists w, z \in S)(\varphi(w) = x \wedge \varphi(z) = y)$

Prendo in $\bar{S}$, $x \bar{*} y$

↳ $x \bar{*} y = \varphi(w) \bar{*} \varphi(z)$

Dato che φ è un omomorfismo

↳ $\varphi(w) \bar{*} \varphi(z) = \varphi(w * z)$

Ma $(S, *)$ è commutativo, quindi

↳ $\varphi(w * z) = \varphi(z * w) = \varphi(z) \bar{*} \varphi(w) = y \bar{*} x$

→ LA COMMUTATIVITÀ SI CONSERVA

PERCHÈ GLI OMOMORFISMI SONO IMPORTANTI?

→ Il fatto che ci siano degli omomorfismi ci dice delle cose molto importanti su $\bar{S}$

↳ A volte può succedere che $\bar{S}$ sia un insieme molto bizzarro e difficile da capire

↳ Possiamo così trovare un insieme S più semplice da descrivere e, visto che c'è l'omomorfismo, ci aiuta a descrivere più facilmente $\bar{S}$ grazie alle proprietà conservate

ESEMPI:

- Consideriamo $S \neq \emptyset$ e definiamo la funzione f:

$$f: \quad X \in \mathcal{P}(S) \mapsto S \setminus X \in \mathcal{P}(S)$$

Sappiamo che la funzione f è biettiva

Sappiamo che $\forall X, Y \in \mathcal{P}(S)$, $\quad S \setminus (X \cup Y) = (S \setminus X) \cap (S \setminus Y)$ → LEGGE DI DE MORGAN

Questa proprietà ci indica che f è un isomorfismo tra $(\mathcal{P}(S), \cup)$ e $(\mathcal{P}(S), \cap)$

SE MI DIMENTICO CHI È L'ELEMENTO NEUTRO DI UNO, BASTA CHE MI RICORDO QUELLO DELL'ALTRO E LO FACCIO L'IMMAGINE TRAMITE f

ELEMENTO NEUTRO DI $\cup = f(\emptyset) = S \setminus \emptyset = S$

ELEMENTO NEUTRO DI $\cap = S$ → STESSA COSA MA DIVERSI ECC...

→ Anche se $\cup$ e $\cap$ sono due operazioni diverse, il fatto che esista un isomorfismo, ci dice che in realtà $(\mathcal{P}(S), \cup)$ e $(\mathcal{P}(S), \cap)$ sono la stessa struttura, quindi qualunque cosa dimostro 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 a due operazioni.

DEFINIZIONE DI ANELLO

Sia a un insieme non vuoto ($a \neq \emptyset$) e siano $+, \cdot$ due operazioni binarie interne di a.

La terna $(a, +, \cdot)$ si dice anello se:

- $(a, +)$ è un gruppo abeliano
- $(a, \cdot)$ è un semigruppo
- Vale la distributività di $\cdot$ rispetto a $+$
  ↳ $(\forall x, y, z \in a)(x \cdot (y + z) = xy + xz)$

ESEMPIO:

- $(\mathbb{Z}, +, \cdot)$ è un anello

ANELLO COMMUTATIVO

- $(a, +, \cdot)$ è un anello commutativo se anche $(a, \cdot)$ è commutativo → $(a, +)$ lo è già per definizione.

ANELLO UNITARIO

- $(a, +, \cdot)$ si dice anello unitario se $(a, \cdot)$ è un monoide → DEVE ESSERE L'UNITÀ MOLTIPLICATIVA

CONVENZIONI

- "0_a" o "0" è l'elemento neutro di $(a, +)$
- "1_a" o "1" è l'elemento neutro di $(a, \cdot)$ (SE C'È)

SOTTOANELLO

SONO QUELLE 2 INDICE

Se $(S, \overset{+}{\cdot}, \cdot)$ è un anello e $S \subseteq a$ chiusa,

↳ S è una parte chiusa di a

↳ S è detto sottoanello di a

ESEMPIO:

DISTRIBUTIVITÀ DI ∩ RISPETTO A ∪

- $\forall x, y, z \in \mathcal{P}(S)$ con $S \neq \emptyset$, vale $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$

Quindi $(\mathcal{P}(S), \cup, \cap)$ è un anello commutativo unitario

↓

- 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 $(a, +)$ → È PRECISAMENTE LA DEFINIZIONE

- $(\forall m \in \mathbb{N} \setminus \{0\})(mx = \underbrace{x + x + \dots + x}_{m \text{ volte}}) \to \forall x \in a$

- $(\forall m \in \mathbb{Z} \setminus \mathbb{N})(mx = \underbrace{-x - x \dots - x}_{m \text{ volte}}) \to \forall x \in a$

- $0 \cdot x = 0_a$ → Sono due zeri diversi

  LO ZERO IN $\mathbb{Z}$ — LO ZERO IN a

  ↓

  DIM $0 \cdot x = (1 - 1)x = 1x + ((-1)x) = x - x = 0_a$

  È LO ZERO DI a PERCHÉ È LA SOMMA DI UN ELEMENTO PIÙ L'OPPOSTO

- $(\forall x \in a)(x \cdot 0_a = 0_a)$ → QUI È UNA COSA OVVIA

  ↓

  DIM $x \cdot 0_a = x(x - x) = x \cdot x - x \cdot x = 0_a$

  DISTRIBUTIVITÀ

- $(\forall m \in \mathbb{N} \setminus \{0\})(x^m = \underbrace{x \cdot x \cdot \ldots \cdot x}_{m \text{ volte}}) \Rightarrow \forall x \in a$

- $(\forall m \in \mathbb{Z} \setminus \mathbb{N})(x^m = \underbrace{x^{-1} \cdot x^{-1} \cdot \ldots \cdot x^{-1}}_{m \text{ volte}}) \rightarrow \forall x \in a$

- $x(-y) = -xy = (-x)y$

$\downarrow$

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 questi sono la stessa cosa.

1) $x(-y) + xy \underset{\substack{\uparrow \\ \text{DISTRIBUTIVITÀ} \\ \text{AL CONTRARIO}}}{=} x(-y+y) = x(0) = 0x = 0$ $\rightarrow$ ELEMENTO NEUTRO DI $(a,+)$

2) $-xy + xy = 0$

3) $(-x)y + xy = y(-x+x) = y(0) = 0 \cdot y = 0$

Quindi $x(-y) = -xy = (-x)y$

- $\cdot$ è distributiva rispetto a "$-$"

- Se $(a, +, \cdot)$ è unitario, vale che:
$(\forall x \in a)(\forall m \in \mathbb{Z})((m \cdot 1_a) \cdot x = m \cdot x)$

Correzione esercizi 05/11/2021 (LEZIONE 18)

1. $f: a \to a$ $\quad S = \{f^4, f, f^2, f^3\}$

$f \in Sym(a)$ è BIETTIVA

$f(W) = X$

$f(X) = Y$

$f(Y) = Z$

$f(Z) = W$

• Dimostrare che $(S, \circ)$ è un gruppo abeliano

PER VEDERE CHE S È UNA PARTE CHIUSA

↳ 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? $f^4(W) = f \circ f \circ f \circ f(W) = f \circ f \circ f(X) = f \circ f(Y) = f(Z) = W$

↳ Se lo vedo con tutti gli elementi, noterò che f^4 non è altro che $Id_a \to f^4 = Id_a$

↓

$S = \{Id_a, f, f^2, f^3\}$

Se prendo un certo i e j tali che: $1 \leq i, j \leq 3$, $f^i \circ f^j = f^{i+j}$ per le proprietà delle potenze.

↳ Noto che se faccio qualsiasi potenza, il risultato sarà sempre in $S \to f^{2+3} = f^6 = f^{4+2} = f^2$ perché f^4 è l'identità

↳ f è una funzione periodica

↓

S è una parte chiusa.

$(S, \circ)$ ha le inverse?

Sì perché $f \circ f^3 = f^4 = 1_S$, $f^4 \circ f^4 = 1_S$, $f^2 \circ f^2 = f^4 = 1_S$ ecc..

↳ $(S, \circ)$ è un gruppo.

Inoltre, $(S, \circ)$ è abeliano perché le potenze commutano tra di loro → Vale la proprietà commutativa

Facciamo la tavola di Cayley:

$\circ$	1_S	f	f^2	f^3
1_S	1_S	f	f^2	f^3
f	f	f^2	f^3	1_S
f^2	f^2	f^3	1_S	f
f^3	f^3	1_S	f	f^2

Confrontiamola con la tavola di Cayley del esercizio 12 lezione 7 →

$*$	u	x	y	z
u	u	x	y	z
x	x	y	z	u
y	y	z	u	x
z	z	u	x	y

Notiamo che hanno la stessa tavola solo con nomi diversi

↳ Sono omorfi → Consideriamo la operazione

↳ Chi è φ?

$$\varphi: 1_S \to u$$
$$f \to x$$
$$f^2 \to y$$
$$f^3 \to z$$

Inoltre, $(S,\circ)$ è un gruppo ciclico perché S è generato da f.

↳ $S = \langle f \rangle$ → CIOÈ f^2, f^3 E f^4 TORNA INDIETRO

3. Dato $T \subseteq S$, l'immersione da T ad S è:

$i: x \in T \mapsto x \in S$

↳ Questo è un monomorfismo (omomorfismo iniettivo)

↳ NON È DETTO CHE È UN ISOMORFISMO PERCHÉ POTREBBE NON ESSERE SURIETTIVA

Essendo l'operazione in S la stessa di quella di G,

↳ $i(x * y) = x * y = i(x) * i(y)$ → È CHIARAMENTE UN OMOMORFISMO

È iniettivo perché i è una Id ma non è suriettivo:

6. $f: X \in \mathcal{P}(a) \mapsto a \cap X \in \mathcal{P}(a)$ è un automorfismo di $(\mathcal{P}(a), \cup)$? E di $(\mathcal{P}(a), \cap)$?

↳ In realtà f è la funzione identità poiché $a \cap X = X$

$f: X \in \mathcal{P}(a) \mapsto X \in \mathcal{P}(a)$ → È un isomorfismo

4-5. $\alpha: (x,y) \in \mathbb{Z} \times \mathbb{Z} \mapsto x+y+1 \in \mathbb{Z}$ $\quad f: m \in \mathbb{Z} \mapsto m+1 \in \mathbb{Z}$

$\gamma: (x,y) \in \mathbb{Q} \times \mathbb{Q} \mapsto \frac{x+y}{2} \in \mathbb{Q}$ $\quad f: a \in \mathbb{Q} \mapsto 2a \in \mathbb{Q}$

4. Voglio far vedere come f si comporta rispetto a $(\mathbb{Z}, +)$ e $(\mathbb{Z}, \alpha)$ → Sono isomorfi!

↳ Prendo due elementi $m, n \in \mathbb{Z}$

$f(m+n) = m+n+1 = m \alpha n$

Se le due strutture fossero state omomorfe con f omomorfismo, ci saremmo dovuti trovare che:

$f(m+n) = m+n+1 = f(m) \alpha f(n)$ → DEFINIZIONE DI OMOMORFISMO

CONTROESEMPIO:

↳ $\left.\begin{array}{l} f(1+1) = f(2) = 3 = 1 \alpha 1 \\ f(1) \alpha f(1) = 2 \alpha 2 = 5 \end{array}\right\}$ Non omomorfismi

5. Anche la funzione f non è un omomorfismo. Infatti, se $x, y \in \mathbb{Q}$:

↳ $\left.\begin{array}{l} f(x+y) = 2(x+y) = 2x+2y \\ f(x) \gamma f(y) = \frac{f(x)+f(y)}{2} = \frac{2x+2y}{2} = x+y \end{array}\right\}$ Non omomorfismi

↳ È possibile fare un controesempio nuovamente con $x=1$ e $y=1$

AUTOMORFISMO

Se $f: a \to a$ è un isomorfismo,
f si dice automorfismo → un isomorfismo da a in a stesso

OMOMORFISMO DI ANELLI

Se ho due anelli $(S, +, \cdot)$ e $(\bar{S}, \bar{+}, \bar{\cdot})$,
$f: S \to \bar{S}$ si dice omomorfismo di anelli se:

$$(\forall x, y \in S)\left(\left(f(x+y) = f(x) \bar{+} f(y)\right) \wedge \left(f(x \cdot y) = f(x) \bar{\cdot} f(y)\right)\right)$$

↳ Inoltre, se S ha l'elemento neutro, $f(1_S) = 1_{\bar{S}}$ → l'elemento neutro va mandato nell'altro elemento neutro

ESEMPIO:

Sappiamo che tra $(\mathcal{P}(S), \cup)$ e $(\mathcal{P}(S), \cap)$ si è un isomorfismo $\varphi: (\mathcal{P}(S), \cup) \overset{\varphi}{\simeq} (\mathcal{P}(S), \cap)$

$$\varphi: X \in \mathcal{P}(S) \longmapsto S \setminus X \in \mathcal{P}(S)$$

Perché? Vale che $\forall X, Y \in \mathcal{P}(S)$, $S \setminus (X \cap Y) = S \setminus X \cup S \setminus Y$

In particolare, φ è un isomorfismo anche tra gli anelli $(\mathcal{P}(S), \cup, \cap) \overset{\varphi}{\simeq} (\mathcal{P}(S), \cap, \cup)$

↳ φ manda $\cup$ in $\cap$ e viceversa → $S \setminus (X \cap Y) = S \setminus X \cup S \setminus Y$ → $S \setminus (X \cup Y) = S \setminus X \cap S \setminus Y$

↳ φ manda l'elemento neutro nell'elemento neutro

↳ Si parla dell'elemento neutro rispetto alla seconda operazione dato che la prima è sempre banale

I due anelli $(\mathcal{P}(S), \cup, \cap)$ e $(\mathcal{P}(S), \cap, \cup)$ sono unitari dato che: $1_{\mathcal{P}(S)} = S$ (il primo anello, dell'intersezione) mentre $1_{\mathcal{P}(S)} = \emptyset$ → dell'unione (il secondo anello)

Infatti, $\varphi(S) = S \setminus S = \emptyset$

↳ Quindi φ è un isomorfismo di anelli

LEGGE DI ANNULLAMENTO DEL PRODOTTO

Se ho l'anello $(a, +, \cdot)$, in a vale la legge di annullamento del prodotto (la indico con "LAP") se:

$$(\forall x, y \in a)(xy = 0_a \longrightarrow x = 0_a \vee y = 0_a)$$

NON PUÒ ESSERE CHE IL PRODOTTO DI DUE ELEMENTI NON NULLI FACCIA 0

Ci sono alcuni anelli dove non vale la LAP.

ESEMPIO:

- Consideriamo $(\mathcal{P}(S), \cup, \cap)$. Voglio dimostrare che qui non vale la legge di annullamento del prodotto, cioè:

$$(\exists x, y \in \mathcal{P}(S))(x \cap y = \emptyset \wedge (x \neq \emptyset \wedge y \neq \emptyset))$$

NEGAZIONE DI LAP

↳ Se $S = \{a, b\}$ (BASTA CHE S ABBIA ALMENO DUE ELEMENTI), in $\mathcal{P}(S)$ c'è $\{a\}$ e $\{b\}$ (SONO SOTTOINSIEMI DI S)

↳ 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 $(a, +, \cdot)$, se in a vale la legge di annullamento del prodotto, a si dice anello integro

DOMINIO DI INTEGRITÀ

Se ho l'anello $(a, +, \cdot)$, se a è un anello commutativo unitario integro, a si dirà dominio di integrità

unitario → HA L'ELEMENTO NEUTRO

integro → VALE LA LAP

DIVISORE SINISTRO DELLO ZERO

Un $x \in a \setminus \{0\}$ si dice divisore sinistro dello 0_a se:

$$(\exists y \in a \setminus \{0\})(xy = 0)$$

SE Y È UN ELEMENTO NON NULLO E IL PRODOTTO CON UN X DIVERSO DA 0 DÀ LO 0, X LO DICO DIVISORE SINISTRO DELLO 0

ESEMPIO: $\{a\} \cap \{b\} = \emptyset \rightsquigarrow \{a\}$ è un divisore sinistro dello 0.

DIVISORE DESTRO DELLO ZERO

Un $x \in a \setminus \{0\}$ si dice divisore destro

$$(\exists \bar{y} \in a \setminus \{0\})(\bar{y}x = 0)$$

DIVISORE DELLO ZERO

Un $x \in a \setminus \{0\}$ si dice divisore dello 0 se è un divisore sinistro e un divisore destro → DEVONO ESSERE DUE Y DIVERSI

TEOREMA

Un $x \in a$ (a È UN ANELLO) è un divisore sinistro dello 0 se e solo se x non è cancellabile a sinistra

DIM

(→) Supponiamo che x è un divisore sinistro dello 0.
Per definizione, $(\exists y \in a \setminus \{0\})(xy = 0)$
Per assurdo, se fosse che x è cancellabile a sinistra, $y = 0$ perché $xy = 0 = x0$ (Y PER DEFINIZIONE). Ma ciò è un assurdo. ↯

(←) Supponiamo che x non è cancellabile a sinistra.
Per definizione, $(\exists y, z \in a)(y \neq z \wedge xy = xz)$ → NON CANCELLABILITÀ A SINISTRA

Visto che vale $xy = xz$ e posso fare le operazioni che posso fare negli anelli, posso fare che: →

Posso avere che:

$x(y-z) = xy - xz$ per la distributività, ma $xy = xz$

quindi $xy - xz = 0$

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 DÀ 0

Stesso ragionamento x x è un divisore destro.

ANELLI BOOLEANI

Un anello $(a, +, \cdot)$ si dice booleano se:

$$(\forall x \in a)(x^2 = x)$$

↑ CIOÈ $x \cdot x$

ESEMPIO: · In $(P(S), \cup, \cap)$, abbiamo che $x \cap x = x$, quindi questo anello è un anello booleano

PROPRIETÀ

- $\boxed{\text{Se } a \text{ è booleano, } a \text{ è commutativo}}$

DIM

Siamo $x, y \in a$ → VOGLIO DIMOSTRARE CHE $x \cdot y = y \cdot x$

$x + y = (x+y)^2$ perché a è un anello booleano

ma $(x+y)^2 = x^2 + xy + yx + y^2 = x + y + xy + yx$

↳ NON POSSO SCRIVERE $2xy$ PERCHÉ NON SAPPIAMO SE $xy = yx$ → NON SAPPIAMO SE VALE LA COMMUTATIVITÀ

Quindi $x + y = x + y + xy + yx$ che, per la cancellabilità di $x+y$, sarà: $xy + yx = 0$, quindi $xy = -yx$

↳ Visto che a è un anello booleano, vale che $xy = -yx = yx$

↳ Quindi $xy = yx$ e abbiamo dimostrato la commutatività

- $\boxed{\text{Se } a \text{ è booleano, } x = -x}$

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 cancellabilità di $x+x$, $2x = 0$

↳ $2x = 0$ equivale a dire che $x + x = 0$, quindi vale che $x = -x$

TEOREMA

- Se $(a,+,\cdot)$ è un anello commutativo unitario, a è un dominio di integrità se e solo se è privo di divisori dello 0

DIM SUPPONIAMO CHE $(a,+,\cdot)$ SIA UN DOMINIO DI INTEGRITÀ

$(\rightarrow)$ Consideriamo, per assurdo, che esista X che è un divisore dello zero. Cioè:

$(\exists Y \in a \setminus \{0\})(XY=0)$. Visto che $(a,+,\cdot)$ 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

$(\leftarrow)$ SUPPONIAMO CHE $(a,+,\cdot)$ SIA PRIVO DI DIVISORI DELLO ZERO

PER IL TEOREMA DI PRIMA

Se privo 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 sono uno che è dato

$XY=X0$

TEOREMA

- Se $(a,+,\cdot)$ è un anello e a ha almeno due elementi, allora 0 non è cancellabile. In particolare 0 non è invertibile.

DIM

L'ANELLO NE HA ALMENO DUE PER IPOTESI

Prendo due elementi, lo 0 (che c'è sempre) e X.

$\hookrightarrow 0 \neq X \in a$

Sappiamo che $0 \cdot X = 0$, ma zero non è cancellabile perché se così fosse avremmo 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

L'anello $(a, +, \cdot)$ si dice corpo se $(a, +)$ e $(a \setminus \{0\}, \cdot)$ sono gruppi e vale la proprietà distributiva

(RISPETTO ALL'ANELLO, $(a \setminus \{0\}, \cdot)$ HA SICURAMENTE L'UNITÀ E GLI INVERSI)

CAMPO

Un corpo commutativo (cioè si riferisce a $(a \setminus \{0\}, \cdot)$) 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 (rispetto a $(a, \cdot)$). 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 corpo non è detto che sia un dominio di integrità perché deve essere commutativo

ESEMPIO:

- $(\mathbb{Z}, +, \cdot)$ è un dominio di integrità dato che vale la LAP ma non è un campo perché $(\mathbb{Z}, \cdot)$ non è un gruppo

RELAZIONI BINARIE → POSSONO ESSERE TUTTE SCRITTE A PARTIRE DA diag S E RELAZIONE OPPOSTA
↳ PROX LEZIONE

Sia a un insieme non vuoto ($a \neq \emptyset$) e ρ una relazione binaria: $\rho(a \times a, g)$ con $g \subseteq a \times a$

1 ρ si dice riflessiva se: $(\forall x \in a)(x \rho x)$ → NEGAZIONE: $(\exists x \in a)((x,x) \notin g)$

2 ρ si dice simmetrica se: $(\forall x, y \in a)(x \rho y \rightarrow y \rho x)$

3 ρ si dice antiriflessiva se: $(\forall x \in a)(\neg(x \rho x))$

↳ LA COPPIA $(x,x) \notin g$

ESEMPIO: ↳ CHIARO CHE "NON RIFLESSIVO" PERCHÉ NON È CHE NUMERI QUALCHE COPPIA (x,x) IN g, MA NON CE NE SONO PROPRIO

- Ad esempio, la relazione "<" è antiriflessiva
  ↳ $1,2 < 2$ È SEMPRE FALSO

4. ρ si dice asimmetrica se:

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

ESEMPIO:

- Ad esempio, la relazione "$\leq$" è asimmetrica → SE $x \leq y$ E $y \leq x$ ALLORA $x = y$

5. ρ si dice relazione duale se: $(\forall x, y \in a)(x \rho y \rightarrow y \rho x)$

6. ρ si dice transitiva se:

$(\forall x, y, z \ldots \in a)(x \rho y \wedge y \rho z \rightarrow x \rho z)$

↳ NON SONO PER FORZA TRE ELEMENTI DISTINTI

RELAZIONE DI EQUIVALENZA

Se ρ è riflessiva, simmetrica e transitiva, ρ si dice relazione di equivalenza

RELAZIONE D'ORDINE

Se ρ è asimmetrica e transitiva, ρ si dice relazione d'ordine

RELAZIONE D'ORDINE LARGO

Se p è riflessiva, asimmetrica e transitiva, p si dice relazione d'ordine largo

↳ QUALCOSA È IN RELAZIONE CON SE STESSO → ESEMPIO $2 \leq 2$

RELAZIONE D'ORDINE STRETTO

Se p è antiriflessiva, asimmetrica e transitiva, p si dice relazione d'ordine stretto

↳ NON IN RELAZIONE CON SE STESSO → ESEMPIO $2 < 2$

↓

Se ho p come relazione d'ordine stretto, l'asimmetria diventa inutile

↳ l'implicazione dell'asimmetria è sempre vera perché $xpy \wedge ypx$ è sempre falsa

↓

Se fosse vero che $xpy \wedge ypx$, vale che per la transitività avremmo che xpx → È un assurdo ↯

↓

DATO CHE UNA RELAZIONE D'ORDINE STRETTO DEVE ESSERE ANTIRIFLESSIVA

ESEMPIO:

- Verificare la transitività della relazione.

↳ Per verificarla devo sempre considerare più di due elementi distinti

↓

Se la facessi con due o meno avrei che:

$(\forall x, x, x \in a)(xpx \wedge xpx \rightarrow xpx)$ → SE xpx È VERO, TUTTO È SEMPRE VERO

Correzione esercizi 03/11/2021 (LEZIONE 19)

2. $(\mathbb{Z} \times \mathbb{Z}, +, \circ)$ → È NON COMMUTATIVO? È UN DOMINIO DI INTEGRITÀ?

$(a,b)+(c,d) := (a+c, b+d)$ → l'elemento neutro è la coppia $(0,0)$ in $(\mathbb{Z}\times\mathbb{Z},+)$

$(a,b)\circ(c,d) := (ac, bc)$

↳ Notiamo che $(\forall d \in \mathbb{Z})(\forall a,b \in \mathbb{Z})((a,b)\circ(1,d) = (a,b))$ — C'È 1 CHE PERCHÉ SIAMO IN $\mathbb{Z}$

↳ Ci sono infiniti elementi neutri a destra

↳ Esistono elementi neutri a sinistra?

ESEMPIO: $(1,1)=(c,d)=(0,0)$ ↳ NON È UN ELEMENTO NEUTRO A SINISTRA

Per il teorema che se c'è un elemento neutro a destra e un elemento neutro a sinistra, questi coincidono ed $u=l=d$ è l'unico elemento neutro

↳ Visto che abbiamo infiniti d, Jack dice che non esistono elementi neutri a sinistra

Infatti, $(ac, bc) \overset{DEF}{=} (a,b)\circ(c,d)$ e vogliamo che sia uguale a (c,d). Quindi $(ac,bc)=(c,d)$.

Affinché ciò sia vero, allora avremo che:

PER ESSERE UGUALI, DUE COPPIE DEVONO AVERE LE COORDINATE ORDINATAMENTE UGUALI

$$\left.\begin{aligned} \cdot\, ac &= c \\ \cdot\, bc &= d \end{aligned}\right\}$$

Questo deve valere sempre, quindi deve valere anche quando $c \neq 0$

↳ Quindi c è cancellabile a destra,

quindi $ad = d$ → $\cdot\, a = 1$

- La condizione $bc = d$ varia di c e d → Non c'è un unico elemento neutro a sinistra

- Tutte le coppie $(0,d)$ sono divisori destri dello 0 (x $d \neq 0$)

↳ Infatti, qualunque coppia (a,b) moltiplicata con $(0,d)$ darà l'elemento nullo ↳ $(a,b)\circ(0,d) = (0,0)$

- Ma qualunque elemento (a,b) è divisore sinistro dello 0 se $c=0$

$(\forall (a,b) \in \mathbb{Z}\times\mathbb{Z})((a,b) \neq (0,0) \to$ È divisore sinistro dello $0)$

↳ ESISTE UN ELEMENTO CHE MOLTIPLICATO A DESTRA NI DÀ 0

DIAGONALE DI S E RELAZIONI BINARIE

$\rho = (S \times S, g)$, $g \subseteq S \times S$ $\quad x \bar{\rho} y \Leftrightarrow y \rho x$ → RELAZIONE CONVERSA

$$\boxed{\text{diag } S = \{(x,y) \in S \times S \mid x = y\} \rightarrow \text{Diagonale di } S}$$

TUTTE LE COPPIE CHE HANNO UGUALI LE DUE COORDINATE

ESEMPIO: • In $\mathbb{Z} \times \mathbb{Z}$ sono

$(1,1)$ $(2,2)$ $(3,3)$ $(-2,-2)$

• In $S = \{a,b\}$

$\text{diag } S = \{(a,a),(b,b)\}$

NON SONO DEFINIZIONI MA MODI PER VEDERLO

• ρ è riflessiva se e solo se $\text{diag } S \subseteq g$

$(\forall x \in S)((x,x) \in g)$

• ρ è simmetrica se e solo se $\rho = \bar{\rho}$

$(\forall x,y \in S)((x,y) \in g \rightarrow (y,x) \in g)$

ESEMPIO: • Se $g = \{(a,b)\}$, $\bar{g} = \{(b,a)\}$ → NON VALE LA SIMMETRIA PERCHÉ $g \neq \bar{g}$

Invece, se $g = \{(a,b),(b,a)\}$, $\bar{g} = \{(b,a),(a,b)\}$ → VALE LA SIMMETRIA PERCHÉ $g = \bar{g}$

• ρ è antiriflessiva se e solo se $\text{diag } S \cap g \neq \emptyset$

$(\forall x \in S)((x,x) \notin g)$

ESEMPIO: • Se ho $g = \{(a,b)\}$, l'intersezione con $\text{diag } S$ è sempre uguale a $\emptyset$ perché non ci sono coppie (a,a) o (b,b) in $g \rightarrow (S \times S, g)$ è antiriflessiva

• ρ è asimmetrica se e solo se $g \cap \bar{g} \subseteq \text{diag } S$

$(\forall x,y \in S)(x \rho y \wedge y \rho x \rightarrow x = y)$

ESEMPIO: • Se ho $a \neq b$, e dico che $g = \{(a,b),(b,a)\}$ → NON ASIMMETRICA PERCHÉ NON DICO CHE $a = b \in \emptyset$

$(a,b) \neq (b,a) \neq (a,a) \neq (b,b)$

$(a,a) \neq (b,b) \notin \emptyset$

• Invece, $g = \{(a,b),(a,a),(b,b)\}$ è asimmetrica

$\bar{g} = \{(b,a),(a,a),(b,b)\} \Rightarrow g \cap \bar{g} = \{(a,a),(b,b)\} \subseteq \text{diag } S$

RELAZIONI DI EQUIVALENZA IMPORTANTI

DEFINIZIONE DI RELAZIONE DI EQUIVALENZA

Preso $p = (S \times S, \rho)$ con $\rho \subseteq S \times S$

p è una relazione di equivalenza se p è riflessiva, simmetrica e transitiva.

RELAZIONE UNIVERSALE

p si dice relazione universale se: $\rho = S \times S$

↳ O RELAZIONE TOTALE

↳ È SIMMETRICA PERCHÉ $p = p$ ATTO CHE $\rho = S \times S$

↳ È RIFLESSIVA PERCHÉ $\mathrm{diag}\, S \subseteq \rho$

↳ È TRANSITIVA SE CE' $x p y$ E $y p x$ ALLORA SE ρ CI SONO PERCHÉ $x p z$ $\forall x, y, z$ E $z p x$ CI SONO SEMPRE PERCHÉ CI SONO TUTTI

CONGRUENZA MODULO m

Sia $m \in \mathbb{Z}$, $\equiv_m$ si dice congruenza modulo m e la definisco così: È PROPRIO LA DEFINIZIONE DI CLASSE DI EQUIVALENZA MODULO m

$$\equiv_m = (\mathbb{Z} \times \mathbb{Z}, \rho)$$

$$(\forall a, b \in \mathbb{Z})((a,b) \in \rho \leftrightarrow ((\exists k \in \mathbb{Z})(a - b = km))$$

ESEMPIO:

- $2 \equiv_2 2$? → 2 È CONGRUO A 2 MODULO 2?

↳ Cioè, $2-2$ deve essere un multiplo di 2 → Sì perché lo è se prendo $k=0$

↳ $(2,2) \in \rho \leftrightarrow (\exists k \in \mathbb{Z})(2-2 = k \cdot 2)$

La congruenza modulo m è una relazione di equivalenza?

1) È RIFLESSIVA? Cioè, è vero che $(\forall x \in \mathbb{Z})(x \equiv_m x)$ vale?

↳ Sì perché $(\forall x \in \mathbb{Z})(x - x = 0)$ ma $0 = 0 \cdot m$ → 0 È UN MULTIPLO DI m

2) È SIMMETRICA? Cioè, $(x \equiv_m y \rightarrow y \equiv_m x)$

↳ Sì perché se prendo $x \equiv_m y$ allora $(\exists k \in \mathbb{Z})(x - y = km)$

Ma se vale che $(x - y = k \cdot m)$ allora $(y - x = (-k) \cdot m)$,

quindi abbiamo che vale $y \equiv_m x$

↳ SE k È PROPRIO L'INVERSO DI QUELLO DI $x \equiv_m y$

3) È transitiva? Cioè, $(x \equiv_m y \wedge y \equiv_m z \rightarrow x \equiv_m z)$

↳ Sì perché $(x \equiv_m y \wedge y \equiv_m z)$ significa che:

$(\exists k_1, k_2 \in \mathbb{Z})(x - y = k_1 \cdot m \wedge y - z = k_2 m)$.

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 UGUAGLIANZA

$\equiv_0$ è la relazione di uguaglianza ↳ LA DIFFERENZA DI DUE NUMERI È UN MULTIPLO DI 0 QUANDO SONO LO STESSO NUMERO

↳ $a - b = k \cdot 0 \leftrightarrow a = b$

$a-b=0$? ↳ È LA DIAGONALE

RELAZIONE UNIVERSALE

$\equiv_1$ è la relazione universale

↳ $a - b = k \cdot 1$ ↳ 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")

Prendo una funzione $f: a \rightarrow b$

$\mathrm{KER}\, f = (a \times a, g)$ si dice nucleo di equivalenza di X, e lo posso indicare anche con $\sim_f$ se:

$(\forall x, y \in a)(x \ \mathrm{KER} f \ y \leftrightarrow f(x) = f(y))$ ↳ DUE ELEMENTI SONO IN RELAZIONE KER f SE E SOLO SE HANNO LE IMMAGINI UGUALI

CLASSE DI EQUIVALENZA DI X (MODULO ρ)

- Sia $\rho = (S \times S, g)$ con $g \subseteq S \times S$, preso $X \in S$, $[X]_\rho$ si dice classe di equivalenza di X (modulo ρ) se:

$[X]_\rho := \{ y \in S \mid x \rho y \}$ → SONO TUTTI GLI Y CHE SONO IN RELAZIONE DI EQUIVALENZA CON X

↳ x SI CHIAMA RAPPRESENTANTE DELLA CLASSE

- Per brevità, se ho che $\rho = \equiv_m$, allora $[X]_{\equiv_m}$ lo indico $[X]_m$

↳ $[X]_{\equiv_m} := [X]_m$

ESEMPIO:

- $[2]_2$ → Sono tutti quanti i numeri tali che 2 - quel numero è un multiplo di 2.

$[2]_2 = \{y \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(2-y = 2k)\}$ → ¿ C'È? SI PERCHÉ 2-4 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 → 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

$[5]_2$ → Sono tutti i numeri dispari.

Inoltre, $[5]_2 = [1]_2$ perché anche $[1]_2$ sono tutti i numeri dispari.

INSIEME QUOZIENTE

S/ρ si dice insieme quoziente di S rispetto a ρ se:

$S/\rho := \{[x]_\rho \mid x \in S\}$ → È L'INSIEME DI TUTTE LE CLASSI DI EQUIVALENZA DI MODULO ρ PER UN QUALCHE ELEMENTO DI S

ρ È SEMPRE UNA RELAZIONE DI EQUIVALENZA

COME FORMULA BEN FORMATA È: $S/\rho := \{y \in \mathcal{P}(S) \mid (\exists x \in S)(y = [x]_\rho)\}$

PROPRIETÀ FONDAMENTALI DELLE CLASSI DI EQUIVALENZA

1) Ogni classe di equivalenza è non vuota. Cioè:

$$(\forall y \in S/\rho)(y \neq \emptyset)$$

DIM

TH: Preso un certo $y \in S/\rho$, y sarà una classe di eq. per la definiz. di S/ρ

Quindi ci sarà un x tale che $y = [x]_\rho$

↳ Per la riflessività di ρ, ho sicuramente $x \rho x$.

Quindi $x \in [x]_\rho$, quindi x sta nella classe di equivalenza di x stesso e quindi $[x]_\rho$ non sarà mai vuota.

2) Le classi di equivalenza sono a due a due disgiunte → SE HO DUE CLASSI DI EQUIVALENZA DIVERSE, LA LORO INTERSEZIONE È IL VUOTO

↳ Se due classi di equivalenza condividono anche un solo elemento, allora sono la stessa classe di equivalenza (LA NEGAZIONE)

$$(\forall y, z \in S/\rho)(y \neq z \rightarrow y \cap z = \emptyset)$$

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 $x \in y \cap z$

Scrivo y e z come classi di equivalenza:

↳ $y = [\bar{y}]_\rho$ e $z = [\bar{z}]_\rho$

↳ PER LA DEFINIZIONE DI INSIEME QUOZIENTE

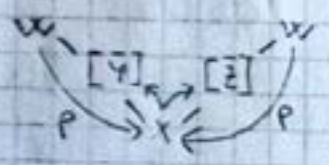
Visto che x sta sia in $[\bar{y}]_\rho$ che in $[\bar{z}]_\rho$, per definizione vale $\bar{y}\,\rho\,x$ e $\bar{z}\,\rho\,x$

Per la simmetria di ρ vale anche: $x\,\rho\,\bar{y}$ e $x\,\rho\,\bar{z}$.
Per la transitività di ρ, se ho $\bar{y}\,\rho\,x$ e $x\,\rho\,\bar{z}$ allora vale $\bar{y}\,\rho\,\bar{z}$. Ma vale anche $\bar{z}\,\rho\,\bar{y}$ da $\bar{z}\,\rho\,x$ e $x\,\rho\,\bar{y}$

Di conseguenza, per definizione di classe di equivalenza:
- $\bar{y}\,\rho\,\bar{z} \rightarrow \bar{z} \in [\bar{y}]_\rho$
- $\bar{z}\,\rho\,\bar{y} \rightarrow \bar{y} \in [\bar{z}]_\rho$

Se prendo un certo elemento $w \in [\bar{y}]_\rho$:
$\underline{w \in [\bar{y}]_\rho} \leftrightarrow \bar{y}\,\rho\,w \leftrightarrow \bar{z}\,\rho\,w \leftrightarrow \underline{w \in [\bar{z}]_\rho}$

Quindi $[\bar{y}]_\rho = [\bar{z}]_\rho$ perché ho appena dimostrato che ogni elemento di $[\bar{y}]_\rho$ appartiene a $[\bar{z}]_\rho$ e viceversa



3) L'unione dell'insieme quoziente è S
↳ $\bigcup S/\rho = S$ ↳ STO PRENDENDO TUTTI GLI ELEMENTI DELLE CLASSI DI EQUIVALENZA

<u>DIM</u>

($\subseteq$) Se $y \in \bigcup S/\rho$ allora $(\exists [x]_\rho)(y \in [x]_\rho)$ → ESISTE UN ELEMENTO DEGLI ELEMENTI TALE CHE GLI APPARTIENE
allora, visto che $[x]_\rho \in \mathcal{P}(S)$, $y \in S$

($\supseteq$) Se prendo $x \in S$, allora $[x]_\rho \in S/\rho$ ↳ x APPARTIENE ALLA PROPRIA CLASSE DI EQUIVALENZA PER LA PROPRIETÀ 1
Quindi $x \in \bigcup S/\rho$

Quindi i due insiemi sono uguali perché gli elementi di uno sono gli elementi dell'altro.

E' EQUIVALENTE DIRE CHE:

$xpy \leftrightarrow ypx \leftrightarrow x \in [y]_p \leftrightarrow y \in [x]_p \leftrightarrow [x]_p = [y]_p \leftrightarrow$
$\leftrightarrow [x]_p \cap [y]_p \neq \emptyset$

Correzione esercizi 10/11/2021 (LEZIONE 20)

3. 1) $f: m \in \mathbb{Z} \longmapsto m+1 \in \mathbb{Z}$ $(\mathbb{Z} \times \mathbb{Z}, g)$

Notiamo che f è iniettiva, quindi:

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

Quindi KER_f è proprio l'uguaglianza, coincide con la relazione "="

ESEMPIO: Se ho $[0]_{KER_f}$, questi sono tutti quanti gli elementi di $\mathbb{Z}$ che hanno per immagine l'immagine di 0

↳ $[0]_{KER_f} = \{0\}$ → CI SONO TANTI SINGLETON QUANTI GLI ELEMENTI DI $\mathbb{Z}$

$\mathbb{Z}/_{KER_f} = \{\{m\} \mid m \in \mathbb{Z}\}$ → NOTAZIONE ALTERNATIVA PER DIRE CHE SONO I SINGLETON DEGLI ELEMENTI DI $\mathbb{Z}$. DOVREI SCRIVERE:

$\mathbb{Z}/_{KER_f} = \{Y \in P(\mathbb{Z}) \mid Y = \{m\}\}$

↳ CON LA RELAZIONE DI UGUAGLIANZA SALI DI UN LIVELLO, METTI LE PARENTESI OPPURE AL ELEMENTO

$\mathbb{Z}/_{KER_f} \cap \mathbb{Z} = \emptyset$ perché $\mathbb{Z}$ ha i numeri, non i singleton dei numeri

$\mathbb{Z}/_{KER_f}$ e $\mathbb{Z}$ sono legati da una relazione isomorfa

↳ ESEMPIO: $\{m\} + \{m\} = \{m+m\}$ ecc...

7. $f: n \in \mathbb{Z} \longmapsto (-1)^n \in \mathbb{Z}$ $(\mathbb{Z} \times \mathbb{Z}, g)$

Trovare KER f. $x \, KER f \, y \Leftrightarrow f(x) = f(y)$

↳ Per vedere come è fatto KER f, devo vedere come sono le immagini $f(x)$ e $f(y)$

Quando $(-1)^x = (-1)^y$? Quando x e y sono entrambi pari o entrambi dispari

$$(-1)^x = (-1)^y \Leftrightarrow \begin{cases} x \text{ e } y \text{ sono pari} \\ x \text{ e } y \text{ sono dispari} \end{cases} \Leftrightarrow x \equiv_2 y$$

STESSO GRAFICO

DUE ELEMENTI SONO IN RELAZIONE KER f SE E SOLO SE SONO IN RELAZIONE $\equiv_2$

Quindi KER f coincide con la relazione $\equiv_2$

↳ Stesso dominio, codominio e grafico

Chi è $\mathbb{Z}/_{KER f}$? L'insieme delle classi di equivalenza modulo KER

$\mathbb{Z}/_{KER f} = \{[0]_{KER f}, [1]_{KER f}\}$ → Perché una classe di equivalenza prende tutte le relazioni "essere pari" e l'altra "essere dispari"

↓

Non ci sono elementi di $\mathbb{Z}$ lasciati fuori, tutti rientrano in una classe di equivalenza

OMOMORFISMO TRA GRUPPI

Prendiamo $f: g_1 \to g_2$ con g_1 e g_2 gruppi e f come omomorfismo tra gruppi.

Sappiamo per definizione che $X \, KER f \, Y \leftrightarrow f(x) = f(y)$

Essendo g_1 e g_2 gruppi, tutti i loro elementi sono invertibili quindi avremo che in g_2:

COME SE FOSSE $f(x)(f(x))^{-1} = 1_{g_2}$

$$f(x) = f(y) \leftrightarrow f(x) \cdot (f(y))^{-1} = 1_{g_2}$$ DEFINIZIONE DI INVERSA

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 KERf PER GLI OMOMORFISMI DI GRUPPI

Quindi abbiamo che $\boxed{X \, KER f \, Y \leftrightarrow f(x \cdot y^{-1}) = 1_{g_2}}$

Se f è iniettiva (è un monomorfismo) allora avremo che se l'immagine è un'identità allora anche l'antiimmagine lo è: $f(x \cdot y^{-1}) = 1_{g_2} \leftrightarrow x \cdot y^{-1} = 1_{g_1}$

QUINDI $x = y$

ESEMPIO:

- Se ho $f: x \in G \mapsto x^{-1} \in G$ con G abeliano, f è un omomorfismo
  - Prendo $xy \in G$, la sua inversa $(xy)^{-1} = y^{-1} \cdot x^{-1}$, ma dato che G è abeliano allora $y^{-1} \cdot x^{-1} = x^{-1} \cdot y^{-1}$ → f è un omomorfismo

MOLTIPLICATO x y DÀ L'IDENTITÀ

$$x \, KER f \, y \leftrightarrow f(x) = f(y) \leftrightarrow \underbrace{x^{-1} = y^{-1}}_{\text{L'INVERSO È UNICO}} \leftrightarrow x = y$$

Se KERf è l'intersezione (nei gruppi) allora è la funzione identità

TEOREMA FONDAMENTALE DI OMOMORFISMO PER INSIEMI (PREMESSE)

$$\begin{tikzcd} a \arrow[r, "f"] \arrow[d, "\pi"'] & b \\ a/_{\sim f} \arrow[r, "\tilde{f}"] & \mathrm{Im}\, f \arrow[u, "\iota"'] \end{tikzcd}$$

- Presi due insiemi a e b, considero una funzione $f: a \to b$
- Esisterà una certa immagine di f che è un sottoinsieme di b
  ↳ $\mathrm{Im}\, f \subseteq b$

  Esisterà quindi la funzione immersione:
  $\iota: x \in \mathrm{Im}\, f \to x \in b$ → funzione iniettiva → È PRATICAMENTE L'IDENTITÀ MA NON SURETTIVA
  ↓ VOTA
- Avremo anche un insieme quoziente di a su KER f
  ↳ Posso prendere una funzione π che associa ad ogni elemento $x \in a$, la classe di equivalenza di x.

  $\pi: x \in a \longmapsto [x]_{\sim f} \in a/_{\sim f}$ → Questa funzione si chiama proiezione canonica di a su a/~f
  ↳ Questa è una funzione ovviamente suriettiva → OGNI ELEMENTO X HA UNA CLASSE DI EQUIVALENZA
  ↳ TUTTE LE CLASSI DI EQUIVALENZA SONO PRESE IN a/~f
- Vogliamo chiudere il diagramma in maniera commutativa. Prendo una funzione $\tilde{f}$ tale che:

  $\tilde{f}: [x]_{\sim f} \in a/_{\sim f} \longmapsto f(x) \in \mathrm{Im}\, f$

  Ma $\tilde{f}$ è ben posta? Potrebbe accadere che, presi 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
  ↳ Controlliamo se $\tilde{f}$ è ben posta

$\tilde{f}$ è ben posta?

Prendo $(x, y \in a)([x]_{\sim f} = [y]_{\sim f})$. Dobbiamo dimostrare che a elementi uguali associa immagini uguali.

$$\tilde{f}([x]_{\sim f}) = f(x) \quad \text{per definizione}$$

Dalle proprietà fondamentali delle classi di equivalenza sappiamo che $[x]_{\sim f} = [y]_{\sim f}$ significa dire che $x \sim_f y$.
Ma la relazione $\sim_f$ è quella di "avere la stessa immagine". Di conseguenza:

↳ DEFINIZIONE DI KER f

$$\tilde{f}([x]_{\sim f}) = f(x) = f(y) = \tilde{f}([y]_{\sim f})$$

Abbiamo fatto vedere che per ogni elemento di $a/_{\sim f}$, ce n'è uno solo nel grafico che ha come prima coordinata l'elemento di $a/_{\sim f}$ e cioè quando come seconda coordinata abbiamo $f(x)$

↳ $f(x)$ non cambia al variare del rappresentante della classe → $f(x)$ non dipende dal rappresentante

Quindi $\tilde{f}$ è ben posta

TEOREMA FONDAMENTALE DI OMOMORFISMO PER INSIEMI

$$\begin{tikzcd} a \arrow[r, "f"] \arrow[d, "\pi"'] & b \\ a/_{\sim f} \arrow[r, "\tilde{f}"] & \mathrm{Im} f \arrow[u, "i"'] \end{tikzcd}$$

Vale che:

1) $\tilde{f}$ è biettiva
2) $f = i \circ \tilde{f} \circ \pi$

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. → $x \sim_f y \Leftrightarrow f(x)$

↳ Hanno tutti la stessa immagine, cioè $f(x)$ → L'IMMAGINE DI x

DIM

1) Definisco α.

$$\alpha : f(x) \in \operatorname{Im} f \longmapsto [x]_{\sim_f} \in A/\sim_f$$

$\overset{\leftarrow}{f}(\{f(x)\})$

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 sola cosa

- α è suriettiva?

  Sia $\bar{y} \in A/\sim_f$, cioè $(\exists y \in A)(\bar{y} = [y]_{\sim_f})$.

  Ma allora, $\alpha(f(y)) = [y]_{\sim_f} = \bar{y}$ quindi α è suriettiva

  ↳ Cioè, presa una classe di equivalenza 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'inversa

Definisco $\tilde{f} := \alpha^{-1}$ → Quindi $\tilde{f}$ è biettiva perché ha l'inversa.

NE' PROPRIO LA FUNZIONE CHE VOLEVAMO PER COME L'ABBIAMO DEFINITA

↳ Il punto 1 è verificato

2) Per vedere che $f = \iota \circ \tilde{f} \circ \pi$ dobbiamo vedere che le due funzioni abbiano 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 $(i \circ \tilde{f} \circ \pi)(x)$?
  ↳ $(i \circ \tilde{f} \circ \pi)(x) = i(\tilde{f}(\pi(x))) = i(\tilde{f}([x]_{\sim_f})) = i(f(x)) = f(x)$

Dato che queste due funzioni hanno lo stesso dominio, lo stesso codominio e lo stesso grafico, allora $f = i \circ \tilde{f} \circ \pi$ → 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 $f: a \to b$, con a e b due insiemi,
esiste un insieme c tale che:

$\exists g$ iniettiva da $c \to b$
$\exists h$ suriettiva da $a \to c$

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 $f: n \in \mathbb{Z} \longmapsto (-1)^n \in \mathbb{Z}$ come composizione di una funzione iniettiva e una suriettiva?

Trovo l'insieme quoziente, in modo tale da scrivere π (la proiezione canonica), scrivo 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.

$$\mathbb{Z}/_{\sim f} = \{[0]_2, [1]_2\}$$

$$\pi: n \in \mathbb{Z} \longmapsto \begin{matrix}\text{PARI}\\ \text{DISPARI}\end{matrix} \in \mathbb{Z}/_{\sim f}$$

MANDA I PARI NEI PARI E I DISPARI NEI DISPARI

$$i: n \in \operatorname{Im} f \longmapsto n \in \mathbb{Z}$$

$$\tilde{f}: \begin{matrix}[0]_{\sim f} \longmapsto f(0) = 1\\ [1]_{\sim f} \longmapsto f(1) = -1\end{matrix} \in \underbrace{\{-1, 1\}}_{\operatorname{Im} f}$$

$$i \circ \tilde{f}: \begin{matrix}[0]_{\sim f}\\ [1]_{\sim f}\end{matrix} \in \mathbb{Z}/_{\sim f} \longmapsto \begin{matrix}1\\ -1\end{matrix} \in \mathbb{Z}$$

$i \circ \tilde{f}$ è iniettiva perché i due elementi di $\mathbb{Z}/_{\sim f}$ li manda in due immagini separate

π è suriettiva perché manda tutti gli $\mathbb{Z}$ o nei pari o nei dispari, in $\mathbb{Z}/_{\sim f}$ non c'è altro oltre i pari o i dispari

$$f = (i \circ \tilde{f}) \circ \pi$$

$f: n \in \mathbb{Z} \mapsto n+1 \in \mathbb{Z}$

Notiamo che f è già di per se iniettiva, quindi basta fare la composizione con l'identità (che è suriettiva)
↳ È BANALE

- $f: n \in \mathbb{Z} \mapsto (-1)^n \in \mathbb{Z}$

Prendo la funzione $\tilde{g}: [n]_{\sim f} \in {}^{a}/_{\sim f} \mapsto n+1 \in \mathbb{Z}$

La funzione $\tilde{g}$ non è ben posta, infatti:

$\tilde{g}([0]_{\sim f}) = 1$
$\tilde{g}([2]_{\sim f}) = 3$

Ma $[0]_{\sim f}$ e $[2]_{\sim f}$ sono lo stesso elemento nell'insieme quoziente, quindi nel grafico della funzione ci sono la coppia $([0]_{\sim f}, 1)$ e $([0]_{\sim f}, 3)$. Di conseguenza $\tilde{g}$ non è una funzione perché a una stessa x sono associate due immagini diverse
↳ Non è ben posta.

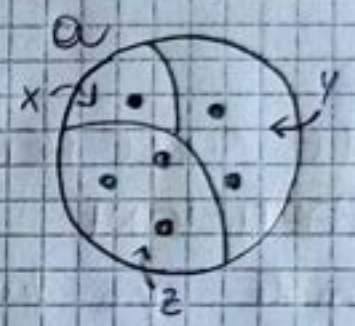
PARTIZIONI DI a

Sia a un insieme. Un insieme $\mathcal{P}$ sottoinsieme delle parti di a ($\mathcal{P} \subseteq \mathcal{P}(a)$) si dice partizione di a se:

↳ CONCETTO SIMILE A QUELLO DI CLASSI DI EQUIVALENZA

1) $(\forall x \in \mathcal{P})(x \neq \emptyset)$
2) $(\forall x, y \in \mathcal{P})(x \neq y \rightarrow x \cap y = \emptyset)$
3) $\bigcup \mathcal{P} = a$

ESEMPIO:



$\mathcal{P} = \{x, y, z\}$

↳ È una partizione

- Se prendevo x, y o z studio allora $\mathcal{P}$ non era una partizione
- Se c'era anche un solo elemento in comune tra x, y o z non c'era la partizione
- Se lasciavo anche un solo elemento fuori, $\mathcal{P}$ non era più una partizione

PARTIZIONI BANALI DI a

Sono partizioni:

- $\mathcal{P} = \{a\}$
- $\mathcal{P} = \{\{x\} \mid x \in a\}$ → LA PARTIZIONE DEI SINGOLI ELEMENTI

RELAZIONE TRA PARTIZIONI E RELAZIONI DI EQUIVALENZA

L'insieme quoziente, rispetto a una relazione di equivalenza, è una partizione → C'è un'applicazione biettiva tra i due concetti

Questa applicazione biettiva ci viene data dal teorema fondamentale sulle relazioni di equivalenza e le partizioni

↳ INFORMAZIONI PRELIMINARI

- Definisco $EQ(a)$ come l'insieme di tutte le relazioni di equivalenza su a

PER L'ASSIOMA DI SEPARAZIONE

- Definisco $PART(a)$ come l'insieme di tutte le partizioni di a

TEOREMA FONDAMENTALE SULLE RELAZIONI DI EQUIVALENZA E LE PARTIZIONI

Per ogni insieme a, esiste una funzione biettiva f che ad una certa relazione di equivalenza $\sim \in EQ(a)$ associa $a/\sim \in PART(a)$

↳ $f: \sim \in EQ(a) \longmapsto a/\sim \in PART(a)$ → OGNI PARTITIZIONE POSSO SCRIVERLA COME RELAZIONE DI EQUIVALENZA

↓

STESSO CONCETTO VISTO SOTTOFORMA DI ELEMENTI IN RELAZIONE E DI SOTTOINSIEMI DI a

<u>DIM</u>

- f è iniettiva? → SE LE IMMAGINI SONO UGUALI ALLORA ANCHE GLI ELEMENTI DA CUI VENGONO SONO UGUALI

Prendo: $\sim_1, \sim_2 \in EQ(a)$

Suppongo che $f(\sim_1) = f(\sim_2)$, cioè che $a/\sim_1 = a/\sim_2$

Quindi per definizione, $a/\sim_1 = a/\sim_2$ significa che:

$$\{[X]_{\sim_1} \mid X \in a\} = \{[X]_{\sim_2} \mid X \in a\}$$

→ DOBBIAMO FAR VEDERE CHE OGNI COPPIA DI ELEMENTI IN RELAZIONE $\sim_1$, SONO ANCHE IN RELAZIONE $\sim_2$

↓

$$\forall X, Y \in a,\ X \sim_1 Y \longleftrightarrow [X]_{\sim_1} = [Y]_{\sim_1} \longleftrightarrow (\exists Z \in a)([X]_{\sim_1} = [Z]_{\sim_2})$$

$$\text{e } (\exists W \in a)([Y]_{\sim_1} = [W]_{\sim_2}) \longleftrightarrow W \sim_2 Z \longleftrightarrow X \sim_2 Y$$

↓

X E Y SONO NELLA STESSA CLASSE DI EQUIVALENZA QUINDI ANCHE W E Z SONO IN RELAZIONE $\sim_2$

Infatti, $x, y \in [z]_{\sim_2}$ e quindi le classi sono equivalenti

Quindi, visto che assurdo $f(\sim_1) = f(\sim_2)$ abbiamo che $x \sim_2 y$, f è iniettiva.

- f è suriettiva? → DOBBIAMO FAR VEDERE CHE ESISTE UNA RELAZIONE DI EQUIVALENZA CHE ABBIA COME IMMAGINE UNA PARTIZIONE

Sia $\mathcal{P} \in PART(a)$

Definisco:

$$(\forall x, y \in a)(x \sim y :\leftrightarrow \underbrace{((\exists z \in \mathcal{P})(x \in z \wedge y \in z))}_{\text{X E Y APPARTENGONO AD UNO STESSO ELEMENTO DELLA PARTIZIONE}}$$

$\sim$ è una relazione di equivalenza?

1) È riflessiva? Sì, perché x e x appartengono a uno stesso elemento della partizione → Ce ne sarà sempre uno che li contiene

↳ $(\forall x \in a)((\exists z \in \mathcal{P})(x \in z))$ perché $\bigcup \mathcal{P} = a$

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:

$(\exists W_1, W_2 \in \mathcal{P})(x \in W_1 \wedge y \in W_1 \wedge y \in W_2 \wedge z \in W_2)$

ma ciò significa che $W_1 \cap W_2 \neq \emptyset$ (c'è y)

↳ Dalla definizione di partizione, se l'intersezione tra i due non è vuota, $W_1 = W_2$ ← PROPRIETÀ 2 DELLE PARTIZIONI

↳ Quindi $x \sim z$, quindi vale la transitività.

Quindi è vero che $f(\sim) = \mathcal{P}$?

Sì, $f(\sim)$ è proprio $\mathcal{P}$ → MOTIVAZIONE PROSSIMA PAGINA

Infatti, essendo $f(\sim)$ l'insieme quoziente, è l'insieme di tutti gli elementi che stanno nella parte della partizione (f)

↳ Ogni singolo elemento di (f) sta in $f(\sim)$ e ogni singola classe di equivalenza è una parte della partizione → $f(\sim)$ e (f) coincidono

↳ PER COME È STATA DEFINITA

PERCHÈ 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, preso un certo insieme, posso definire la relazione di equivalenza semplicemente facendo delle partizioni a caso dell'insieme

↳ Ora posso, ad esempio, elencare tutte le relazioni di equivalenza di un insieme con tre elementi

↳ MI BASTA FARE DELLE PARTIZIONI DELL'INSIEME CON TRE ELEMENTI

Correzione esercizi 12/11/2021 (LEZIONE 21)

1. $f: m \in \mathbb{Z} \longmapsto m^2 \in \mathbb{Z}$

Scrivere la funzione f come composizione di una funzione iniettiva e una suriettiva

↳ Usiamo il teorema fondamentale per l'omomorfismo tra gli insiemi

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "f"] \arrow[d, "\pi"'] & \mathbb{Z} \\ \mathbb{Z}/\sim_f \arrow[r, "\tilde{f}"'] & \mathrm{Im} f \arrow[u, "i"'] \end{tikzcd}$$

1. Bisogna trovare il KER f per trovare la funzione π

↓

UN MODO PER SCRIVERE RELAZIONE KER

$\mathrm{KER} f = (\mathbb{Z} \times \mathbb{Z}, \sim_f)$ dove

$\sim_f = \{m, n \in \mathbb{Z} \times \mathbb{Z} \mid f(m) = f(n)\}$ → TUTTE LE COPPIE DI ELEMENTI CHE HANNO LA STESSA IMMAGINE

UN ALTRO MODO DI SCRIVERE KER f

↕

$m \ \mathrm{KER} f \ n \iff f(m) = f(n) \iff m^2 = n^2$

Ma due numeri elevati al quadrato sono uguali se e solo se sono uguali oppure uno è l'opposto dell'altro → PROPRIETÀ ARITMETICA IN $\mathbb{Z}$ DOVE $\sqrt{m^2} = \pm m$

↳ $m^2 = n^2 \iff m = n \vee m = -n$ ↳ DIAMO PER SCONTATE 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 → $m \ \mathrm{KER} f \ n \iff m = n \vee m = -n$

↳ $[m]_{\mathrm{KER} f} = \{m, -m\}$ → $f(m) = m^2$, $f(-m) = m^2$

Quindi, $\mathbb{Z}/\sim_f$, che è per definizione l'insieme di tutte le classi di equivalenza di modulo $\sim_f$, è proprio l'insieme delle coppie $\{m, -m\}$ $\forall m \in \mathbb{Z}$

↳ ANCHE $\{0, -0\}$ CHE IN REALTÀ È $\{0\}$

Quindi, π (SURIETTIVA): $m \in \mathbb{Z} \longmapsto [m]_{\sim_f} \in \mathbb{Z}/\sim_f$

cioè, $\pi: m \in \mathbb{Z} \longmapsto \{m, -m\} \in \mathbb{Z}/\sim_f$ → PER ESSERE PIÙ ESPLICITA

$\tilde{f}$ è quella relazione che a qualunque classe di equivalenza associa f di un qualunque rappresentante della classe

↳ $\tilde{f}: [m]_{\sim f} \in \mathbb{Z}/_{\sim f} \longmapsto f(m) \in \operatorname{Im} f$

Ma $\operatorname{Im} f$ è proprio $\mathbb{N}$ dato che m^2 è un numero sempre positivo

↳ $\tilde{f}: \{m, -m\} \in \mathbb{Z}/_{\sim f} \longmapsto m^2 \in \mathbb{N}$

$$\underbrace{\overset{\text{IMMERSIONE}}{i} \circ \tilde{f}}_{\text{INIETTIVA}}: \{m, -m\} \in \mathbb{Z}/_{\sim f} \longmapsto m^2 \in \mathbb{Z}$$

Ho trovato le due funzioni tali che $f = (i \circ \tilde{f}) \circ \pi$

8. $a = \{0, 1, 2, 3, 4, 5, 6, 7\}$ $\quad \rho = (a \times a, \varrho)$ ↗ RELAZIONE DI EQUIVALENZA

Vale: $0 \rho 6$ $\quad 0 \rho 7$ $\quad (1,4) \in \varrho$ $\quad \{3, 4, 5, 7\} \subseteq [2]_\rho$

Visto che abbiamo che $\{3,4,5,7\} \subseteq [2]_\rho$, allora in relazione con 2 sono:

- 2 perché ρ è riflessiva essendo una relazione di equivalenza
- 3, 4, 5, 7 perché $\{3, 4, 5, 7\} \subseteq [2]_\rho$
- 0 perché, per la transitività 0 è in relazione con 7 e 7 è in relazione con 2
- 6 per simmetria e transitività tra $0 \rho 6$ e $0 \rho 7$
- 1 perché $(1,4) \in \varrho$ (cioè 1 è in relazione con 4) e si ha la transitività

Quindi $[2]_\rho = a \rightsquigarrow a/_\rho = \{a\}$

↳ C'è una sola classe di equivalenza, quindi la relazione di equivalenza è univocamente determinata

Quindi ϱ è quella dove tutti sono in relazione con tutti

↳ la relazione universale $\rightarrow \varrho = a \times a \rightarrow$ RELAZIONE BANALE

RELAZIONE D'ORDINE

Una relazione d'ordine è una relazione asimmetrica e transitiva. Inoltre, se vale 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:

$$\left[OL(a) = \left\{ \underbrace{\rho \in \mathcal{P}(\mathcal{P}(\mathcal{P}(a \times a)))}_{\text{PERCHE'?}} \;\middle|\; \underbrace{RIFL}_{(x \in a \Rightarrow (x,x) \in \rho)} \wedge ASIMM \wedge TRANS \wedge \dots \right\} \right]$$

Verifichiamo a chi appartiene ρ.

↳ $\rho = (a \times a, \emptyset)$

Per definizione della coppia ordinata, $\rho = \{\{a \times a\}, \{a \times a, \emptyset\}\}$

$\{a \times a\}$ di chi è sottoinsieme?

↳ $a \times a \subseteq a \times a$ (E' OVVIO)

Quindi il singleton di $a \times a$ è un sottoinsieme delle parti di $a \times a$

↳ $\{a \times a\} \subseteq \mathcal{P}(a \times a)$

Visto che $\{a \times a\} \subseteq \mathcal{P}(a \times a)$ e $\emptyset \subseteq a \times a$, allora $\{a \times a, \emptyset\} \subseteq \mathcal{P}(a \times a)$

Noi vogliamo scoprire ρ di chi è elemento. Essendo $\{a \times a\}$ e $\{a \times a, \emptyset\}$ delle parti di $a \times a$, allora questi saranno elementi delle parti delle parti di $a \times a$

↳ $\{a \times a\} \in \mathcal{P}(\mathcal{P}(a \times a))$ e $\{a \times a, \emptyset\} \in \mathcal{P}(\mathcal{P}(a \times a))$

Per avere un altro livello di parentesi e ottenere $\{\{a \times a\}, \{a \times a, g\}\}$ devo andare nella $\mathcal{P}(\mathcal{P}(\mathcal{P}(a \times a)))$

↳ Quindi, $\{\{a \times a\}, \{a \times a, g\}\} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(a \times a)))$

Per questo: $p = (a \times a, g) = \{\{a \times a\}, \{a \times a, g\}\} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(a \times a)))$

INSIEME DELLE RELAZIONI DI ORDINE STRETTO

Sia $a \neq \emptyset$, definisco l'insieme di tutte le relazioni di ordine stretto:

$$OS(a) = \{p \in \mathcal{P}(\mathcal{P}(\mathcal{P}(a \times a))) \mid \text{ANTIRIFL} \wedge \text{ASIMM} \wedge \text{TRANS}\}$$

RELAZIONE TRA OL(a) E OS(a)

È possibile definire un'applicazione biettiva tra i due insiemi → CIÒ CI PERMETTE DI STUDIARE UN SOLO TIPO DI RELAZIONE E TROVARE LE PROPRIETÀ ANCHE NELL'ALTRO

Sia $p \in OL(a)$, definisco:

RO GREVE $p^\wedge : (\forall x, y \in a)(x \, p^\wedge \, y :\longleftrightarrow (x p y \wedge x \neq y))$

Sia $p \in OS(a)$, definisco:

$p^\vee : (\forall x, y \in a)(x \, p^\vee \, y :\longleftrightarrow (x p y \vee x = y))$

Si può dimostrare che l'applicazione f:

$f: p \in OL(a) \longmapsto p^\wedge \in OS(a)$ è biettiva.

La sua inversa sarà:

$f^{-1}: p \in OS(a) \longmapsto p^\vee \in OL(a)$

LA DIMOSTRAZIONE SI FA FACENDO VEDERE CHE SE p È DI ORDINE LARGO, ALLORA $p^\wedge$ È DI ORDINE STRETTO, CIOÈ VALE LA ANTIRIFLESSIVITÀ E LA TRANSITIVITÀ, VICEVERSA CON f^{-1}

ESEMPI DI RELAZIONI D'ORDINE:

- $\leq$ in $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{N}$...
- $\subseteq$ in $\mathcal{P}(S)$ con S insieme
- La divisibilità in $\mathbb{N}$

↳ $n \mid m \longleftrightarrow (\exists k \in \mathbb{N})(m = nk)$ → n DIVIDE m SE ESISTE UN $k \in \mathbb{N}$ TALE CHE $n \cdot k$ E' PROPRIO m

PERCHE' LA DIVISIBILITA' E' UNA RELAZIONE D'ORDINE?

↳ 1) n divide se stesso

2) Se $n \mid m$ e $p \mid n$ allora: $p \mid m$:

↳ $m = nk \wedge n = hp \longrightarrow m = hkp$ → TRANSITIVITA'

3) Se $m \mid n$ e $n \mid m$ allora $m = n$:

↳ $m = nk \wedge n = mh \longrightarrow m = mhk$ → ASIMMETRIA

VALE L'ASIMMETRIA

a) Se $m = 0$ allora anche $n = 0$ perché $n = mh$

b) Se $m \neq 0$, visto che in $\mathbb{N}$ tutti gli elementi sono cancellabili, m è cancellabile.
Di conseguenza $m = mhk \rightarrow hk = 1$.
In $\mathbb{N}$, l'unico elemento invertibile è solo 1.
Quindi $h = k = 1$, quindi $m = n$

Quindi la divisibilità in $\mathbb{N}$ è una relazione di ordine largo

Se invece definisco la divisibilità in $\mathbb{Z}$, cioè:

↳ $n \mid m \longleftrightarrow (\exists k \in \mathbb{Z})(m = nk)$, questa non è una relazione d'ordine, infatti non è asimmetrica

↳ Quando arrivo al passaggio in cui $h \cdot k = 1$, questo può essere sia se $h = k = -1$ che quando $h = k = 1$

↳ Infatti, in $\mathbb{Z}$, $2 \mid -2$ e $-2 \mid 2$ ma $-2 \neq 2$

UNO DI ESSI È L'INVERSO DELL'ALTRO

INSIEMI ORDINATI

Sia $S \neq \emptyset$ e $\rho = (S \times S, \varrho)$. Sia ρ una relazione d'ordine su S.

La coppia (S, ρ) si dice insieme ordinato

RELAZIONE D'ORDINE

↳ SI DIVENTA ORDINATO QUANDO ORDINO GLI ELEMENTI CON UNA RELAZIONE D'ORDINE

RELAZIONE D'ORDINE INDOTTO

Se $\underbrace{t \in \mathcal{P}(S) \setminus \{\emptyset\}}_{t \subseteq S}$, la relazione

$\rho_t = (t \times t, \varrho \cap (t \times t))$ si dice relazione d'ordine indotto da (S, ρ) su t

ESEMPIO:
PRENDO L'ORDINE DI $\mathbb{N}$ E LO RITROVO ANCHE IN UN SUO SOTTOINSIEME

SOTTOINSIEME ORDINATO

(t, ρ_t) lo chiamo sottoinsieme ordinato di (S, ρ)

ESEMPIO:
Se ho $(\mathbb{Z}, \leq)$, dovrei indicare il sottoinsieme ordinato su $\mathbb{N}$ con:

$(\mathbb{N}, \leq_{\mathbb{N}})$ → Per brevità scriverò: $(\mathbb{N}, \leq)$

È LA STESSA DI PRIMA MA RISTRETTA AD $\mathbb{N}$

CONFRONTABILI IN (S, ρ)

Due elementi $x, y \in S$ si dicono confrontabili se vale $x \rho y \vee y \rho x$, preso (S, ρ) insieme ordinato

ESEMPIO:

- In $(\mathbb{N}, \leq)$ tutti gli elementi sono sempre confrontabili
- In $(\mathbb{N}, |)$ non tutti gli elementi sono confrontabili perché non vale ne che $2|3$ ne che $3|2$

ORDINE TOTALE

Se tutti gli elementi di S sono confrontabili rispetto a p, p si dice ordine totale su S

MINIMO → SI HA SOLO SE $p \in O(S)$

Un elemento $m \in S$ si dice minimo di (S, p) ↓ lo indico con $min(t)$

se: $(\forall x \in S)(m\,p\,x)$ → m E X SONO NELLO STESSO INSIEME

↳ IL MINIMO STA PRIMA

MASSIMO → SI HA SOLO SE $p \in O(S)$

Un elemento $M \in S$ si dice massimo di (S, p) ↓ lo indico con $max(t)$

se: $(\forall x \in S)(x\,p\,m)$ → m E X SONO NELLO STESSO INSIEME

↳ IL MASSIMO STA DOPO

INSIEME BEN ORDINATO

(S, p) si dice ben ordinato se ogni parte diversa dal $\emptyset$ ha minimo → IL MINIMO DELLA PARTE RISPETTO LA RELAZIONE INDOTTA → IL MINIMO DI $\{x\}$ È X, CHE È ANCHE IL MASSIMO

↳ p DEVE ESSERE PER FORZA DI ORDINE LARGO, CIOÈ PER $x \in S$ VALE $x\,p\,x$

UNICITÀ DEL MINIMO (O DEL MASSIMO)

Se esiste il minimo, questo è unico

DIM

Siano 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 asimmetria $m_1 = m_2$. Stesso ragionamento per il massimo

ESEMPI:

- $(\mathbb{N}, \leq)$ è ben ordinato perché ogni parte non vuota ha il minimo → Anche tutto $\mathbb{N}$ ce l'ha

- $(\mathbb{Z}, \leq)$ non è ben ordinato perché l'insieme "tutto $\mathbb{Z}$" non ha minimo

- Se ho l'insieme $a = \mathbb{Z} \cup \{-\infty\}$, dove $-\infty$ è un elemento che è sempre più piccolo di tutti gli interi, e $\rho = (a \times a, g)$ allora:

$(\forall m, n \in \mathbb{Z})(m \rho n \leftrightarrow m \leq n)$ e ho anche che $(\forall m \in \mathbb{Z})(-\infty \rho m)$ e, per la riflessività, anche $-\infty \rho -\infty$.

Anche se l'insieme a ha minimo, c'è la parte di a (cioè $\mathbb{Z}$) che non ha minimo, di conseguenza $(\mathbb{Z} \cup \{-\infty\}, \rho)$ non è ben ordinato

- L'insieme $a = \mathbb{N} \cup \{-\infty\}$ con $\rho = (a \times a, g)$ e con g definita così:
  - $(\forall m, n \in \mathbb{N})(m \rho n \leftrightarrow m \leq n)$
  - $(\forall m \in \mathbb{N})(-\infty \rho m)$
  - $-\infty \rho -\infty$

È ben ordinato perché ogni parte di a ha minimo $\rightarrow$ $\mathbb{N} \cup \{-\infty\}$ È UN INSIEME IMPORTANTE PER I POLINOMI

INSIEME TOTALMENTE ORDINATO

Se (S, ρ) è ben ordinato (QUINDI HA SEMPRE IL MINIMO) allora (S, ρ) è anche totalmente ordinato (TUTTI GLI ELEMENTI DI S SONO CONFRONTABILI)

↳ IL CONTRARIO NON È SEMPRE VERO

DIM Supponiamo che (S, ρ) sia ben ordinato.

Preso $x, y \in S$, $\{x, y\} \subseteq S \setminus \{\emptyset\}$

Dato che (S, ρ) è ben ordinato, per definizione:

$(\exists m \in S)(m = MIN(\{x, y\}))$
- Se $m = x$ allora $x \rho y$
- Se $m = y$ allora $y \rho x$

RELAZIONE DI COPERTURA

Dato l'insieme ordinato (S, ρ)

y <u>COPRE</u> x se $x \rho y \wedge (\forall z \in S)(\neg(x \rho z \wedge z \rho y))$

Z NON STA IN MEZZO A X E Y

↳ Cioè y sta subito dopo x e tra x e y non c'è nient'altro in mezzo

SOLO LA RELAZIONE DI COPERTURA NOSSO DETERMINARE L'ORDINE DELL'INSIEME

L'unica cosa che manca affinché "COPRE" sia una relazione d'ordine è la transitività

↳ In $(\mathbb{N}, \leq)$
- 2 COPRE 1
- 3 COPRE 2
- MA 3 NON COPRE 1 → Non vale la transitività

↳ C'È IL 2 IN MEZZO

Y si dice immediato successore di X

DIAGRAMMI DI HASSE

Il diagramma di Hasse di (S, ρ) è la coppia $(S \times S, g)$ con $(x, y) \in g \Leftrightarrow y$ 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

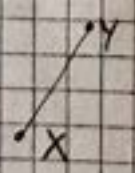
↳ COPRE SE ATTRAVERSO IL $\leq$ E NON IL $<$

↓

X NON COPRE X PERCHÉ CI SAREBBE L'ELEMENTO STESSO X CHE STA IN MEZZO

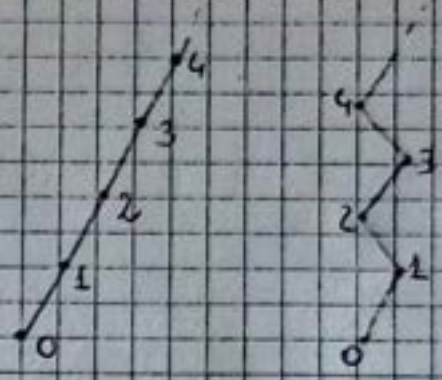
ESEMPIO:

Se ho due elementi di S tali che y COPRE x, li rappresenterò così: →



ESEMPI:

- In $\mathbb{N}$, avremo una rappresentazione del tipo:

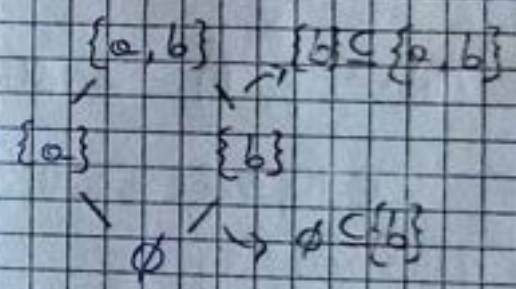


È VISUALE, PERÒ CHE LE LINEE NON SIANO ORIZZONTALI

- Prendo $S = \{a, b\}$ e ordino le parti di S con l'inclusione

$\hookrightarrow (\mathcal{P}(S), \subseteq)$

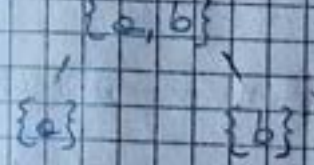
Chi è $(\mathcal{P}(S), \subseteq)$? $(\mathcal{P}(S), \subseteq) = (\{\emptyset, \{a\}, \{b\}, \{a,b\}\}, \subseteq)$



→ SI PERMETTE DI DIRE CHE È INCLUSO IN ECC.

→ IL $\emptyset$ È IL MINIMO DELL'INSIEME E $\{a, b\}$ È IL MASSIMO

- Se ho $S = \{a, b\}$ e $(\mathcal{P}(S) \setminus \{\emptyset\}, \subseteq)$ avrò:



→ IN QUESTO CASO NON HO IL MINIMO

NOTIAMO CHE...

- Se S è totalmente ordinato e si è la relazione di copertura (S è finito), il diagramma di Hasse è una linea.

↳ DO ESEMPIO: $\mathbb{Q}$ È TOTALMENTE ORDINATO MA NON POSSIAMO RAPPRESENTARLO COME LINEA PERCHÉ NON C'È LO SUCCESSORE

FUNZIONE CRESCENTE

Siano (S, p) e $(\bar{S}, \bar{p})$ insiemi ordinati e la funzione:

$f: S \to \bar{S}$

xpy POTREBBE ESSERE FALSA, PRENDO ALTERNATIVE VERA DIMOSTRAZIONE ↳ PERDO INFORMAZIONI

f si dice crescente se: $(\forall x, y \in S)(x p y \to f(x) \bar{p} f(y))$

↳ SEMBRA LA DEFINIZIONE DI OMOMORFISMO MA NON LO È

ISOMORFISMO TRA STRUTTURE ORDINATE

Siano (S, p) e $(\bar{S}, \bar{p})$ insiemi ordinati e la funzione:

$f: S \to S$

f si dice isomorfismo se: $(\forall x, y \in S)(x p y \leftrightarrow f(x) \bar{p} f(y))$

↳ DEVE ESSERE BIETTIVA

$x p y$ SE E SOLO SE $f(x) \bar{p} f(y)$

ESEMPIO:

- Prendo $(\mathbb{N} \setminus \{0\}, \leq)$ e $(\mathbb{N} \setminus \{0\}, |)$. Inoltre, prendo la funzione $f: x \in \mathbb{N} \mapsto x \in \mathbb{N}$, che è biettiva e crescente tra $(\mathbb{N} \setminus \{0\}, |)$ e $(\mathbb{N} \setminus \{0\}, \leq)$.

↓

Prendo $m, n \in \mathbb{N} \setminus \{0\}$: $m | n$

↓

Siamo in $\mathbb{N}$, quindi $m \leq n$.

↳ Vuol dire che: $(\forall m, n \in \mathbb{N} \setminus \{0\})(m | n \to f(m) \leq f(n))$

↓

Notiamo che f è un isomorfismo solo se abbiamo il $\leq$ e solo $\leq$. Infatti, se è vero che $2 | 4$ allora $2 \leq 4$, il contrario non è sempre vero.

↳ Anche se $3 \leq 4$, non è vero che $3 | 4$

INSIEMI ISOMORFI E DIAGRAMMI DI HASSE

Siano (S, ρ) e $(\bar{S}, \bar{\rho})$ insiemi ordinati finiti.

↓

- (S, ρ) e $(\bar{S}, \bar{\rho})$ sono isomorfi se e solo se si possono rappresentare con <u>lo stesso</u> diagramma di Hasse. ↳ SE SONO ISOMORFI, LA RELAZIONE DI COPERTURA È LA STESSA

<u>DIM</u>

(→) Sia f un isomorfismo tra (S, ρ) e $(\bar{S}, \bar{\rho})$

↳ Voglio dimostrare che $(\forall x, y \in S)(y \text{ copre } x \leftrightarrow f(x) \text{ copre } f(y))$

Presi due (elementi) $x, y \in S$, consideriamo un certo z:

$(\exists z \in S)(x \rho z \wedge z \rho y)$ z STA IN MEZZO

↳ Questa cosa è vera se e solo se

$(\exists z \in \bar{S})(f(x) \bar{\rho} z \wedge z \bar{\rho} f(y))$ DATO CHE f È UN ISOMORFISMO

↓

Ma $\bar{z}$ è proprio $f(z)$, quindi:

$(\exists z \in S)(x \rho z \wedge z \rho y) \leftrightarrow (\exists f(z) \in \bar{S})(f(x) \bar{\rho} f(z) \wedge f(z) \bar{\rho} f(y))$

Ho quindi fatto vedere che c'è uno z in mezzo se e solo se c'è un $f(z)$ in mezzo

↳ Ho così dimostrato che $(\forall x, y \in S)(y \text{ copre } x \leftrightarrow f(y) \text{ copre } f(x))$ negando la relazione di copertura, cioè usando la tautologia $(p \leftrightarrow q) \leftrightarrow (\neg p \leftrightarrow \neg q)$

(←) PER LA DIMOSTRAZIONE DELL'ALTRO VERSO SERVE LA DEFINIZIONE DI "ESSERE UN INSIEME FINITO", QUINDI LA FAREMO PIÙ AVANTI

↳ 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

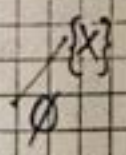
$\downarrow$ $\mathcal{P}(a)$ è totalmente ordinato rispetto a $\subseteq$?

No, $(\mathcal{P}(a), \subseteq)$ non è totalmente ordinato perché abbiamo che $\{x\} \nsubseteq \{y\}$ e che $\{y\} \nsubseteq \{x\}$

[Basta che ci siano almeno due elementi in $\mathcal{P}(a)$, che le parti non sono totalmente ordinate]

$\downarrow$ Infatti, preso $b = \{x\}$

$(\mathcal{P}(b), \subseteq)$ sono totalmente ordinate. Infatti il diagramma di Hasse è:



$\downarrow$

[Solo se b ha un solo elemento (o zero) allora è totalmente ordinato] $\rightarrow$ le parti di $\emptyset$ è $\{\emptyset\}$

MASSIMALE

Dato l'insieme ordinato (S,ρ) e un elemento $m \in S$, m si dice massimale di S se:

$$(\forall x \in S)(\underbrace{(x \rho m \vee m \rho x)}_{\text{ESSERE CONFRONTABILE}} \rightarrow x \rho m)$$

SE, PER OGNI ELEMENTO DI S CONFRONTABILE CON m, m STA SOPRA, ALLORA m È UN MASSIMALE

MINIMALE

Dato l'insieme ordinato (S,ρ) e un elemento $m \in S$, m si dice minimale di S se:

$$(\forall x \in S)(\underbrace{(x \rho m \vee m \rho x)}_{\text{ESSERE CONFRONTABILE}} \rightarrow m \rho x)$$

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:

$$(\forall x \in t)(x \rho m)$$

SONO GLI ELEMENTI DI S CHE SONO PIÙ GRANDI DI TUTTI GLI ELEMENTI DI t

LA DIFFERENZA CON IL MASSIMO È CHE x ∈ t INVECE DI S → x STA IN UN SOTTOINSIEME E m STA FUORI

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

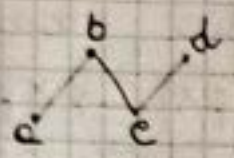
INSIEME DI TUTTI I MAGGIORANTI / MINORANTI

L'insieme dei maggioranti di t in S lo indico con $MAGGIOR_{(S,\rho)}(t)$

L'insieme dei minoranti di t in S lo indico con $MINOR_{(S,\rho)}(t)$

ESEMPIO:

Consideriamo l'insieme ordinato (S,ρ) con questo diagramma di Hasse:



Consideriamo $t=\{a,c\}$

- t non ha minimo
- t non ha massimo
- $MAGGIOR_{(S,\rho)}(t)=\{b\}$ PERCHÉ È CONFRONTABILE CON a, c
- $MINOR_{(S,\rho)}(t)=$ Non esiste $\rightarrow$ Il $MINOR_{(S,\rho)}(\{b\})=\{a,c\}$

Consideriamo (S,ρ), quindi con $S=\{a,b,c,d\}$, $\rho=(S\times S,\varrho)$ e $\varrho=\{(a,b),(c,b),(c,d)\}$

↳ ρ POTREBBE ANCHE ESSERE RIFLESSIVA E CONTENERE LE COPPIE (a,a), (b,b), (c,c), (d,d)

- b è massimale perché:
  - è confrontabile con a e c e sta sopra
  - non è confrontabile con d, quindi l'implicazione è vera perché la prima parte è falsa

[Essere 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 (LEZIONE 23)

2 a) $S = \{x \in \mathcal{P}(\mathbb{N}) \mid x \text{ è SINGLETON}\}$ $(S, \subseteq)$

In questo insieme nessuna coppia di elementi è confrontabile

↳ se $x \neq y$ con $x, y \in S$, non è né vero che $x \subseteq y$ né che $y \subseteq x$ → IL DIAGRAMMA DI HASSE È TUTTO SCONNESSO .....

↓

Visto che nessuno è confrontabile allora sono tutti sia massimale che minimale → L'ANTECEDENTE DEL "→" È FALSO QUINDI LA FRASE È VERA NELLA DEFINIZIONE DI MASSIMALE E MINIMALE

c) $(\mathbb{Z}, |)$

$|$ non è una relazione d'ordine perché non è asimmetrica

↳ Non possiamo cercare massimo e minimo ma massimali e minimali perché non sono definiti

Possiamo, però, trovare un numero che è diviso da tutti gli altri numeri

↳ $x | y :\Longleftrightarrow (\exists k \in \mathbb{Z})(x \cdot k = y) \xrightarrow{\text{su } (\mathbb{N},|)}$ cioè 0, che sta sempre a destra, cioè è un "massimo"

↳ 1, invece, è il "minimo"

min = 1

mat = 0

Dato che 1 è il minimo, questo coincide con l'elemento minimale → 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 minimali sono quei numeri i cui divisori sono soltanto loro stessi

↳ m È MINIMALE $\longleftrightarrow (\forall x \in \mathbb{N} \setminus \{1\})(x$ È m CONFRONT $\rightarrow m|x)$

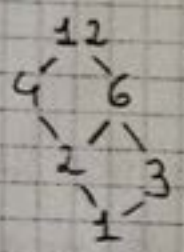
↓

Ad esempio i minimali sono i numeri primi

• Prendo S uguale ai divisori di 12 in $\mathbb{N}$

$S = \{1, 2, 3, 4, 6, 12\}$ con $(S, |)$

Se facciamo il diagramma di Hasse avremo:



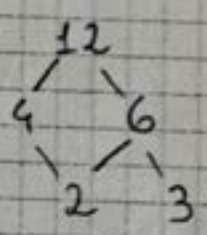
• 12 è il massimo

→ • 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 minimali sono 2 e 3

↳ DUE ELEMENTI CHE SOTTO NON HANNO NULLA

↓

Tutto $\mathbb{N}$ è un grafico del genere con sotto tutti i numeri primi

↳ Possono esserci infiniti elementi minimali se manca il minimo

INSIEME LIMITATO SUPERIORMENTE

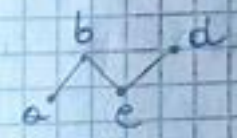
Dato $t \subseteq S$, e (S,ρ) insieme ordinato, t si dice limitato superiormente in S se:
$MAGGIOR_{(S,\rho)}(t) \neq \emptyset$

INSIEME LIMITATO INFERIORMENTE

Dato $t \subseteq S$ e (S,ρ) insieme ordinato, t si dice limitato inferiormente in S se:
$MINOR_{(S,\rho)}(t) \neq \emptyset$

ESEMPIO:

Considerando (S,ρ) e $t = \{a, e\} \subseteq S$ con diagramma di Hasse del tipo:



- Possiamo dire che t è limitato superiormente perché $MAGGIOR_{(S,\rho)}(t) = \{b\}$
- Se invece abbiamo $N = \{d\}$, N è illimitato superiormente perché non c'è nessuno al di sopra di d, anche se S è un insieme finito

NON È NECESSARIO CHE SI ABBIA UN INSIEME INFINITO PER ESSERE ILLIMITATI

INSIEME NATURALMENTE ORDINATO

L'insieme ordinato (S,ρ) si dice naturalmente ordinato se è ben ordinato e ogni parte non vuota superiormente limitata ha massimo.

→ ESSERE BEN ORDINATO, VUOL DIRE CHE CI TROVIAMO SU UNA RELAZIONE D'ORDINE LARGO
→ RISPETTO ALL'ESEMPIO DI PRIMA, VALE $x \rho x$, QUINDI ANCHE I SINGOLI ELEMENTI HANNO IL MASSIMO

SE QUESTA CON CHE PARTE È LIMITATA

ESISTENZA DI $\mathbb{N}$

Notiamo che di ciò che abbiamo studiato, non c'è nulla che giustifichi l'esistenza di $\mathbb{N}$ → BISOGNA INTRODURRE L'ASSIOMA DELL'INFINITO MA LO FAREMO PIÙ AVANTI
↳ DOPO TEOREMA FONDAMENTALE ARITMETICA

↓
lo considero come assioma:
Esiste un insieme naturalmente ordinato e non superiormente limitato. Questo insieme lo chiamo $\mathbb{N}$

↳ 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 vera.

↳ 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 → Posso farlo perché $\mathbb{N}$ è ben ordinato

↳ Da qui entriamo 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

$\mathbb{N}_{MIN\,X}$

Considero una parte di $\mathbb{N}$ non vuota

↳ Sia $X \in \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\}$, definisco $\mathbb{N}_{MIN\,X}$:

$$\mathbb{N}_{MIN\,X} = \{ n \in \mathbb{N} \mid MIN\,X \leq n \}$$ → TUTTI GLI n APPARTENENTI AD $\mathbb{N}$ TALI CHE TUTTI SONO PIÙ GRANDI DEL MINIMO DELLA PARTE X

PRINCIPIO DI INDUZIONE DI I FORMA

$$(\forall X \in \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\})((((\forall n \in \mathbb{N})(n \in X \rightarrow n+1 \in X)) \rightarrow X = \mathbb{N}_{MIN\,X})$$

↳ Cioè, per ogni X, sottoinsieme di $\mathbb{N}$ non vuoto, questa parte di $\mathbb{N}$ è proprio quella parte che sta sopra il minimo di X

ESEMPIO:

Se il minimo di X è 3, la parte X coincide proprio con $\{3, 4, 5, 6, 7, 8, \ldots\}$

↳ L'ipotesi su X è che, per ogni n naturale, se $n \in X$ allora anche $n+1 \in X$ → SE n STA IN X, ANCHE IL SUCCESSIVO STA IN X

ESEMPIO:

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

Sia $m := \min X$

L'INSIEME CHE HA UN MINIMO IN N

Per Assurdo, sia $X \neq \mathbb{N}_{\min X}$

TUTTI I NUMERI DI X SONO MAGGIORI DEL MINIMO DI X

Ovviamente, $m \in \mathbb{N}_{\min X}$, quindi $X \subset \mathbb{N}_{\min X}$

Visto che $X \neq \mathbb{N}_{\min X}$, definisco $Y := \mathbb{N}_{\min X} \setminus X$

↳ $Y \neq \emptyset$ per ipotesi dell'assurdo

Visto che Y non è vuoto e visto che $\mathbb{N}$ è ben ordinato, possiamo prendere il minimo di Y

↳ $n := \min Y$

Visto che i numeri di Y sono tutti i numeri che non stanno in X, ovviamente $m \neq n$.

Inoltre, $m < n$ perché n l'ho preso da Y che sono tutti i numeri naturali più grandi di m meno l'insieme X → Sono comunque numeri più grandi di m

Da qui segue che $m \leq n-1$, e ovviamente $n-1 < n$

↳ $m \leq n-1 < n$

Ciò significa che $n-1 \in X$ perché $n-1$ è maggiore del minimo di X ma è minore strettamente del minimo dei numeri che non appartengono ad X.

Se $n-1 \in X$, allora anche $(n-1)+1 \in X$, cioè $n \in X$, per ipotesi del principio di induzione

Ma ciò è un assurdo ↯

↓

È UNA DIMOSTRAZIONE PER CONTROESEMPIO MINIMO →

- PRENDO IL PIÙ PICCOLO DI QUELLI CHE NON C'È
- PRENDO QUELLO DI PRIMA CHE C'È
- PER IPOTESI PRENDO QUELLO DI DOPO MA QUELLO DOPO DI QUELLO DI PRIMA È LA STESSO ↯

CHI È $m-1$?

Nella dimostrazione del principio di induzione di prima forma abbiamo detto che, preso $Y = \mathbb{N}_{min\,x} \setminus X$, $Y \neq \emptyset$ quindi possiamo prendere il min Y

Abbiamo chiamato $m = \min Y$ e abbiamo visto che se $\underbrace{m-1}\in X \rightarrow m \in X$ ↯

$m-1$ è il massimo degli elementi minori di m

↳ È il massimo dei numeri naturali che sono strettamente minori di m

$m-1$ è il massimo perché $\mathbb{N}$ è naturalmente ordinato

↳ 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 $\min X \rightarrow S \neq \emptyset$

↳ S è superiormente limitata perché esiste m che è il maggiorante di S

Quindi, esiste il $\max S$ che chiamo $m-1$.

PRINCIPIO DI INDUZIONE DI II FORMA

$$(\forall X \in \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\})((\forall m \in \mathbb{N})((\forall k \in \mathbb{N})(\min X \leq k < m \to k \in X) \to m \in X) \to X = \mathbb{N}_{\min X}))$$

QUESTA E' LA PARTE CHE CAMBIA RISPETTO ALLA PRIMA FORMA

Con il principio di induzione di seconda forma non andiamo di successivo in successivo 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 rimpiazzata con: $(\forall k \in \mathbb{N})(\min X \leq k < m \to k \in X)$

↳ TUTTI QUELLI PRIMA DI m E MAGGIORI DEL MINIMO STANNO IN X

<u>DIM</u> PRINCIPIO DI INDUZIONE DI SECONDA FORMA

Sia $m := \min X$

Per Assurdo, sia $X \neq \mathbb{N}_{\min X}$, quindi $X \subset \mathbb{N}_{\min X}$.

Posso definire $Y := \mathbb{N}_{\min X} \setminus X$, quindi $Y \neq \emptyset$ per ipotesi dell'assurdo. Posso 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, devo far vedere che $(\forall k \in \mathbb{N})(\min x \leq k < m \rightarrow k \in X)$ è vera così da avere che l'implicazione è vera e che $m \in X$

↳ Sia $k \in \mathbb{N}$ tale che $m \leq k < m$

Cioè, prendo un certo k che sta tra il minimo di x e il minimo di y

↳ Ma $k \in X$ 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,

$(\forall k \in \mathbb{N})(m \leq k < m \rightarrow k \in X)$

Posso ora usare l'ipotesi del Teorema dato che è verificata

↳ Segue che $m \in X$ ↯

NUMERO PRIMO

I PRIMI NON DEVONO ESSERE INVERTIBILI, INFATTI IN $\mathbb{R}$ NON CI SONO NUMERI PRIMI PERCHÉ TUTTO È DIVISIBILE PER TUTTO

$p \in \mathbb{Z}$ si dice primo se $p \neq 1 \wedge p \neq -1$ e:

↳ I PRIMI SONO

$(\forall a, b \in \mathbb{Z})(p \mid ab \rightarrow (p \mid a \vee p \mid b))$ ↳ DEFINIZIONE EQUIVALENTE AL FATTO DI AVERE SOLO 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

↳ $\underbrace{\{m \in \mathbb{Z} \mid m \mid p\}}_{\text{INSIEME DEI DIVISORI DI } p} = \underbrace{\{-p, -1, 1, p\}}_{\text{INSIEME DEI DIVISORI OVVI (O DIVISORI BANALI)}}$

<u>DIM</u>

Prendo un qualunque divisore di p che chiamo m

↳ 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

↳ 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 ottengo che
   $p \cdot h \cdot k = p$ → Di conseguenza $h \cdot k = 1$
   Visto che ci troviamo in $\mathbb{Z}$, allora vale che
   $h = k = 1 \vee h = k = -1$
   ↳ 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 "$m \cdot k = p$", quindi ottengo che
   $p \cdot m \cdot l = p$ → Di conseguenza $m \cdot l = 1$
   Di conseguenza $m = l = 1 \vee m = l = -1$
   ↳ Segue che $m = 1 \vee m = -1$

Abbiamo quindi dimostrato che i divisori di un numero primo sono o ± 1 o $\pm p$

LEMMA 2

L'INSIEME DI TUTTI I NUMERI NATURALI TALI CHE m DIVIDA m·b

DIVIDE

Siano $m, b \in \mathbb{N} \setminus \{0\}$, sia $X = \{m \in \mathbb{N} \setminus \{0\} \mid m \mid m \cdot b\}$,

X È SEMPRE DIVERSO DAL VUOTO PERCHÉ m·b PUÒ ANCHE ESSERE PROPRIO m

sia $S = \min X$.

↳ S divide tutti gli elementi di X

IL MINIMO DELL'INSIEME X DIVIDE TUTTI GLI ALTRI

↳ Cioè, $(\forall y \in X)(S \mid y)$

DIM — È UNA DIMOSTRAZIONE PER CONTROESEMPIO MINIMO

Per assurdo, dico che S non divide tutti gli elementi di X → l'insieme degli elementi di X che non sono divisi da S non è vuoto

↳ Cioè, per assurdo, non è vuoto l'insieme degli $y \in X$ tali che $S \nmid y$

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 chiamo questo elemento z.

Visto che ci troviamo ancora nell'insieme X, per definizione di X ho che $m \mid z \cdot b$ e $m \mid S \cdot b$

↳ Ciò significa che vale che $mh = zb$ e $mk = Sb$, 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 da 0, allora $[z - S < z]$ perché sottraiamo a z una quantità non nulla

Visto che $z-S < z$, cioè è più piccolo del minimo per cui vale che $S \times y$, allora per $z-S$ vale che viene diviso 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 riscriverlo 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 $m = q_1 \cdot q_2 \cdot \dots \cdot q_s$ allora $r = s$ ed esiste una funzione biettiva $f: \{1, \dots, r\} \to \{1, \dots, r\}$ tale che $(\forall i \in \{1, \dots, r\})(p_i = \pm q_{f(i)})$

E' QUASI LA STESSA DECOMPOSIZIONE

IL NUMERO DI FATTORI 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

a. Dato che il principio di induzione è riferito a $\mathbb{N}$ e $\mathbb{Z}$ non è ben ordinato, dobbiamo ridurci ad $\mathbb{N}$ inizialmente → Sia $m \in \mathbb{N}$

L'IPOTESI È CHE $m \in \mathbb{Z}$

↳ Voglio procedere per induzione di seconda forma → HO BISOGNO DELLA BASE DI INDUZIONE

↳ Voglio dimostrare che tutti i numeri naturali maggiori o uguali a due si possono scrivere come prodotto di primi → Il passo base è che 2 verifichi la tesi

PRINCIPIO DI INDUZIONE SU $\mathbb{N}$

Voglio dimostrare che 2 è primo. → DEVO FAR VEDERE CHE $2 \mid b$

↳ 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 $a = 2h + 1$

Posso sostituire "$2h+1$" in "$2k = ab$", quindi avrò che $2k = 2hb + b$

↳ Di conseguenza $b = 2(k - hb)$, quindi $2 \mid b$

Ciò significa che 2 è primo per la definizione di numero primo.

Posso usare il principio di induzione di seconda forma

1. Suppongo vera la tesi per tutti gli m tali che $2 \leq m < m$ → SE LA PROPRIETÀ VALE PER GLI m (I PICCOLI DI m) ALLORA VALE ANCHE PER m → CON CUI APPLICO IL PRINCIPIO DI INDUZIONE

SUPPONGO CHE TUTTI QUI m SIANO DISPARI PER PRIMI O SIANO PRODOTTO DI PRIMI

(Se m è primo, la tesi è ovvia perché è proprio se stesso. → m È PRODOTTO DI PRIMI PERCHÉ m 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 → DEVO DIMOSTRARLO

• Dato che m non è primo allora:

$(\exists h, k \in \mathbb{N})(m \mid h \cdot k \wedge (m \nmid h \wedge m \nmid k))$ → 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: ↲ SIAMO SICURI? DIMOSTRIAMOLO

$\{n \in \mathbb{N} : n \mid m\} = \{1, m\}$

Definisco l'insieme X:

$X := \{n \in \mathbb{N} \setminus \{0\} : m \mid n \cdot k\}$ e nominio $s = \min X$

Noto che: $h, m \in X$. → PERCHÉ?

• $h \in X$ perché per ipotesi $m \mid h \cdot k$, mentre $m \in X$ perché $m \mid m \cdot k$

Dunque, per il lemma 2 abbiamo che:

$S \mid h \wedge \underbrace{S \mid m}$ → S è un divisore di m

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 $m \mid k$ → Questa cosa non può essere dalla definizione di non primo

↳ Se $S = m$, allora dal fatto che $S \mid h$ si ha che $m \mid h$ → Anche questo è falso dalla definizione

Quindi non è vero che ci sono soltanto divisori banali → S può essere anche altra cosa oltre 1 e m

↳ Ciò significa che:

$(\exists a, b \in \mathbb{N} \setminus \{0, 1\})(m = a \cdot b)$ → a non può essere né 1 né m perché altrimenti b dovrebbe essere 0 o 1

↳ Se $m = 12$, posso prendere $a = 3$ e $b = 4$, basta che esistono i due valori

• Se a e b sono diversi da 1 e m, allora $1 < a, b < m$

• Avevo, inoltre, supposto che l'asserto valesse per tutti gli n: $2 \leq n < m$

Ciò significa che esistono $p_1, p_2, \dots, p_t, p_{t+1}, \dots, p_{u+t}$ primi tali che:

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_t \quad e \quad b = p_{t+1} \cdot p_{t+2} \cdot \dots \cdot p_{u+t}$$

Se questa cosa è vera, allora significa che vale anche per m, infatti:

$$m = a \cdot b = p_1 \cdot p_2 \cdot \dots \cdot p_t \cdot p_{t+1} \cdot p_{t+2} \cdot \dots \cdot p_{u+t}$$

Quindi per induzione di II forma, tutti i numeri naturali in $\mathbb{N} \setminus \{0,1\}$ verificano l'asserto → SE VERIFICANDO CHE SE LA COSA VALE PER I NUMERI PRIMA DI m ALLORA VALE ANCHE PER m, ALLORA VALE PER TUTTI I NUMERI NATURALI MAGGIORI DI m

↓

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 $m = (-p_1) \cdot p_2 \cdot \dots \cdot p_r$ → $-p_1$ 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 $\exists\, f : \{1, \dots, r\} \longrightarrow \{1, \dots, r\}$ biettiva tale che f $(\forall i \in \{1, \dots, r\})(p_i = \pm q_{f(i)})$

ESEMPIO: • $12 = \overset{p_1}{2} \cdot \overset{p_2}{2} \cdot \overset{p_3}{3} = \overset{q_1}{2} \cdot \overset{q_2}{(-2)} \cdot \overset{q_3}{(-3)} = 3 \cdot 2 \cdot 2$

Usiamo l'induzione di prima forma 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 banali

↳ $s = r = 1$ 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'asserto vero per $r-1$

p_1 è primo per definizione e, dato che

$p_1 = m = q_1 \cdot \ldots \cdot q_s$, $p_1 \mid q_1 \cdot \ldots \cdot q_s$

↳ Dalla definizione di primo, p_1 deve dividere uno tra $q_1, q_2, \ldots, q_s$ (almeno)

↳ $(p_1 \mid q_1 \vee p_1 \mid q_2 \cdot \ldots \cdot q_s) \xrightarrow{\text{per induzione}} (p_1 \mid q_1 \vee \ldots \vee p_1 \mid q_s)$

Dato che $(p_1 \mid q_1 \vee \ldots \vee p_1 \mid q_s)$ possiamo supporre, senza ledere la generalità (WLOG) che $p_1 \mid q_1$

WITHOUT LOSS OF GENERALITY

USANDO IL PRODOTTO È COMMUTATIVO QUINDI MI BASTA CAMBIARE GLI INDICI SE $p_1 \mid q_3$ INVECE DI q_1

↓

Poiché q_1 è primo e non può essere ± 1, allora $p_1 = \pm q_1$ per il lemma 1.

Di conseguenza ho che $p_1 \cdot p_2 \cdot \ldots \cdot p_r = m = \pm p_1 \cdot q_2 \cdot \ldots \cdot q_s$

↳ Ciò significa p_1 è cancellabile, quindi ho che $p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s$ → LA DECOMPOSIZIONE CON $r-1$ FATTORI È UGUALE A QUELLA CON $s-1$ FATTORI

Per l'ipotesi di induzione ho che $\underbrace{r-1 = s-1}$, cioè $r = s$

TUTTI QUELLI CON $r-1$ FATTORI HANNO LO STESSO NUMERO DI FATTORI

Inoltre, $\exists\, \sigma : \{2, \ldots, r\} \to \{2, \ldots, r\}$ biettiva tale che $(\forall i \in \{2, \ldots, r\})(p_i = \pm q_{\sigma(i)})$ ↳ SI HA UNA PERMUTAZIONE DEGLI INDICI

Dobbiamo far vedere che abbiamo un funzione $f : \{1, \ldots, r\} \to \{1, \ldots, r\}$ tale che $(\forall i \in \{1, \ldots, r\})(p_i = \pm q_{f(i)})$

↳ Definisco $f : \{1, \ldots, r\} \to \{1, \ldots, r\}$ tale che:

↓ f CONTINUA AD ESSERE BIETTIVA

$f(1) = 1$ e $(\forall i \in \{2, \ldots, r\})(f(i) = \sigma(i))$

CALCOLO COMBINATORIO

DEFINIZIONI

- Un insieme X si dice finito se esiste una biezione 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 biezione 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 $\Longleftrightarrow$ DA QUI SI HA L'ESISTENZA DI UN INSIEME NATURALMENTE ORDINATO NON SUPERIORMENTE LIMITATO, CIOÈ $\mathbb{N}$, E VICEVERSA

↳ Cioè esiste un insieme equipotente ad una parte propria

ESEMPIO: ($\leftarrow$)

- $f: n \in \mathbb{N} \longmapsto 2n \in 2\mathbb{N}$ → È UNA FUNZIONE BIETTIVA TRA $\mathbb{N}$ E UNA PARTE PROPRIA DATO CHE $2\mathbb{N} \subset \mathbb{N}$

($\rightarrow$) È DIFFICILE E NON LO FACCIAMO

TEOREMA

$(\forall m \in \mathbb{N} \setminus \{0\})(\{1, 2, \dots, m\}$ non è infinito$)$

↳ Serve per dire che un insieme finito è non infinito

NO DIM

TEOREMA → DIM NEGLI ESERCIZI DEL 19/11/2021

Se S è un insieme finito, allora ho che

$|\mathcal{P}(S)| = 2^{|S|}$

↑ L'ORDINE DELLE PARTI DI S

Correzione esercizi 19/11/2021 (LEZIONE 29)

3) TEOREMA

Se S è un insieme finito allora ho che se $|S| = n$ allora $|\mathcal{P}(S)| = 2^n$

DIM → PER INDUZIONE DI PRIMA FORMA

Th: $(\forall n \in \mathbb{N})(|S| = n \rightarrow |\mathcal{P}(S)| = 2^n)$

BASE DI INDUZIONE: Per $n=0$ 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 avere un'applicazione suriettiva nel vuoto, 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 deve essere vera per definizione, allora "$(\forall x)(x \in S)$" è falsa, cioè $S = \emptyset$

Noi sappiamo 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 $n=0$

PASSO INDUTTIVO: Suppongo vero l'asserto per tutti gli insiemi di ordine $n \geq 0$ → DEVO FAR VEDERE CHE VALE PER $n+1$

Prendo S di ordine $|S| = n+1$

Visto che $m \geq 0$, allora $S \neq \emptyset$ perché esiste f biettiva che $f: S \to \{1, 2, \dots, m, m+1\}$

- Prendo 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:

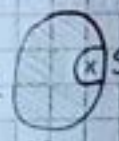
CONSIDERO GRANDI UGUALI NO PERCHÉ, CIOÈ, m È GIÀ COMPRESO CHE f È BIETTIVA NESSUN ALTRO VA CON m

$$f_{|t} : t \longrightarrow \operatorname{Im} f_{|t} = \{1, 2, \dots, m-1, m+1, \dots, m, m+1\}$$

Dato che abbiamo tolto m, $|t| = m$, quindi c'è un'applicazione biettiva che:

$$f_{|t} : t \xrightarrow{Bi} \{1, 2, \dots, m-1, m+1, \dots, m, m+1\} \xrightarrow{Bi} \{1, \dots, m\}$$

- Dall'ipotesi induttiva, abbiamo che $|\mathcal{P}(t)| = 2^m$
- Dato graficamente ho che:



$S = t \cup \{x\}$

$u \subseteq S$
$u = P_1 \cup P_2$
$P_1 \subseteq t$, $P_2 \subseteq \{x\}$

Ogni parte di S è uguale a una parte di t unita a una parte di X.

Le parti di X sono 2, cioè $\mathcal{P}(x) = \{\emptyset, \{x\}\}$

↳ Ciò significa che $|\mathcal{P}(S)| = 2^m \cdot 2 = 2^{m+1}$

- Possiamo ora dire che per induzione di I forma segue la tesi, cioè che l'asserto vale $\forall m \in \mathbb{N}$

PRINCIPIO DI INCLUSIONE - ESCLUSIONE

Se $a_1, a_2, \dots, a_m$ sono insiemi, scrivo:

$$\bigcup_{i=1}^{m} a_i := a_1 \cup a_2 \cup \dots \cup a_m$$

TEOREMA DEL PRINCIPIO DI INCLUSIONE-ESCLUSIONE

$$\left|\bigcup_{i=1}^{m} a_i\right| = \sum_{i=1}^{m} |a_i| - \sum_{1 \le i < j \le m} |a_i \cap a_j| + \sum_{1 \le i < j < k \le m} |a_i \cap a_j \cap a_k| - \dots +$$

$$+ (-1)^{m-1} \cdot |a_1 \cap a_2 \cap \dots \cap a_m|$$

I SEGNI SONO ALTERNI

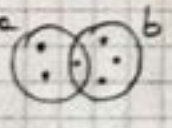
Il concetto di questo teorema è che:
Se ho m insiemi, prendo l'unione di tutti questi insiemi. Poi, mi accorgo che ho preso degli elementi in più che stanno nelle intersezioni e che non ri-conterò facendo la cardinalità dell'insieme unione. Quindi il principio di inclusione-esclusione ci permette di calcolare la corretta cardinalità dell'unione di più insiemi.

ESEMPI:

CON DUE INSIEMI

$|a| = 3$

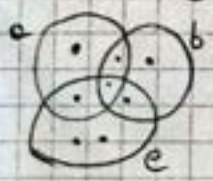
$|b| = 4$



$\rightarrow a \cup b = (a \Delta b) \cup (a \cap b)$

$|a \cup b| = 6$ perché dobbiamo fare $3+4-1=6$, altrimenti considereremmo due volte l'elemento nell'intersezione.

CON TRE INSIEMI



Vogliamo trovare $|a \cup b \cup c|$

$|a| = 4$
$|b| = 4$
$|c| = 5$

PRINCIPIO DI INCLUSIONE - ESCLUSIONE $\rightarrow 4+4+5-2-2-2+1 = 8 = |a \cup b \cup c|$

$|a \cup b \cup c| = 8$ perché:

- Sommiamo prima tutte le cardinalità $|a|+|b|+|c|$
- Sottraiamo le intersezioni a due a due:

$$|a|+|b|+|c| - |a \cap b| - |a \cap c| - |b \cap c|$$

- Ma così facendo eliminiamo tutta l'intersezione di tutti e tre, quindi dato ricaviamo:

$$|a|+|b|+|c| - |a \cap b| - |a \cap c| - |b \cap c| + |a \cap b \cap c|$$

ESEMPI:

- $|a| = 5$
$|b| = 9$
$|a \cap b| = 3$

$|a \cup b|$?

$|a \cup b| = |a| + |b| - |a \cap b| = 11$

- $|a| = 5$
$|b| = 9$

$|a \cap b|$?

$|a \cup b| = 2k \rightarrow$ CIOÈ, SE L'UNIONE È UN MULTIPLO DI 2, QUANTO PUÒ VALERE L'INTERSEZIONE?

$2k = |a| + |b| - |a \cap b|$

$2k = 14 - |a \cap b| \rightarrow |a \cap b| = 2(7-k)$

L'intersezione non può essere più grande di $|a|$ e non può essere minore di 0, quindi:

$0 \leq |a \cap b| = 2(7-k) \leq 5$, di conseguenza

$|a \cap b|$ può valere 0, 2 o 4 $\rightarrow |a \cap b| \in \{0, 2, 4\}$

FATTORIALE

DEFINISCO:
- $0! = 1$
- Se $m > 0$, $m! = (m-1)!\, m$

ESEMPIO:

$3! = 2!\cdot 3 = 1!\, 2\cdot 3 = 0!\cdot 1\cdot 2\cdot 3 = 1\cdot 1\cdot 2\cdot 3 = 6$

TEOREMA

Siano a e b insiemi: $|a| = m$, $|b| = n$, allora:

1) ci sono n^m applicazioni da a a b

DIM (Per induzione di prima forma su m)

- BASE: $m = 0$, cioè $a = \emptyset$ → PER ESSERE VERIFICATA, CI DEVONO ESSERE $n^0 = 1$ FUNZIONI CHE $\emptyset \to b$

Prendo $f: \emptyset \to b$ → è una coppia $(\emptyset \times b, g)$

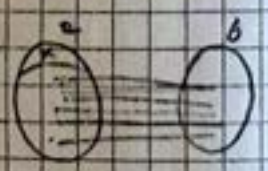
SE NON CI SONO ELEMENTI IN a, NON POSSIAMO MANDARE NULLA IN b QUINDI $g = \emptyset$ → ma $g \subseteq \emptyset \times b = \emptyset$, quindi f è solo $(\emptyset \times b, \emptyset)$. Abbiamo verificato il passo base perché vi è una sola $f: \emptyset \to b$

- PASSO INDUTTIVO: Suppongo vero per $m > 0$

Sia $x \in a$, sia $t = a \setminus \{x\}$ (PRENDO TUTTI GLI ELEMENTI TRANNE x) Per ipotesi di induzione ci sono n^m applicazioni da t a b

Da a a b ci sono $n^m \cdot n$ applicazioni, cioè n^{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) SAPPIAMO AVERE n^m FUNZIONI. QUELL'UNICO ELEMENTO x PUÒ ANDARE IN OGNI ELEMENTO DI b, CIOÈ CI POSSONO ESSERE n FUNZIONI $\{x\} \to b$

2) a. Esistono applicazioni iniettive da a in b se e solo se $m \leq n$

DIM

($\rightarrow$) Sia $a \xrightarrow{f_{IN}} b$. Avremo che esistono delle applicazioni biettive che: $\{1,\dots,m\} \overset{\varphi}{\simeq} a \xrightarrow{f_{IN}} b \overset{\psi}{\simeq} \{1,\dots,n\}$ componendole ho che:

↳ Esiste φ iniettiva di $\{1,\dots,m\}$ in $\{1,\dots,n\}$

Quindi $m \leq n$ — con φ biettiva, infatti che $\{1,\dots,m\} \subseteq \{1,\dots,n\}$

($\leftarrow$) Posso fare la stessa dimostrazione di prima ma con un'applicazione al contrario, cioè:

$m \leq n$, quindi esiste φ iniettiva $\{1,\dots,m\} \rightarrow \{1,\dots,n\}$ dato che risulterà $\{1,\dots,m\} \subseteq \{1,\dots,n\}$ e allora che esistono applicazioni biettive $a \simeq \{1,\dots,m\} \xrightarrow{\varphi} \{1,\dots,n\} \simeq b$.

↳ Quindi esiste $\varphi: a \rightarrow b$ iniettiva

2) b. Le applicazioni iniettive da a in b in numero sono o 0 o $\frac{n!}{(n-m)!}$

DIM

- Se $n < m$ allora le applicazioni iniettive da a in b sono 0.
- Sia $m \leq n$ per l'induzione di prima forma su m

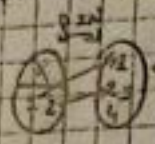
BASE: $m = 0$ → cioè c'è una sola applicazione iniettiva. Infatti: $\frac{n!}{(n-0)!} = 1$ ✓

PASSO INDUTTIVO. Suppongo $m > 0$ e suppongo vero l'asserto per $m-1$. → Voglio far vedere che vale 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 $t \to b$ per ipotesi induttiva.

Segue che da a a b ci sono $\frac{m!}{(m-(m-1))!} \cdot \underbrace{m = (m-1)}$ applicazioni iniettive.



QUESTO PERCHÉ INIZIALMENTE CI SONO m ELEMENTI, X PUÒ ANDARE SOLO NEGLI ELEMENTI DEL CODOMINIO RIMASTI NON PRESI

Ma:

$$\frac{m!}{(m-(m-1))!}(m-(m-1)) = \frac{m!}{(m-m+1)!}(m-(m-1)) =$$

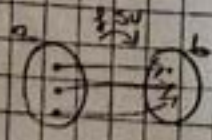
$$= \frac{m!}{(m-m+1)(m-m)!}(m-m+1) = \frac{m!}{(m-m)!}$$

Dal principio di induzione di prima forma vale la tesi.

3) Esistono applicazioni suriettive da a in b se e solo se $a = b = \emptyset \vee 0 < n \leq m$

DIM

- da suriettività si ha se e solo se, per definizione, $(\forall y \in b)((\exists x \in a)(f(x) = y)) \to$ Questa cosa è vera se $b = \emptyset$, ma affinché $b = \emptyset$ e' è bisogno che anche $a = \emptyset$.
  ↳ la funzione $\emptyset \to \emptyset$ è suriettiva
- Nel caso in cui $0 < n \leq m$, la dimostrazione è identica a quando f è iniettiva.



$(\to)$ $\{1, \dots, m\} \overset{\varphi}{\simeq} a \xrightarrow{f \text{ su}} b \simeq \{1, \dots, n\}$

Esiste φ suriettiva $\{1, \dots, m\} \xrightarrow{su} \{1, \dots, n\}$, quindi il codominio è tutto preso, cioè $n \leq m$

$(\leftarrow)$ UGUALE MA AL CONTRARIO

4) Esistono applicazioni biettive da a in b se e solo se $n = m$

DIM

($\rightarrow$) La dimostrazione è un corollario delle due di prima, perché f per essere biettiva deve essere:

- SURIETTIVA $\rightarrow$ $n \leq m$
- INIETTIVA $\rightarrow$ $n \geq m$

$\Big\} n = m$

($\leftarrow$) Esistono, quindi, applicazioni biettive $a \simeq \{1, \dots, n\} \simeq b$

5) $|Sym(a)| = n!$

DIM Dato che Sym(a) sono le applicazioni biettive da a in a, allora queste applicazioni sono anche iniettive. Di conseguenza:

$$\frac{n!}{(n-n)!} = \frac{n!}{0!} = \frac{n!}{1} = n! \quad \text{dato che } n = n$$

6) Sia $n = m$ (a e b hanno lo stesso ordine) e $f: a \rightarrow b$

f è iniettiva se e solo se è biettiva se e solo se è suriettiva.

DIM • Se f è biettiva, allora implica che f è anche suriettiva e iniettiva. Inoltre:

• (INIETTIVA $\rightarrow$ BIETTIVA)

In questo caso, le funzioni iniettive sono $\frac{n!}{(n-n)!} = n!$, proprio come quelle biettive.

↳ DATO CHE L'INSIEME IN È BIETTIVO È UN SOTTOINSIEME DI QUELLO INIETTIVO E I DUE INSIEMI HANNO SOLO IL NUMERO DI ELEMENTI

• (SURIETTIVA $\rightarrow$ BIETTIVA)

Prendo $g: b \rightarrow a$ sezione di f, cioè tale che $f \circ g = Id_b$

Dato che Id_b è iniettiva, allora g è iniettiva.

↳ g è quindi biettiva e notiamo che $f = g^{-1}$

↳ PERCHÉ INIETTIVA E SURIETTIVA

Infatti, $f = g^{-1}$ perché abbiamo che:

$$f \underset{\text{ASSOCIATIVITÀ}}{=} (f \circ g) \circ g^{-1} = Id_b \circ g^{-1} = g^{-1}$$

Quindi, avendo l'inversa, f è biettiva

ATTENZIONE: Questa cosa si ha se a e b sono insiemi finiti, ma non se sono infiniti

ESEMPIO:

- $f: n \in \mathbb{N} \mapsto 2n \in \mathbb{N}$ è iniettiva ma non suriettiva

TEOREMA

Sia $(S, *)$ un monoide commutativo finito (S È FINITO) e sia $x \in S$, allora x è cancellabile se e solo se è invertibile

DIM

($\Leftarrow$) Il caso in cui invertibile $\rightarrow$ cancellabile ($\forall a, b \in S)(x \cdot a = x \cdot b \rightarrow a = b$) l'abbiamo già fatto

($\Rightarrow$) σ_x e δ_x sono iniettive (DATO CHE X È CANCELLABILE) $\rightarrow$ allora sono biettive per il teorema di prima. Essendo σ_x e δ_x biettive, avremo che: $(\exists y \in S)(\sigma_x(y) = 1)$, di conseguenza x è invertibile

(ANCHE 1 HA L'ANTIIMMAGINE ESSENDO σ_x BIETTIVA)

$\hookrightarrow$ Quindi $x \cdot y = 1$,

Inoltre, $(\exists z \in S)(\delta_x(z) = 1)$

$\hookrightarrow$ Quindi $z \cdot x = 1$

Di conseguenza x è invertibile

COROLLARIO

TUTTI ELEMENTI ESPRIMIBILI

PERCHÉ TUTTI INVERTIBILI

1) Gli anelli unitari integri finiti sono corpi

2) I domini di integrità finiti sono campi

SONO COMMUTATIVI

FUNZIONE CARATTERISTICA DI t IN S

Sia S un insieme e sia $t \subseteq S$.

Definisco: $\chi_{t,S} : x \in S \longmapsto \begin{cases} 0 & \text{se } x \notin t \\ 1 & \text{se } x \in t \end{cases}$

"CHI"

La funzione $\chi_{t,S}$ si chiama funzione caratteristica di t in S → MI PERMETTE DI VEDERE CON L'IMMAGINE DI χ 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 $S \to \{0,1\}$

TEOREMA

Sia S un insieme.

Allora $\varphi : t \in \mathcal{P}(S) \longmapsto \chi_{t,S} \in \{0,1\}^S$ è biettiva

DIM

1. Sia $f \in \{0,1\}^S$, cioè è una funzione $S \to \{0,1\}$

↳ Definisco $t = \{x \in S \mid f(x) = 1\}$

Allora, $\varphi(t) = \chi_{t,S}$ e:

- Se $x \in t$ $\chi_{t,S}(x) = 1 = f(x)$
- Se $x \notin t$ $\chi_{t,S}(x) = 0 = f(x)$

Quindi, $\chi_{t,S} = f$ e quindi φ è suriettiva

↳ A OGNI f CORRISPONDE UN $\chi_{t,S}$ PERCHÉ HANNO UGUALE IMMAGINE

2. Sia $t \subseteq S$ e $N \subseteq S$ con $t \neq N$

INIETTIVA

WLOG prendo $x \in t \setminus N$ → un x che sta solo in t

SENZA LEDERE LE GENERALITÀ

- $\chi_{t,S}(x) = 1$
- $\chi_{N,S}(x) = 0$

Ma $\chi_{t,S} \neq \chi_{N,S}$ cioè φ è iniettiva

↳ t diverse → φ diverse

COROLLARIO

Se S è un insieme finito $|\mathcal{P}(S)| = 2^{|S|}$

↳ visto che $\varphi: t \in \mathcal{P}(S) \to \chi_t \in \{0,1\}^S$ è iniettiva il numero di elementi di $\mathcal{P}(S)$ è uguale a quello di $\{0,1\}^S$ ma l'ordine di $\{0,1\}^S$ è $|\{0,1\}|^{|S|} = 2^{|S|}$

COEFFICIENTE BINOMIALE

- Se $m \in \mathbb{N} \setminus \{0\}$, definisco $I_m := \{1, \dots, m\}$
- $\forall m, k \in \mathbb{N}$, definisco $\binom{m}{k} := |\mathcal{P}_k(I_m)|$ → è l'ordine delle k-parti di I_m

COEFFICIENTE BINOMIALE m su k

↳ $\mathcal{P}_k(S)$ si dice "k-parti di S"

ESEMPIO:

- $\binom{0}{3} = 0$ → è la cardinalità delle 3-parti di $I_0 = \emptyset$
- $\binom{4}{4} = 1$ → quante parti di I_4 ci sono con 4 elementi? 1
- Se $m < k$, $\binom{m}{k} = 0$ → per avere un numero maggiore di 0 dovrei mettere in un insieme k elementi avendone a disposizione un numero inferiore

TEOREMA

$$(\forall m \in \mathbb{N})\left(\sum_{k=0}^{m} \binom{m}{k} = 2^m\right)$$

DIM

$$\mathcal{P}(I_m) = \mathcal{P}_0(I_m) \cup \mathcal{P}_1(I_m) \cup \dots \cup \mathcal{P}_m(I_m)$$

Gli ordini di ogni k-parte è, per definizione, $\sum_{k=0}^{m} \binom{m}{k}$ e l'ordine di $\mathcal{P}(I_m)$ sappiamo essere 2^m

TEOREMA

$$(\forall m, k \in \mathbb{N})\left(k \leq m \rightarrow \binom{m}{k} = \binom{m}{m-k}\right)$$

PER OGNI PARTE CON K ELEMENTI CE NE STA UNA SOLA CON m-k ELEMENTI, E' LA DIFFERENZA

DIM

$f: X \in \mathcal{P}(I_m) \mapsto I_m \setminus X \in \mathcal{P}(I_m)$ sappiamo essere biettiva

Ma $\vec{f}(\mathcal{P}_k(I_m)) = \mathcal{P}_{m-k}(I_m)$ → INFATTI LE PARTI CON K ELEMENTI LE MANDO NELLE PARTI IN m-k ELEMENTI DATO CHE STO FACENDO LA DIFFERENZA

Se faccio $f_{|\mathcal{P}_k(I_m)}: X \in \mathcal{P}_k(I_m) \mapsto I_m \setminus X \in \mathcal{P}(I_m)$, posso poi immergerla nella $\mathcal{P}_{m-k}(I_m)$ che è l'$\mathrm{Im} f_{|\mathcal{P}_k(I_m)}$

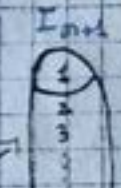
RESTRINGO IL CODOMINIO ALL'$\mathrm{Im} f$

FORMULA RICORSIVA PER I COEFFICIENTI BINOMIALI

$$(\forall m, k \in \mathbb{N})\left(k \leq m \Rightarrow \binom{m+1}{k+1} = \binom{m}{k} + \binom{m}{k+1}\right)$$

DIM

- Prendo le $k+1$ parti di I_{m+1} che non contengono 1 e chiamo questo insieme "a".



- b = $(k+1)$ parti di I_{m+1} che contengono 1.

$\{a, b\}$ è una partizione di $\mathcal{P}_{k+1}(I_{m+1})$

ESSENDO UNA PARTIZIONE

Allora: $\binom{m+1}{k+1} \overset{\text{ESSENDO UNA PARTIZIONE}}{=} |\mathcal{P}_{k+1}(I_{m+1})| = |a| + |b| = \binom{m}{k+1} + \binom{m}{k}$

$|a| = \binom{m}{k+1}$ 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 1 lo do per scontato, deve stare per forza nelle parti, quindi ci possono essere solo k parti di I_m combinazioni diverse

TRIANGOLO DI TARTAGLIA

$$\binom{0}{0}$$

$$\binom{1}{0} \quad \binom{1}{1}$$

$$\binom{2}{0} \quad \binom{2}{1} + \binom{2}{2}$$

$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$

$m+1$

$k+1$

$$\begin{array}{ccccccccccc} & & & & & 1 & & & & & \\ & & & & 1 & & 1 & & & & \\ & & & 1 & & 2 & & 1 & & & \\ & & 1 & & 3 & & 3 & & 1 & & \\ & 1 & & 4 & & 6 & & 4 & & 1 & \\ 1 & & 5 & & 10 & & 10 & & 5 & & 1 \end{array}$$

TEOREMA

$$(\forall m, k \in \mathbb{N})\left(k \leq m \rightarrow \binom{m}{k} = \frac{m!}{(m-k)!\,k!}\right)$$

DIM Uso il principio di induzione di seconda forma su m → USO LA SECONDA FORMA PERCHÉ NEI COEFFICIENTI BINOMIALI AVRÒ $m-1$ CHE È MINORE DI m

BASE: Se $m=0$

$$\binom{0}{k} = \binom{0}{0} = 1 = \frac{0!}{0!\,0!}$$

APPROFONDIMENTO 2 PAGINE AVANTI

PASSO INDUTTIVO: Suppongo vera la tesi per* tutti gli i: $0 \leq i < m$

FORMULA RICORSIVA

$$\binom{m}{k} = \binom{m-1}{k-1} + \binom{m-1}{k} = \text{Per l'ipotesi induttiva} =$$

$$= \frac{(m-1)!}{(m-1-(k-1))!\,(k-1)!} + \frac{(m-1)!}{(m-1-k)!\,k!} = \frac{(m-1)!}{(m-k)!\,(k-1)!} + \frac{(m-1)!}{(m-k-1)!\,k!} =$$

MOLTIPLICO E DIVIDO PER k

MOLTIPLICO E DIVIDO PER $m-k$

ORA HO LO STESSO DENOMINATORE

$$= \frac{(m-1)!\,k}{(m-k)!\,k!} + \frac{(m-1)!\,(m-k)}{(m-k)!\,k!} = \frac{(m-1)!\,(k+m-k)}{(m-k)!\,k!} = \frac{(m-1)!\,m}{(m-k)!\,k!} =$$

$$= \frac{m!}{(m-k)!\,k!}$$

Correzione esercizi 23/11/2021 (LEZIONE 25)

6.

$2 \to \binom{2}{1} \quad \binom{2}{2}$

$3 \to \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$

$4 \to \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3}$

$5 \to \binom{5}{1} \quad \binom{5}{2} \quad \binom{5}{3}$

$\binom{6}{1} \quad \binom{6}{3}$

PER LA FORMULA RICORSIVA PER I COEFFICIENTI BINOMIALI

$\binom{7}{3}$ ← VOGLIAMO CALCOLARLO CON IL TRIANGOLO DI T.

PER LA FORMULA RICORSIVA PER I COEFFICIENTI BINOMIALI

ESEMPIO:

$\binom{3}{2} = 3$ → perché se ho l'insieme $\{1,2,3\}$, le 2-parti di tre sono: $\{1,2\}, \{1,3\}, \{2,3\}$

↳ Quindi secondo la formula ricorsiva il triangolo di Tartaglia sarà:

2 1

3 3 1

4 6 4

5 10 10

15 20

35

QUESTI LI RICAVO FACENDO LA SOMMA DEI DUE DI PRIMA, CHE CONOSCO PERCHÉ SU È FACILE CAPIRE $\binom{n}{1}$ E $\binom{n}{n}$

→ Quindi $\binom{7}{3} = 35$

Posso anche calcolare $\binom{7}{3}$ senza il triangolo di Tartaglia, grazie alla formula → $\frac{7!}{(7-3)!\,3!} = \frac{7!}{4!\cdot 3!} = \frac{7\cdot 6\cdot 5\cdot 4!}{4!\cdot 6} = 35$

Invece, $\binom{7}{4} = \frac{7!}{(7-4)!\,4!} = \frac{7!}{3!\cdot 4!} = 35$

7 $a = \{ n \in \mathbb{N} \mid n \leq 9 \}$ insieme di 10 elementi

NON C'È UNA PARTE DI 11 ELEMENTI SOLO PERCHÉ L'INSIEME È DI 10

- $|\mathcal{P}_{11}(a)| = 0$
- $|\mathcal{P}_{10}(a)| = 1$
- $\binom{10}{3} = \frac{10!}{7!\,3!} = \frac{10\cdot 9\cdot 8}{6} = 120$
- $\binom{10}{7} = \frac{10!}{3!\cdot 7!} = 120$

• $|\{t \in \mathcal{P}_4(a) \mid 0 \in t\}| = \binom{9}{3} = \frac{9!}{6!\,3!} = \frac{9 \cdot 8 \cdot 7}{6} = 84$

↓

È l'insieme delle 4-parti di a che contengono 0 → 0 lo dò per scontato, quindi quello che può cambiare sono tre elementi in $a \setminus \{0\}$

↳ le parti sono del tipo: $\{0, x, y, z\}$ e $x, y, z \in a \setminus \{0\}$

INSIEMI ISOMORFI E DIAGRAMMI DI HASSE

Già sappiamo che dati due insiemi ordinati finiti (S, ρ) e (S', ρ'), questi sono isomorfi se e solo se sono rappresentati dallo stesso diagramma di Hasse.

Abbiamo dimostrato l'implicazione (→).

Dimostriamo anche (←) → PRIMA CI SERVIVA IL CONCETTO DI FINITEZZA

DIM (←)

Sia γ una relazione di copertura su (S, ρ) e γ' una relazione di copertura su (S', ρ').

Per ipotesi esiste $f: S \to S'$ biettiva:

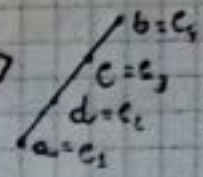
$(\forall a, b \in S)(a \gamma b \leftrightarrow f(a) \gamma' f(b))$ → AVERE LO STESSO DIAGRAMMA DI HASSE SIGNIFICA AVERE LA STESSA RELAZIONE DI COPERTURA

↳ la relazione di copertura non è una relazione di equivalenza perché non è transitiva

Definisco la rendo transitiva

$$(\forall a, b \in S)(a \leq b \leftrightarrow ((\exists n \in \mathbb{N})((\exists e_1, e_2, \dots, e_n \in S)$$
$$(a = e_1 \wedge e_1 \gamma e_2 \wedge e_2 \gamma e_3 \wedge \dots \wedge e_{n-1} \gamma e_n \wedge e_n = b)))$$

Cioè, così facendo, posso dire che $a \leq b$ se c'è una relazione di copertura a catena da b fino ad a

↳ 

In questo caso ho che b copre c, c copre d, d copre a, quindi $a \leq b$

↓

Ho così reso transitiva la copertura, o meglio, ho estrapolato una nuova relazione che è anche transitiva

↳ Si verifica facilmente che $\leq$ è una relazione d'ordine su S

Analogamente, definisco la relazione $\leq'$ su S':

$$(\forall a', b' \in S')(a' \leq' b' \leftrightarrow ((\exists m \in \mathbb{N})(\exists c'_1, c'_2, \dots, c'_m \in S')$$
$$(a' = c'_1 \wedge c'_1 \gamma' c'_2 \wedge c'_2 \gamma' c'_3 \wedge \dots \wedge c'_{m-1} \gamma' c'_m \wedge c'_m = b')))$$

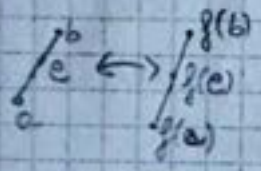
Notiamo che $\leq = \rho$ e $\leq' = \rho'$

→ SE L'INSIEME NON È FINITO, LA RELAZIONE DI COPERTURA NON GENERA UNA RELAZIONE D'ORDINE CON LA CATENA TRA a E b

↳ Infatti, se abbiamo una relazione di copertura estesa come quella definita, abbiamo che se vale $a \leq b$ allora vale anche $a \rho b$.
Se, invece, abbiamo $a \rho b$, visto che l'insieme è finito allora abbiamo una relazione di copertura e quindi vale anche $a \leq b$

Inoltre, notiamo che vale che:

$$(\forall a, b \in S)(a \leq b \leftrightarrow f(a) \leq' f(b))$$



↳ In base a come abbiamo definito le due relazioni di copertura, se consideriamo $a' = f(a)$, $b' = f(b)$ ecc; se è verificata γ' allora è verificata anche $\leq'$

Abbiamo così dimostrato la tesi, cioè $(S, \rho) \overset{?}{\simeq} (S', \rho')$ ISOMORFO

*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 lessicografico

Volevo dimostrare che:

$$\forall k \quad \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

→ Per usare il principio di induzione di II forma devo dimostrare che valga per tutti i numeri più piccoli di k

Per dare un ordine ai coefficienti binomiali simile all'ordine in $\mathbb{N}$ uso un ordine lessicografico

Vedo $\binom{n}{k}$ come la coppia (n,k) e ordino le coppie in modo lessicografico

ORDINE LESSICOGRAFICO

$$(0,0) < (1,0) < (1,1) < (2,0) < (2,1) < (2,2) < (3,0) < \dots$$

↳ Prima confronto il valore a sinistra della coppia, se sono uguali allora confronto il valore a destra

Infatti, noto che $\binom{n-1}{k-1} < \binom{n-1}{k} < \binom{n}{k}$ nell'ordine lessicografico, quindi posso usare il principio di induzione di II forma

TEOREMA BINOMIALE O FORMULA DI NEWTON

$$(a+b)^n = \binom{n}{0} a^n b^0 + \binom{n}{1} a^{n-1} b^1 + \dots + \binom{n}{n-1} a^1 b^{n-1} + \binom{n}{n} a^0 b^n$$

→ SIA S UN ANELLO UNITARIO, $a,b \in S$ E TALI CHE $ab=ba$

<u>DIM</u>

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), m si dice:

MASSIMO: $m = \text{MAX } S \iff (\forall x \in S)(x\, p\, m)$

MASSIMALE: $(\forall x \in S)(\text{SE } x \text{ E } m \text{ SONO CONFRONTABILI} \rightarrow x\, p\, m)$

MAGGIORANTE: $m \in \text{MAGGIOR}_{(S,p)}(t) \iff (\forall x \in t)(x\, p\, m)$ con $t \subseteq S$

MINIMO: $m = \text{MIN } S \iff (\forall x \in S)(m\, p\, x)$

MINIMALE: $(\forall x \in S)(\text{SE } x \text{ E } m \text{ SONO CONFRONTABILI} \rightarrow m\, p\, x)$

MINORANTE: $m \in \text{MINOR}_{(S,p)}(t) \iff (\forall x \in t)(m\, p\, x)$ con $t \subseteq S$

Notiamo che ciò che cambia tra massimo e minimo, massimale e minimale, maggiorante e minorante è la posizione di m rispetto a x. (L'ORDINE DELLA COPPIA)

↳ Possiamo usare un'operazione duale del tipo:

Dato (S,p) con $p := (S \times S, g)$, l'operazione opposta sarà $\bar{p} := (S \times S, \bar{g})$ con $(a,b) \in \bar{g} \iff (b,a) \in g$

↓

Da qui posso ottenere, ad esempio, che:

$m = \max(S,p) \iff m = \min(S,\bar{p})$

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, ρ) ordinato,
Se $m = \min(S, \rho)$ allora m è l'unico minimale in (S, ρ)

DIM

Prendo n elemento minimale di (S, ρ).
Per ipotesi, visto che m è il minimo, vale $m \rho n$
↳ Dunque, m e n sono confrontabili
Allora per definizione di elemento minimale, vale $n \rho m$
Ma la relazione è asimmetrica, quindi si ha che $n = m$ → SE ESISTE IL MINIMO, È L'UNICO MINIMALE

Posso dimostrare questo teorema anche per il massimo
↳ Posso considerare l'insieme $(S, \bar{\rho})$
Questo teorema vale anche in $(S, \bar{\rho})$, 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 $t \subseteq \mathbb{N}$
  - $\text{minor}_{(\mathbb{N},\leq)}(t)$? Ad esempio, $\text{minor}_{(\mathbb{N},\leq)}(2\mathbb{N}) = \{0\}$
- $(\mathbb{N}, |)$ $t \subseteq \mathbb{N}$
  - $\text{minor}_{(\mathbb{N},|)}(t)$? Ad esempio, $\text{minor}_{(\mathbb{N},|)}(\{2,3\}) = \{1\}$
    $\text{minor}_{(\mathbb{N},|)}(2\mathbb{N}) = \{1, 2\}$

SONO I DIVISORI COMUNI DELL'INSIEME

  - $\text{maggior}_{(\mathbb{N},|)}(t)$? Ad esempio, $\text{maggior}_{(\mathbb{N},|)}(\{2,3\}) = 6\mathbb{N}$ → I MULTIPLI DI 6
    $\text{maggior}_{(\mathbb{N},|)}(2\mathbb{N}) = \{0\}$

SONO I MULTIPLI COMUNI DELL'INSIEME

0 È MULTIPLO DI OGNI NUMERO, INFATTI $0 = 0 \cdot m$

- $(\mathcal{P}(S), \subseteq)$ $\quad t \subseteq \mathcal{P}(S)$

UNIONE UNARIA DI t

- $y \in \text{maggior}_{(\mathcal{P}(S),\subseteq)}(t) \longleftrightarrow \bigcup t \subseteq y$

SONO TUTTE LE PARTI CHE CONTENGONO GLI ELEMENTI DI Y

ESEMPIO:

$S = \{1,2,3\}$ e prendo $t = \{\{1\},\{2\}\}$

$\text{maggior}_{(\mathcal{P}(S),\subseteq)}(\{\{1\},\{2\}\})$ = 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, x se solo se $\{1,2\} = \bigcup t \subseteq y$

$\hookrightarrow 1 \in y \wedge 2 \in y$

INTERSEZIONE UNARIA DI t

- $y \in \text{minor}_{(\mathcal{P}(S),\subseteq)}(t) \longleftrightarrow y \subseteq \bigcap t$

ESEMPIO:

$\text{minor}_{(\mathcal{P}(S),\subseteq)}(\emptyset) = \mathcal{P}(S)$ → UN ELEMENTO DI $\mathcal{P}(S)$ APPARTIENE AI MINORANTI DI $\emptyset$ SE E SOLO SE $(\forall x \in \emptyset)(y \subseteq x)$, MA QUESTA COSA È SEMPRE VERA DATO CHE, COME FBF, SI HA UN "→" CHE HA LA PRIMA PARTE FALSA, QUINDI I MINORANTI SONO TUTTI GLI ELEMENTI DI $\mathcal{P}(S)$

DALLA DEFINIZIONE

↓

DALL'ASSIOMA DI SEPARAZIONE ABBIAMO CHE QUESTO È TUTTO $\mathcal{P}(S)$ PERCHÈ SAREBBE DOVUTO ESSERE L'INSIEME DI TUTTI GLI INSIEMI

TEOREMA

Sia (S,p) un insieme ordinato finito non vuoto e $p \in OL(S)$.
Allora (S,p) ha elementi minimali ed elementi massimali

<u>DIM</u>

Per Assurdo, sia che (S,p) non ha elementi minimali
Considero $x \in S$, che per l'ipotesi di assurdo non è un minimale

↳ Se $S = \{x\}$, x risulta essere un minimale, quindi necessariamente $(\exists y \in S)(x \neq y)$ ↳ S NON PUO' ESSERE UN SINGLETON

↓

Questo y non è un minimale per ipotesi di assurdo e, inoltre, vale $y p x$.

• PERCHÈ VALE $y p x$?
NOI SAPPIAMO DALLA DEFINIZIONE CHE:
x è minimale $\leftrightarrow (\forall y \in S)((x p y \vee y p x) \rightarrow (x p y))$
SE FACCIAMO LA NEGAZIONE DI "ESSERE MINIMALE" AVREMO:
x non è minimale $\leftrightarrow (\exists y \in S)((x p y \vee y p x) \wedge (\neg x p y)) \leftrightarrow$ DISTRIBUTIVITÀ DI $\wedge$ RISPETTO $\wedge$ $\vee$
$\leftrightarrow (\exists y \in S)((\underbrace{x p y \wedge (\neg x p y)}_{F}) \vee (y p x \wedge (\neg x p y))) \leftrightarrow$
$\leftrightarrow (\exists y \in S)(y p x \wedge (\neg x p y))$

Di conseguenza ho che y è più piccolo di x, quindi nel diagramma di Hasse ho che: $\begin{smallmatrix} x \\ | \\ y \end{smallmatrix}$

Visto che y non è minimale, allora ho che $(\exists z \in S)(z \neq y \wedge z p y)$

↳ Inoltre $z \neq x$ perché se fosse uguale a x, allora potrei avere $x p y$, ma abbiamo detto che non è vero

Posso continuare andando oltre $|S|$ ↯ $\begin{smallmatrix} x \\ | \\ y \\ | \\ z \end{smallmatrix}$

TEOREMA

Se un insieme finito ordinato ha un unico elemento minimale, questo è anche il minimo

Se un insieme finito ordinato ha un unico elemento massimale, questo è anche il massimo

NO DIM

Questo non vale se l'insieme è infinito

ESEMPIO:

- $(\mathbb{N}, \leq)$ e prendo un insieme X.

$S := \mathbb{N} \cup \{x\}$

$\leq = (\mathbb{N} \times \mathbb{N}, G)$

Considero $p = (S \times S, g)$ con $g = G \cup \{(x,x)\}$

↳ DEFINISCO UN'ALTRA RELAZIONE D'ORDINE, UGUALE AL $\leq$, MA CHE HA ANCHE LA COPPIA (x,x) NEL GRAFICO OLTRE A QUELLE CON I NUMERI NATURALI

$0 p 10$? Sì $\rightarrow (0,10) \in g$

$0 p x$? Sì $\rightarrow (0,x) \in g$

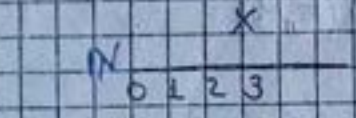
$x p x$ Sì $\rightarrow (x,x) \in g$

(S, p) non ha massimo perché non c'è un elemento che è più grande di tutti gli altri, ma

C'È UN ELEMENTO 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



RELAZIONE D'ORDINE INDOTTA DA f SU a

Se $f: a \to b$ e $\rho \in OL(b)$ definisco:

$(\forall x, y \in a)(x \rho_f y \leftrightarrow f(x) \rho f(y))$ e la chiamo relazione d'ordine indotta da f su a

ESTREMO INFERIORE

(S, ρ) insieme, con $t \subseteq S$, se esiste il massimo di $MINOR_{(S,\rho)}(t)$ lo dico $inf_{(S,\rho)}(t)$ → il MASSIMO DEI MINORANTI

ESTREMO SUPERIORE

(S, ρ) insieme, con $t \subseteq S$, se esiste il minimo di $MAGGIOR_{(S,\rho)}(t)$ lo dico $sup_{(S,\rho)}(t)$ → il MINIMO DEI MAGGIORANTI

ESEMPIO:

- $(\mathbb{N}, \leq)$ $\quad SUP_{(\mathbb{N},\leq)}(\{3,4\}) = 4$

  $SUP_{(\mathbb{N},\leq)}(2\mathbb{N}) = \nexists$ → IN $2\mathbb{N}$ NON CI SONO MAGGIORANTI

  $INF_{(\mathbb{N},\leq)}(2\mathbb{N}) = \{0\}$

RETICOLO

(S, ρ) ordinato si dice reticolo se per ogni $x, y \in S$, $\{x, y\}$ ha estremo superiore ed estremo inferiore.

OPERAZIONI INF E SUP

Se (S, ρ) è un reticolo, definisco:

- $\wedge$ (WEDGE): $(x,y) \in S \times S \mapsto INF_{(S,\rho)}(\{x,y\})$
- $\vee$ (VEE): $(x,y) \in S \times S \mapsto SUP_{(S,\rho)}(\{x,y\})$

$(S, \wedge, \vee)$ è una struttura algebrica a 2 operazioni interne

RETICOLO LIMITATO

Un reticolo (S, ρ) si dice limitato se ha massimo e minimo

RETICOLO COMPLETO

Un reticolo (S, ρ) si dice completo se ogni sua parte diversa dal vuoto ammette estremo superiore ed estremo inferiore

DEFINIZIONE FORMALE DI RETICOLO

(S, ρ) è un reticolo $\Leftrightarrow (\forall a, b \in S)(\exists \sup(\{a, b\}) \wedge$
$\wedge \exists \inf(\{a, b\}))$ → se sup e inf sono di S

Se ho degli elementi non confrontabili, l'implicazione diventa subito falsa, quindi automaticamente esistono sup e inf, quindi (S, ρ) è un reticolo

Correzione esercizi 24/11/2021 (LEZIONE 26)

1) a. $(\mathbb{N}, \leq)$

CIOÈ È L'ELEMENTO SUBITO DOPO O, CIOÈ TALE CHE NON CE NE SIA NESSUNO IN MEZZO

0 è coperto da 1

1 è coperto da 2

2 è coperto da 3

b. $(\mathbb{N}, |)$ → x COPRE 0 <-> $0|x$ E NON C'È NESSUN ALTRO ELEMENTO IN MEZZO

Ma $0|x \leftrightarrow x=0$ → ma 0 è uguale a x stesso, quindi nessun elemento copre 0

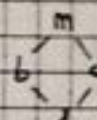
COSÌ NON È NEGLI DIVISORI DA SOLO 1

↳ 1 è coperto da tutti e soli i numeri primi

↳ ESEMPIO:

Se prendo un certo numero primo p, di certo $1|p$

Se prendo un certo $x \in \mathbb{N}$: $1|x \wedge x|p \rightarrow x=1 \vee x=p$

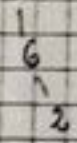


← Se prendo m non primo → $m=ab$ con $1<a, b<m$

↳ m non copre 1

2 è coperto da tutti e soli i numeri divisibili per due e non per quattro

↳ ESEMPIO: 12 → 12 NON COPRE 2 PERCHÉ C'È 6 IN MEZZO



c. $(\mathbb{Q}, \leq)$ Dato che $\mathbb{Q}$ è denso, nessun numero è coperto da alcun numero

ESEMPIO: Preso $x \in \mathbb{Q}$ $(\forall y \in \mathbb{Q} \setminus \{x\})(\exists z \in \mathbb{Q})(x<z<y \vee y<z<x)$

Esiste sempre un numero z tra x e y

↓

Nessun numero è coperto da nessun altro numero

RETICOLO

P DEVE ESSERE DI ORDINE LARGO

(S,p) è un reticolo $\leftrightarrow (\forall a,b \in S)(\exists \sup(\{a,b\}) \wedge \exists \inf(\{a,b\}))$

- Se a e b sono confrontabili, ad esempio se apb, allora $\sup_{(S,p)}(\{a,b\}) = \{b\}$ → DATO PRENDENDO TUTTI I MAGGIORANTI DI $\{a,b\}$, VI TROVO CHE LE bpb ELEVA IL SUP È PROPRIO b → GLI ALTRI MAGGIORANTI SCRIVO DEL TIPO bpx

- Nel caso in cui abbiamo:

  $S = \mathbb{N} \cup \{x\}$, per tutti gli elementi di $\mathbb{N}$ possiamo trovare il sup e l'inf poiché gli elementi sono confrontabili

  Ma, se tutti i numeri n sono più grandi di 0, non possiamo confrontare x con altri numeri

  ↳ $\nexists \sup_{(S,p)}(\{0,x\})$ perché solo x è confrontabile con x, quindi non ci sono maggioranti

- Dato l'insieme $(\mathcal{P}(S), \subseteq)$, con $t, u \in \mathcal{P}(S)$
  - $\sup(\{t,u\}) = t \cup u$
  - $\inf(\{t,u\}) = t \cap u$ → COME SI DIMOSTRA?

    ↓ $t \cap u$ è UN MINORANTE?

Sì, dato che $t \cap u \subseteq t \wedge t \cap u \subseteq u$, di conseguenza $t \cap u \in MINOR(\{t,u\})$

↓ È ELEMENTO CONTENE OGNI MINOR?

Preso $x \in MINOR(\{t,u\})$, cioè $x \subseteq t \wedge x \subseteq u$, allora $x \subseteq t \cap u$. Di conseguenza $t \cap u = \inf(\{t,u\})$

Quindi $(\mathcal{P}(S), \subseteq)$ è un reticolo ed è completo dato che ogni parte di $\mathcal{P}(S)$ ha sup e inf

↳ Se $t \subseteq \mathcal{P}(S)$, $\inf(t) = \cap t$

$\sup(t) = \cup t$

SUP = MCM INF = MCD

- Preso $(\mathbb{N}, |)$, questo è un reticolo, è limitato perché 1 è il minimo e 0 è il massimo, ma non è completo
- Preso $(\mathbb{N} \setminus \{0\}, |)$, questo non è un reticolo limitato perché $\nexists \sup(2\mathbb{N})$
  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, ρ) un reticolo, dico $(S, \bar{\rho})$ il reticolo duale di (S, ρ).
$\bar{\rho}$ COME ρ MA CON LE COPPIE SCAMBIATE

Se E è un enunciato sui reticoli, dico enunciato duale $(\bar{E})$ l'enunciato che si ottiene scambiando in E tutti i ρ con $\bar{\rho}$, i "$\wedge$" con "$\vee$" e "$\vee$" con "$\wedge$"
Sono i sup e inf → NON I CONNETTIVI LOGICI

TEOREMA (PRINCIPIO DI DUALITÀ PER I RETICOLI)

Se E è una formula valida per ogni reticolo, allora anche $\bar{E}$ lo è.

DIM

Se E è valida per ogni reticolo, allora E è valida anche per $(S, \bar{\rho})$ → Dato che $(S, \bar{\rho})$ è comunque un reticolo
↳ Ma in $(S, \bar{\rho})$ gli inf sono i sup di (S, ρ) e viceversa, per cui E riferito a $(S, \bar{\rho})$ è esattamente $\bar{E}$ riferito a (S, ρ)

Possiamo, così, risparmiare molto tempo nelle dimostrazioni dei teoremi sui reticoli

TEOREMA

In un reticolo, ogni elemento minimale è minimo

DIM

Sia m un elemento minimale e $x \in S$. Prendo l'inf di $\{m, x\}$. Poiché $(m \wedge x)\, \rho\, x$ ma m è minimale, ho che $m \wedge x = m$, ovvero $m \rho x$ → MAX È L'INF DI $\{m, x\}$, QUINDI È PIÙ PICCOLO DI m → NIENTE È PIÙ PICCOLO DI m

↳ m è il minimo perché confrontabile con ogni $x \in S$

Per il principio di dualità, posso scrivere che:

In un reticolo, ogni elemento massimale (rispettivamente massimale) è minimo (rispettivamente massimo)

TEOREMA

Sia (S, ρ) un reticolo. Allora, ogni parte finita di S ha inf e sup in (S, ρ)

DIM ← PER IL PRINCIPIO DI DUALITÀ POSSIAMO LIMITARCI A inf

1) Siano a, b parti finite di S. Allora,

$MINOR_{(S,\rho)}(a \cup b) = MINOR(a) \cap MINOR(b)$

→ DIM

($\subseteq$) Prendo $x \in MINOR(a \cup b)$ → x è un MINORANTE DI $a \cup b$

$x \in MINOR(a \cup b) \leftrightarrow (\forall y \in a \cup b)(x \rho y)$ ma ciò significa che x è un minorante di tutti gli elementi di a e di tutti gli elementi di b.

O ANCHE POSSIAMO DIMOSTRARLO PER ESTENSIONALITÀ

Cioè $x \in MINOR(a) \cap x \in MINOR(b)$

($\supseteq$) Vale anche il verso contrario per le stesse motivazioni a ritroso, quindi:

$x \in MINOR(a \cup b) \leftrightarrow x \in MINOR(a) \cap x \in MINOR(b)$

2) Sia $m = \inf_{(S,\rho)}(a)$, se esiste.

Allora $MINOR(a) = MINOR(\{m\}) = \{x \in S \mid x \rho m\}$

↳ Dato che m è più piccolo di ogni elemento di a, è ovvio che per transitività ogni minorante di m lo è anche di a e viceversa

3) Siano $m_1 = \inf(a)$ e $m_2 = \inf(b)$, se esistono.

Allora, per 1) e 2) ho che:

$MINOR(a \cup b) = MINOR(a) \cap MINOR(b) =$

$= MINOR(\{m_1\}) \cap MINOR(\{m_2\}) = MINOR(\{m_1, m_2\})$

I MINORANTI DI $a \cup b$ NON SONO ALTRO CHE I MINORANTI DELLA COPPIA CON GLI inf

4) (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. → $\boxed{t = \{x\},\ \inf(t) = \{x\} = t}$

Sia $|t| > 1$ e chiamo l'ordine di t, n. $|t| = n$

Quindi $n > 1$ e sia vero l'asserto per tutte le parti di S di ordine $n-1$

• Prendo $x \in t$, quindi $t = v \cup \{x\}$

Di conseguenza, $v = t \setminus \{x\}$ e $|v| = n-1$. Quindi, per l'ipotesi di induzione prendo $m = \inf(v)$.

Allora per il punto 3):

$MINOR(t) = MINOR(v \cup \{x\}) = MINOR(\{m, x\})$

↳ Poiché siamo in un reticolo, $MINOR(\{m, x\})$ ha massimo.

↳ $\{m, x\}$ è un RETICOLO

↓

Di conseguenza t ha inf. → DATO CHE ABBIAMO DIMOSTRATO L'ASSERTO PER UNA PARTE DI ORDINE n DA UNA DI ORDINE $n-1$, L'ASSERTO VALE PER OGNI PARTE FINITA

ATTENZIONE!

Se prendiamo una parte infinita l'asserto non vale, infatti in $(\mathbb{N}, \leq)$, $\mathbb{N}$ non ha il sup

PROPRIETA' DI $(S, \wedge, \vee)$

Già sappiamo che $(S, \wedge, \vee)$ è una struttura algebrica tra

PROPRIETA' COMMUTATIVA

In $(S, \wedge, \vee)$ vale la proprietà commutativa, infatti:

DIM Preso $x, y \in S$:

$x \wedge y = \inf_{(S,\rho)}(\{x, y\}) = \inf_{(S,\rho)}(\{y, x\}) = y \wedge x$. Inoltre,

$x \vee y = \sup_{(S,\rho)}(\{x, y\}) = \sup_{(S,\rho)}(\{y, x\}) = y \vee x$

Quindi vale la proprietà commutativa per $\vee$ e $\wedge$.

Inoltre vale sempre che:

- $x \rho (x \vee y)$ e $y \rho (x \vee y)$
- $(x \wedge y) \rho x$ e $(x \wedge y) \rho y$

PROPRIETA' ASSOCIATIVA

Vale la proprietà associativa per $\vee$ e per $\wedge$ in $(S, \wedge, \vee)$

DIM Considero $\vee$.

Siano $x, y, z \in S$. Vale $\underline{x \rho (x \vee (y \vee z))}$ (sono elementi). Inoltre vale che $\underline{(y \vee z) \rho (x \vee (y \vee z))}$. Per lo stesso motivo vale:

$\underline{y \rho (y \vee z)}$ e $\underline{z \rho (y \vee z)}$. Quindi per transitività vale che:

$\underline{y \rho (x \vee (y \vee z))}$ e $\underline{z \rho (x \vee (y \vee z))}$.

Allora $\underline{(x \vee y) \rho (x \vee (y \vee z))}$, vale e vale $\underline{((x \vee y) \vee z) \rho (x \vee (y \vee z))}$.

Analogamente ho che $(x \vee (y \vee z)) \rho ((x \vee y) \vee z)$ e, per l'asimmetria, ho che $(x \vee (y \vee z)) = ((x \vee y) \vee z)$.

Inoltre, per il principio di dualità, anche $\wedge$ è associativa

PROPRIETÀ DI ASSORBIMENTO

$(\forall x, y \in S)((\underbrace{x \vee (x \wedge y) = x}_{\text{"x assorbe } (x \wedge y)}) \wedge (x \wedge (x \vee y) = x))$

PROPRIETÀ DI ITERATIVITÀ (O IDEMPOTENZA)

$(x \wedge x = x \wedge x \vee x = x)$ → SEGUE DALLA PROPRIETÀ DI ASSORBIMENTO

STRUTTURE ALGEBRICHE CON COMMUTATIVITÀ, ASSOCIATIVITÀ E ASSORBIMENTO SONO RETICOLI

Abbiamo considerato (S, ρ) come reticolo (con $\rho \in OL(S)$)

$\wedge_\rho$ e $\vee_\rho$ sono gli inf e sup definiti attraverso la relazione d'ordine → sono operazioni su S che dipendono da ρ (lo esplicitiamo con $\wedge_\rho$ e $\vee_\rho$)

- Quindi, in $(S, \wedge_\rho, \vee_\rho)$ vale la commutatività, l'associatività e l'assorbimento, e notiamo che queste strutture algebriche, con queste proprietà, in realtà sono dei reticoli

TEOREMA

Sia S un insieme non vuoto e sia $\mathcal{R}$ l'insieme delle relazioni d'ordine ρ su S tali che:

$\rho \in \mathcal{R} \Leftrightarrow (S, \rho)$ è un reticolo. → L'INSIEME $\mathcal{R}$ È FATTO SOLO DA RELAZIONI D'ORDINE CHE DEFINISCONO UN RETICOLO

Sia $\mathcal{B}$ l'insieme delle coppie ordinate di operazioni binarie interne di S tali che:

una certa $(\alpha, \beta) \in \mathcal{B} \Leftrightarrow$ sono associative, commutative e in (S, α, β) vale la legge di assorbimento

Allora l'applicazione che: $\rho \in \mathcal{R} \mapsto (\wedge_\rho, \vee_\rho) \in \mathcal{B}$ è biettiva.

↳ Possiamo parlare indistintamente di reticolo nel senso dell'ordine e di reticolo nel senso di struttura algebrica (se con quelle indicate)

SEMPLIFICA LE DIMOSTR

DIM Voglio trovarmi l'inverso di $p \in R \xmapsto{f} (\wedge_p, \vee_p) \in b$,

Sia $(\wedge, \vee) \in b$. Definisco:

$(\forall x, y \in S)(x p y :\Leftrightarrow x = x \wedge y)$ → DA QUESTO SEGUE CHE $x \vee y = (x \wedge y) \vee y =$ PER ASSORBIMENTO y, QUINDI SICURAMENTE VALE CHE $x p y \Leftrightarrow x = x \wedge y \Leftrightarrow y = x \vee y$*

1) p è d'ordine largo?

- $x = x \wedge x$ per l'iteratività. Dunque $(\forall x \in S)(x p x)$, quindi p è riflessiva
- Se $x = x \wedge y$ e $y = y \wedge x$, allora $x = x \wedge y = y \wedge x = y$, quindi p è asimmetrica
- Se $x p y \wedge y p z$, $x = x \wedge y \wedge y = y \wedge z$. Quindi vale che $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$, quindi vale $x p z$ e di conseguenza p è transitiva

2) Vogliamo che $\forall x, y \in S$, $\inf_{(S,p)}(\{x, y\}) = x \wedge y$ e che $\sup_{(S,p)}(\{x, y\}) = x \vee y$ → cioè sto applicando f a p

Per assorbimento $(x \wedge y) \vee x = x$, ovvero, per definizione con $\vee$, ho $(x \wedge y) p x$ → QUESTO PERCHÉ PRECEDENTEMENTE $(x \wedge y) \vee y = y$* MA ECCO LA x

Allo stesso modo anche $(x \wedge y) p y$ vale. VOGLIO CHE $x \wedge y$ VERIFICHI CHE È UN MINORANTE

Dunque $x \wedge y \in MINOR_{(S,p)}(\{x, y\})$. Prendo $z \in MINOR_{(S,p)}(\{x, y\})$, cioè vale $z p y$ e $z p x$, di conseguenza $z = z \wedge y$ e $z = z \wedge x$, quindi $z = z \wedge x = (z \wedge y) \wedge x = z \wedge (x \wedge y)$.

Per definizione, quindi, $z p (x \wedge y)$, cioè:

$$x \wedge y = \inf_{(S,p)}(\{x, y\})$$

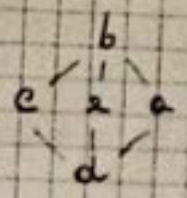
Analogamente si può dimostrare per sup.

Abbiamo dimostrato che $(\wedge, \vee) \in b \mapsto p \in R$ è l'inversa di f, infatti applicando questa funzione e poi f riotteniamo gli stessi sup e inf

C'È LA DIMOSTRAZIONE

Correzione esercizi 25/11/2021 (LEZIONE 27)

1)



(S, ρ) con $S = \{a, b, c, d, e\}$

$\rho = (S \times S, g)$

$$g = \{\underbrace{(a,a), (b,b), (c,c), (d,d), (e,e)}_{\text{DIAG S?}}, (d,a), (d,e), (d,c), (d,b), (a,b), (e,b), (c,b)\}$$

RIFLESSIVITÀ

TRANSITIVITÀ

Per far vedere che (S, ρ) è un reticolo dobbiamo vedere se esiste il sup e l'inf per tutte le coppie di g → L'INCOMPARABILE È VIGLIERO TRA GLI ELEMENTI NON CONFRONTABILI

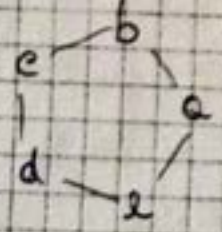
- $INF_{(S,\rho)}(\{d, a\}) = d$ → CIOÈ (c, a), E NOTIAMO CHE I MINORANTI DI (c, a) È d, QUINDI (S, ρ) È UN RETICOLO
- $MAGGIOR_{(S,\rho)}(\{d, a\}) = MAGGIOR_{(S,\rho)}(\{a\})$

$\downarrow$

$\min(\{a\}) = a$

SE $a > d$, ALLORA È CHIARO CHE → $d \rho x$ / $a \rho x = a \rho x$ PERCHÉ SE $x > a$ ALLORA È ANCHE MAGGIORE DI d PERCHÉ $a > d$

2)



I minoranti di (c, a) sono solo e, stessa cosa anche per (d, a)

↳ Quindi l'inf è sempre d

→ CIOÈ, I MINORANTI SONO TUTTI GLI ELEMENTI TALI CHE $x \rho c$ E $x \rho a$

RICAPITOLO DELLA SCORSA VOLTA

$(S, \rho) \rightarrow (S, \wedge_\rho, \vee_\rho)$ → STESSO RETICOLO MA $\wedge$ E $\vee$ IN MODO DIVERSO

ESEMPIO:

- $(\mathcal{P}(S), \subseteq) \rightarrow (\mathcal{P}(S), \cap, \cup)$

$INF_{(\mathcal{P}(S), \subseteq)}(\{X, Y\}) = X \cap Y$

ISOMORFISMO TRA RETICOLI

Sia $(S, \wedge, \vee)$ un reticolo e $(S', \wedge', \vee')$ un altro reticolo.

La funzione $f: S \to S'$ si dice isomorfismo della struttura algebrica $(S, \wedge, \vee)$ in $(S', \wedge', \vee')$ se f è biettiva e vale che:

$$(\forall x, y \in S)\big(f(x \wedge y) = f(x) \wedge' f(y) \text{ e } f(x \vee y) = f(x) \vee' f(y)\big)$$

QUANDO CHE SI PARLA DI STRUTTURE ALGEBRICHE CON DUE OPERAZIONI, L'ISOMORFISMO DEVE AVERE PER ENTRAMBE LE OPERAZIONI

Se, invece, vediamo i reticoli come strutture ordinate (S, ρ) e (S', ρ'), allora f si dice isomorfismo se e solo se $x \rho y \leftrightarrow f(x) \rho' f(y)$ ed f è una funzione biettiva

TEOREMA → FARE L'ISOMORFISMO DI RETICOLI VISTI COME STRUTTURE ALGEBRICHE O STRUTTURE ORDINATE È LA STESSA COSA

Siano $(S, \wedge, \vee)$ e $(S', \wedge', \vee')$ reticoli e sia $f: S \to S'$ biettiva.

f è un isomorfismo tra $(S, \wedge, \vee)$ e $(S', \wedge', \vee')$ se e solo se f è un isomorfismo tra $(S, \rho_{(\wedge, \vee)})$ e $(S', \rho_{(\wedge', \vee')})$

DIM

Siano (S, ρ) e (S', ρ') reticoli

($\leftarrow$) Sia f un isomorfismo tra (S, ρ) e (S', ρ'), ovvero tale che $x \rho y \leftrightarrow f(x) \rho' f(y)$ → VOGLIAMO FAR VEDERE CHE QUESTO È ANCHE UN ISOMORFISMO TRA STRUTTURE ALGEBRICHE → CIOÈ CHE CONSERVA LE OPERAZIONI $\wedge$ E $\vee$

(S, ρ) lo possiamo anche vedere come $(S, \wedge_\rho, \vee_\rho)$

(S', ρ) lo possiamo anche vedere come $(S', \wedge_{\rho'}, \vee_{\rho'})$

DIMOSTRIAMO CHE SI CONSERVA $\wedge$

• Sappiamo che $\forall x, y \in S$ valgono $(x \wedge_\rho y) \rho x$ e $(x \wedge_\rho y) \rho y$ → CIOÈ È MINORE DI ENTRAMBI

Essendo f un isomorfismo, posso fare f a entrambe le relazioni e ottengo che:

$(x \wedge_p y)\, p\, x \longleftrightarrow f(x \wedge_p y)\, p'\, f(x)$ e ho che
$(x \wedge_p y)\, p\, y \longleftrightarrow f(x \wedge_p y)\, p'\, f(y)$, cioè sto dicendo
che $f(x \wedge_p y) \in MINOR_{(S',p')}(\{f(x), f(y)\})$

$f(x \wedge_p y)$ è l'INF DI (S',p')?

• Ora devo far vedere che $f(x \wedge_p y)$ è il più grande dei minoranti, quindi prendo un certo z tale che $z \in MINOR_{(S',p')}(\{f(x), f(y)\})$.
Cioè sto prendendo z tale che $z\, p'\, f(x)$ AND $z\, p'\, f(y)$

DATO CHE È 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 $w\, p\, x \wedge_p y$ → SE È PIÙ PICCOLO DI ENTRAMBI ALLORA È 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 $f(x \wedge_p y) = INF_{(S',p')}(f(x), f(y)) =$
↳ z È PIÙ PICCOLO DEL MINORANTE $f(x \wedge_p y)$
ISOMORFISMO → $= f(x) \wedge_{p'} f(y)$

ALLO STESSO MODO SI PUÒ DIMOSTRARE 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 ALGEBRICHE ASSOCIATE

(→) Sia f un isomorfismo tra $(S, \wedge_p, \vee_p)$ e $(S', \wedge_{p'}, \vee_{p'})$
Prendo $x, y \in S$ tali che $x\, p\, y$.
↳ VOGLIO DIMOSTRARE CHE VALE $x\, p\, y \longleftrightarrow f(x)\, p'\, f(y)$
↳ Per definizione ho che $x = x \wedge_p y$ ↳ SE x È PIÙ PICCOLO TRA x E y, ALLORA È 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 $f(x \wedge_p y) = f(x) \wedge_{p'} f(y)$
↳ Per definizione ho che $f(x)\, p'\, f(y) \rightarrow$
↳ DI $\wedge_{p'}$

HO COSÌ DIMOSTRATO CHE $x\, p\, y \rightarrow f(x)\, p'\, f(y)$.
PER DIMOSTRARE L'ALTRO VERSO $f(x)\, p'\, f(y) \rightarrow x\, p\, y$ SEGUO LO STESSO RAGIONAMENTO AL CONTRARIO ESSENDO f SURIETTIVA ALLORA ANCHE LE ANTIIMMAGINI SONO UGUALI *

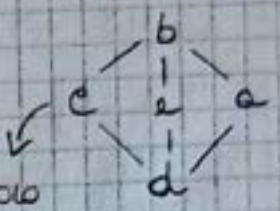
SOTTORETICOLI

Sia $(S, \wedge, \vee)$ un reticolo e sia $t \in \mathcal{P}(S) \setminus \{\emptyset\}$ ← È UN SOTTOINSIEME DI S NON VUOTO

Se t è una parte chiusa rispetto a $\wedge$ e $\vee$, t è detto sottoreticolo di $(S, \wedge, \vee)$

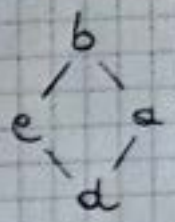
ESEMPIO:

- Dato il reticolo:



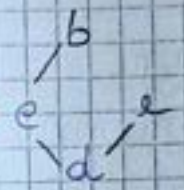
RETICOLO TRIRETTANGOLO

Il reticolo:



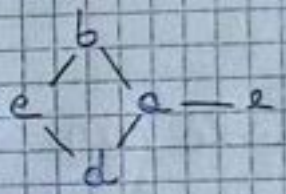
È UNA PARTE CHIUSA RISPETTO ALLE OPERAZIONI DI PRIMA

è un suo sottoreticolo

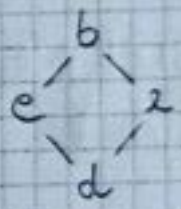
- 

Non è un reticolo perché: $\nexists \sup(\{b, e\})$

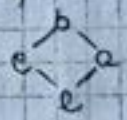
- Dato il reticolo:

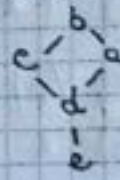


e il reticolo:



Pur essendo entrambi dei reticoli, il secondo non è un sottoreticolo del primo perché nel primo abbiamo che $b \wedge e = a$, mentre nel secondo $b \wedge e = e$

↳ O ANCHE 

$c \wedge e = e$ MENTRE 

$c \wedge a = d$

INTERVALLO (CHIUSO)

Sia (S, ρ) un insieme ordinato e $\rho \in OL(S)$.

$I \subseteq S$ 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 CI SONO TUTTI QUELLI IN MEZZO

ESEMPIO:

- In $(\mathbb{N}, \leq)$ $\{1, 2, 3\}$ è un intervallo

  $\{1, 3\}$ non è un intervallo → NON C'È 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 ce ne sono infiniti in mezzo

- $(\mathbb{N}, |)$ $\{m \in \mathbb{N} \mid n|m\}$ è un intervallo
  ↳ $\forall x, y \in I$, se $x|z$ e $z|y \rightarrow z|m$ → PER TRANSITIVITÀ
    ↳ 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

- $(\mathbb{Q}, |)$ non ci sono intervalli perché ogni numero è diviso da ogni numero (tranne 0)

PROPOSIZIONE

Gli intervalli di un reticolo sono dei sottoreticoli

ESEMPIO:

- In $(\mathbb{N}, |)$, $\{1, 2, 3, 4, 6, 12\}$ è un sottoreticolo

ELEMENTO NEUTRO DI UN RETICOLO 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 $\vee_p$ → C'È IL MASSIMO E IL MINIMO DEL RETICOLO

DIM → FACCIAMOLO CON IL MASSIMO, CON IL MINIMO SI DIMOSTRA NELLO STESSO MODO

Prendo $x \in S$

($\rightarrow$) Considero $M \wedge_p x$, per definizione di massimo, vale $x \, p \, M$

Per definizione di $\wedge_p$ ho che $M \wedge_p x = x \rightarrow M$ è neutro per $\wedge_p$

($\leftarrow$) Se M è l'elemento neutro, allora:

$(\forall x \in S)(M \wedge_p x = x) \rightarrow$ Per definizione $(\forall x \in S)(x \, p \, M) \rightarrow M$ è il massimo

RETICOLO COMPLEMENTATO

Sia $(S, \wedge, \vee)$ un reticolo limitato. Il reticolo si dice complementato se:

IL SUP TRA x E y È IL MAX DI S

$$(\forall x \in S)((\exists y \in S)(x \wedge y = MIN(S) \text{ AND } x \vee y = MAX(S)))$$

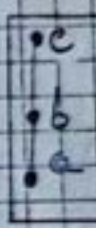
NON ESISTONO NA UNA COMPLEMENTO

SUP INF TRA x E y È IL MIN DI S

Inoltre, y si dice complemento di x e x si dice complementato da y → OGNI CON ELEMENTO IL SUO COMPLEMENTO È UNICO

ESEMPIO:

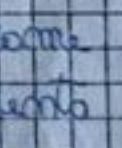
- Un insieme totalmente ordinato con più di due elementi non è complementato
  - ↳ $(\mathbb{N}, \leq)$ non lo è perché infinito
    - ↳ NON HA NESSUNO IL MASSIMO



→ IN QUESTO CASO NON ESISTE UN COMPLEMENTO DI b PERCHÉ $a \wedge b = MIN(S)$ MA $a \vee b = b$ CHE NON È IL MASSIMO DI S

- In $(\mathbb{N}, |)$, se prendo m primo, non ci sono divisori comuni con $m+1$ non banali
  - ↳ $m \wedge m+1 = 1$, quindi per ogni elemento di $\mathbb{N}$ si ha il $MIN(S)$

Ma $(\forall n \neq 0)((\nexists m)(n \vee m = 0))$ quindi $(\mathbb{N}, |)$ è un reticolo limitato ma non complementato.



- → Questo è un reticolo complementato perché e ha come complemento c e b ha come complemento d

TEOREMA → BUONO SE DUE ELEMENTI SONO COMPLEMENTATI MA NON SONO MINIMO E MASSIMO, ALLORA QUESTI DUE ELEMENTI NON SONO COMPARABILI

Due elementi sono complementati e confrontabili se e solo se sono il minimo e il massimo

DIM

(←) MIN E MAX SONO CHIARAMENTE CONFRONTABILI E COMPLEMENTARI TRA LORO

(→) (COMPLEMENTATI + CONFRONTABILI) = $(x \wedge y = MIN + x \rho y) \rightarrow x \wedge y = x = MIN$

$x \vee y = y \wedge x = y \wedge y = y$

DISTRIBUTIVITÀ DEL RETICOLO

Un reticolo (S,ρ) si dice distributivo se:

$$(\forall a,b,c \in S)(a \wedge_\rho (b \vee_\rho c) = (a \wedge_\rho b) \vee_\rho (a \wedge_\rho c) \text{ AND}$$

$$\text{AND } a \vee_\rho (b \wedge_\rho c) = (a \vee_\rho b) \wedge_\rho (a \vee_\rho c))$$

posso limitarmi a una delle due

Si può dimostrare che se vale che $a \wedge_\rho (b \vee_\rho c) = (a \wedge_\rho b) \vee_\rho (a \wedge_\rho c)$ allora vale anche l'altro → Quindi solo questa prima è la condizione necessaria affinché si abbia la distributività.

TEOREMA

Se (S,ρ) è un reticolo distributivo, allora ogni complemento è unico.

DIM

Sia $X \in S$ un elemento complementato. Siano Y e Z complementi di X.

Suppongo (S,ρ) limitato. Dico $M = \max S$ e $m = \min S$.

uso che ho elementi che sono complementi

Vale che:

$$Y = Y \wedge_\rho M \overset{Z \text{ è un complemento}}{=} Y \wedge_\rho (X \vee_\rho Z) \underset{\text{distr. diretta}}{=} (Y \wedge_\rho X) \vee_\rho (Y \wedge_\rho Z) \overset{Y \text{ è un complemento}}{=} m \vee_\rho (Y \wedge_\rho Z) =$$

$$= Y \wedge_\rho Z$$

cioè $Y \rho Z$, analogamente $Z \rho Y$, dunque $Y = Z$

CRITERIO DI DISTRIBUTIVITÀ DI BIRKHOFF

Un reticolo è distributivo se e solo se non contiene sottoreticoli isomorfi al reticolo triangolo e al reticolo pentagono

NO DIM

Correzione esercizi 26/11/2021 (LEZIONE 28)

2) $(S, |) \leq (\mathbb{N}, |)$ è complementato? → CIOÈ, SE $\forall m, m \in S$ HO CHE $m \vee, m = 30$ E $m \wedge, m = 1$ → MAX E MIN DI S

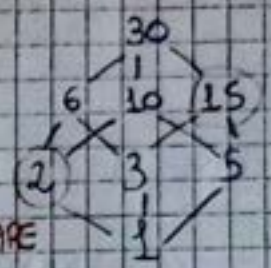
sottoreticolo di $(\mathbb{N}, |)$

tutti i divisori di 30

$$S = \{ m \in \mathbb{N} \mid m | 30 \} = \{1, 2, 3, 5, 6, 10, 15, 30\}$$

POSSO APPUNTARE A VEDERLO VALO A UNO CASO CHE DEVO CONTROLLARE SOLO 3 ELEMENTI

Il reticolo disegnato sarà:



CHI È IL COMPLEMENTARE DI 2?

IL SUP DELLA DIVISIONE → mcm

- Esiste $x \in S$ tale che $2 \vee, x = 30$?

Dobbiamo trovare x tra gli elementi non confrontabili a 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 → MCD

- Inoltre, esiste $x \in S$ tale che $2 \wedge, x = 1$, e notiamo che x è proprio 15 → $2 \wedge, 15 = 1$

<u>Quindi 15 è complementare di 2</u>

Notiamo che:
- 15 e 2 sono complementati
- 3 e 10 sono complementati
- 5 e 6 sono complementati
- 30 e 1 sono complementati

PERCHÉ MINIMO E MASSIMO

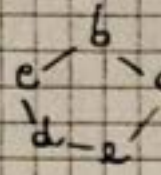
TUTTI GLI ELEMENTI SONO COMPLEMENTATI

↓

IL RETICOLO È COMPLEMENTATO

IL RETICOLO PENTAGONALE E' DISTRIBUTIVO

Consideriamo il reticolo pentagonale:



→ Il reticolo pentagonale non è distributivo perché contiene $\mathcal{N}$ stesso, quindi per il criterio di distributività di Birkhoff non è distributivo

Infatti notiamo che c'è una terna di elementi che:

$$\left.\begin{array}{l} c \wedge (d \vee a) = c \wedge b = c \\ (c \wedge d) \vee (c \wedge a) = d \vee e = d \end{array}\right\} \text{NON E' DISTRIBUTIVA}$$

DISTRIBUTIVITA' DI RETICOLI E SOTTORETICOLI

- Se il reticolo è distributivo, tutti i suoi sottoreticoli sono distributivi
- Se il reticolo non è distributivo, tutti i sottoreticoli non sono distributivi

RETICOLO BOOLEANO

Sia (S, ρ) un reticolo booleano. Il reticolo booleano è un reticolo distributivo e complementato

ALGEBRA BOOLEANA (O ALGEBRA DI BOOLE)

La struttura alg. $(S, \wedge_\rho, \vee_\rho, ')$ è chiamata algebra di Boole

- S → è il reticolo booleano visto come struttura algebrica
- $\wedge_\rho$, $\vee_\rho$ → WEDGE, VEL → OPERAZIONI BINARIE INTERNE
- $'$ → COMPLEMENTAZIONE (UN APOSTROFO) → OPERAZIONE UNARIA INTERNA

PROPRIETA' DELL' ALGEBRA BOOLEANA

1) $\wedge_p$ e $\vee_p$ sono commutative
2) $\wedge_p$ e $\vee_p$ sono associative
3) Tra $\wedge_p$ e $\vee_p$ valgono 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 $\wedge_p$ → cioè 1 è il massimo
   0 è l'elemento neutro di $\vee_p$ → cioè 0 è il minimo
6) Vale che: posso mettere l'apice perché so che per ogni elemento il suo complementato è unico

$$(\forall x \in S)(x \vee_p x' = 1 \text{ AND } x \wedge_p x' = 0)$$

} definisco ' come "il complementare"

Abbiamo già visto che è possibile passare, grazie a un teorema, da un reticolo booleano all'algebra di Boole e viceversa

↳ (S, p) RETICOLO BOOLEANO $\longleftrightarrow$ $(S, \wedge_p, \vee_p, ')$ ALGEBRA BOOLEANA

ESEMPIO:

- $(\mathcal{P}(S), \cap, \cup, \setminus)$ è un'algebra di Boole

ANELLO BOOLEANO

→ DA UN ANELLO BOOLEANO POSSO DEFINIRE UN RETICOLO BOOLEANO

$(a, +, \cdot)$ è un anello booleano se è un anello unitario e si ha che $(\forall x \in a)(x^2 = x)$

↳ $(a, \cdot)$ È UN MONOIDE → ESISTE L'ELEMENTO NEUTRO DI $\cdot$

ESSENDO UN ANELLO, SI HA CHE: $(a, +)$ È UN GRUPPO ABELIANO
$(a, \cdot)$ È UN SEMIGRUPPO
VALE LA DISTRIBUTIVITÀ DI $\cdot$ RISPETTO A $+$

SI È DIMOSTRATO CHE GLI ANELLI BOOLEANI SONO COMMUTATIVI

↳ $(a, \cdot)$ È COMMUTATIVO MENTRE $(a, +)$ LO È GIÀ PER DEFINIZIONE

INOLTRE, NEGLI ANELLI BOOLEANI, $(\forall x \in a)(2x = 0)$
$(\forall x \in a)(x + x = 0)$

RETICOLO BOOLEANO E ANELLO BOOLEANO

Sia $(a, +, \cdot)$ un anello booleano → SE CI PONIAMO NEL CASO CONCRETO DI $(\mathcal{P}(S), \cap, \cup, \setminus)$, IL $\cdot$ È L'INTERSEZIONE, MA IL $+$ NON È PROPRIO L'UNIONE

Definisco che $(\forall x, y \in a)(x \, p \, y \longleftrightarrow x \cdot y = x)$

Allora, (a, p) è un reticolo booleano

DIM ($\rightarrow$) ANELLO BOOLEANO → RETICOLO BOOLEANO

- p è una relazione di ordine largo?

1) p è riflessiva, infatti, essendo l'anello booleano, $x \cdot x = x$ quindi per l'ipotesi vale $x \, p \, x$

2) p è asimmetrica, infatti:
$x \, p \, y$ AND $y \, p \, x \longleftrightarrow x \cdot y = x$ AND $y \cdot x = y$, ma dato che l'anello booleano è commutativo allora $x = x \cdot y = y \cdot x = y$, cioè $y = x$

3) p è transitiva, infatti:
$x \, p \, y$ AND $y \, p \, z \longrightarrow x \cdot y = x$ AND $y \cdot z = y$
Allora $x \cdot z = (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot y = x$, cioè $x \, p \, z$

- Affinché $(a, +, \cdot)$ sia un reticolo, dobbiamo dimostrare che per ogni coppia di elementi di a ci sono sup e inf e devo vedere chi sono $\wedge_p$ e $\vee_p$
↳ Voglio dimostrare che $x \vee_p y = x + y + x \cdot y$, e $x \wedge_p y = x \cdot y$ LA DIMOSTRAZIONE È SULLO STESSO PROCEDIMENTO

1) $x + y + x \cdot y$ è un maggiorante, infatti:
ALLO STESSO MODO DIMOSTRO $\vee_p(x, y, x \cdot y)$ vale $x \, p \, (x + y + x \cdot y)$,
$x \cdot (x + y + x \cdot y) \underset{\text{DISTRIBUTIVITÀ}}{=} x^2 + xy + x^2 y \underset{\text{È UN ANELLO BOOLEANO}}{=} x + x \cdot y + x \cdot y = x$, cioè ovvero $x + y + x \cdot y$ è un maggiorante

2) $x + y + x \cdot y$ è il più piccolo dei maggioranti, infatti:
Preso $z \in a$ tale che $x \, p \, z$ e $y \, p \, z$ ho che $x \cdot z = x$ e $y \cdot z = y$. Di conseguenza avrò che
$(x + y + x \cdot y) \cdot z = x \cdot z + y \cdot z + x \cdot y \cdot z = x + y + x \cdot y$, cioè vale
$(x + y + x \cdot y) \, p \, z$, ovvero $x + y + x \cdot y$ è il più piccolo dei maggioranti

• (a, ρ) è limitato?

↳ Preso $x \in a$, vale che $0 \cdot x = 0$, cioè vale $0 \rho x$, cioè 0 è il minimo di (a, ρ)

↳ Preso $x \in a$, vale che $x \cdot 1 = x$, cioè vale $x \rho 1$, cioè 1 è il massimo di (a, ρ)

• (a, ρ) è distributivo?

↳ Presi $x, y, z \in a$, vogliamo dimostrare che:

$x \wedge_\rho (y \vee_\rho z) = (x \wedge_\rho y) \vee_\rho (x \wedge_\rho z)$ AND $x \vee_\rho (y \wedge_\rho z) = (x \vee_\rho y) \wedge_\rho (x \vee_\rho z)$

↳ $(x \wedge_\rho y) \vee_\rho (x \wedge_\rho z) = (x \cdot y) \vee_\rho (x \cdot z) = xy + x^2yz + xz =$ $x^2 = x$ IN ANELLO BOOLEANO

$= xy + xyz + xz = x \cdot (y + yz + z) = x \wedge_\rho (y + yz + z) = x \wedge_\rho (y \vee_\rho z)$

↳ STESSO PROCEDIMENTO PER LIMITATO

• (a, ρ) è complementato?

Se $x \in a$, vale che $x \wedge_\rho (1 + x) = x(1 + x) = x + x^2 = x + x = 0$

vale che $x \vee_\rho (1 + x) = x + 1 + x + 0 = 1$

Quindi $x + 1 = x'$ → È il complemento di x

• Abbiamo così dimostrato che dall'anello booleano si può passare a un reticolo booleano.

RETICOLO BOOLEANO → ANELLO BOOLEANO

(←) Dimostriamo 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 ESSERE UN ANELLO HO BISOGNO DELL'ELEMENTO NEUTRO DELLA SOMMA E DEL PRODOTTO

• Definisco $x + y = (x \wedge_\rho y') \vee_\rho (x' \wedge_\rho y)$ e $x \cdot y = x \wedge_\rho y$

Dimostro che $(S, +, \cdot)$ è un anello booleano → UN ANELLO UNITARIO E CHE: $(\forall x \in S)(x^2 = x)$

• ASSOCIATIVITÀ:

1) DI $\cdot$: $x(y \cdot z) = x \wedge (y \wedge z) = (x \wedge y) \wedge z = (x \cdot y) \cdot z$

2) DI $+$: PROCEDIMENTO ANALOGO MA MOLTO LUNGO. SARÀ TRA GLI ESERCIZI DELLA LEZIONE 29

• COMMUTATIVITÀ DI $+$: COMMUTATIVITÀ DI $\wedge$ E $\vee$

$x + y = (x \wedge y') \vee (x' \wedge y) = (y' \wedge x) \vee (y \wedge x') = (y \wedge x') \vee (y' \wedge x) = y + x$

COMMUTATIVITÀ DI $\cdot$:
$x \cdot y = x \wedge_p y = y \wedge_p x = y \cdot x$

DISTRIBUTIVITÀ DI $\cdot$ SI DIMOSTRA TRAMITE CALCOLI, NEGLI ESERCIZI DELLA LEZIONE 29

MINIMO E MASSIMO: Definiamo $m = \min(S)$ e $M = \max(S)$
$x + m = (x \wedge m') \vee (x' \wedge m) = (x \wedge M) \vee (x' \wedge m) = x \vee m = x \rightarrow m = 0_S$
$x \cdot M = x \wedge M = x \rightarrow M = 1_S \rightarrow$ L'UNITÀ DEL $\cdot$ È IL MASSIMO

L'UNITÀ DEL $+$ È IL MINIMO

ANELLO BOOLEANO: $x^2 = x \cdot x = x \wedge_p x = x$

Abbiamo così dimostrato che anello booleano, reticolo booleano e algebra di Boole sono strutture equivalenti
↳ ANCHE GLI ISOMORFISMI SONO EQUIVALENTI

ESEMPIO:
Sia $S \neq \emptyset$ e consideriamo il reticolo booleano $(\mathcal{P}(S), \subseteq)$. Questo reticolo è corrispondente all'algebra di Boole $(\mathcal{P}(S), \cap, \cup, ')$
↳ SAREBBE $S \setminus$
S MENO QUALCOSA

$\downarrow$

$(\mathcal{P}(S), \subseteq) \longleftrightarrow (\mathcal{P}(S), \cap, \cup, ')$

Preso $X, Y \in \mathcal{P}(S)$, $x \cdot y = x \cap y \rightarrow$ DATO CHE $x \cdot y = x \wedge_p y$

$$x + y = (x \cap S \setminus y) \cup (y \cap S \setminus x) = (x \setminus y) \cup (y \setminus x) =$$
$$= x \Delta y$$

Quindi l'anello booleano associato è $(\mathcal{P}(S), \Delta, \cap)$

TEOREMA DI STONE

Sia $a \neq \emptyset$ e $(a, +, \cdot)$ anello booleano.
Allora, esiste $S \neq \emptyset$ tale che:
$(a, +, \cdot) \simeq (\mathcal{P}(S), \Delta, \cap)$ ↳ TUTTI GLI ANELLI BOOLEANI SONO ISOMORFI A $(\mathcal{P}(S), \Delta, \cap)$
↳ Inoltre, se a è finito, potrò scegliere S finito non vuoto tale che $(a, +, \cdot) \simeq (\mathcal{P}(S), \Delta, \cap)$

Il teorema di Stone si applica allo stesso modo per i reticoli booleani con almeno 2 elementi,
↳ sono tutti isomorfi a $(\mathcal{P}(S), \subseteq)$

PER PASSARE DALL'ANELLO AL RETICOLO, MA IN REALTÀ IL TEOREMA NASCE ANCHE SE IL RETICOLO NON ...

NO DIM

COROLLARI DEL TEOREMA DI STONE

1) Se $(a, +, \cdot)$ è un anello booleano e $|a| = m$ dove $m \in \mathbb{N}_2$ → $m \in \mathbb{N}$ e $m \geq 2$ 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 $(\mathcal{P}(S), \Delta, \cap)$, dato che $|\mathcal{P}(S)| = 2^m$ allora anche l'anello booleano ha $|a| = 2^m$ perché vi è un'applicazione biettiva

2) Se (a, p) è un reticolo booleano e $|a| = m$ dove $m \in \mathbb{N}_1$ → $m \in \mathbb{N}$ e $m \geq 1$

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 $(\mathcal{P}(S), \Delta, \cap)$

ALGEBRE DI BOOLE E FUNZIONI CARATTERISTICHE

PER RICORDARE:

- $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z} = \{\underset{\text{PARI}}{[0]_2}, \underset{\text{DISPARI}}{[1]_2}\}$
- $x \equiv_2 0 \longleftrightarrow (\exists k \in \mathbb{Z})(x - 0 = 2k)$
- FUNZIONE CARATTERISTICA: Dato $t \subseteq S$, $\chi_{t,S} : x \in S \mapsto \begin{cases} 0 & \text{se } x \notin t \\ 1 & \text{se } x \in t \end{cases}$

INSIEME DELLE STRINGHE CON 0 E 1

Considerato $m \in \mathbb{N} \setminus \{0\}$, definisco $a = \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{\text{PRODOTTO CARTESIANO } m \text{ VOLTE}} \approx$

$\approx$ stringhe di "0" e "1" di lunghezza m

ESEMPIO:

- $m = 3$ → LA TERNA

$([0]_2, [0]_2, [1]_2) \in a$

$\equiv$

$(0, 0, 1) \in a \approx 001 \in a$ POSSO VEDERLA COME

SOMMA PUNTUALE E MOLTIPLICAZIONE PUNTUALE

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:

- $([0]_2, [0]_2, [1]_2) + ([1]_2, [1]_2, [0]_2) = (1, 1, 1)$
- $(1, 1) + (1, 1) = (0, 0)$
- $11 + 10 = 01$
- $11 \cdot 10 = 10$

FUNZIONE CARATTERISTICA E STRINGHE

Prendo l'insieme S tale che $|S| = m$ con $m > 0$

Dato $t \subseteq S$ ho che:

$$\underset{\text{chi}}{\chi_{t,s}} : x \in S \longmapsto \begin{cases} 0 & \text{se } x \notin t \\ 1 & \text{se } x \in t \end{cases}$$

Dunque $\chi_{t,s} \in \{0,1\}^s \approx a$ (stringhe)

ESEMPIO:

$S = \{1, 2, 3, 4, 5\}$ e $t = \{1, 3, 4\}$

$$\begin{array}{ccccc} \chi_{t,s} \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 0 & 1 & 1 & 0 \end{array}$$

Quindi ogni funzione caratteristica possiamo vederla come una stringa di "1" e "0" lunga m elementi

↳ $\chi_{t,s} = 10110$ ↳ ALL'IMMAGINE DEL PRIMO ELEMENTO DI LA PRIMA POSIZIONE, ALL'IMMAGINE DEL SECONDO LA SECONDA POSIZIONE ECC.

TEOREMA

Sia $n \in \mathbb{N} \setminus \{0\}$ e $S = \{1, 2, \dots, n\}$

Allora $\varphi : t \in \mathcal{P}(S) \longmapsto \chi_{t,S} \in \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}_{n \text{ VOLTE}}$ è un isomorfismo tra:

$(\mathcal{P}(S), \Delta, \cap)$ e $(\overbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}^{n \text{ volte}}, +, \cdot)$ con $+$ e $\cdot$ somma e prodotto puntuale PUNTUALI

NO DIM

OPERAZIONI BIT A BIT (BIT-BY-BIT)

ESEMPI:

Se vediamo le operazioni (puntuali) come operazioni su $\mathcal{P}(S)$ abbiamo ora:

SOMMA: Si comporta come lo XOR o differenza simmetrica

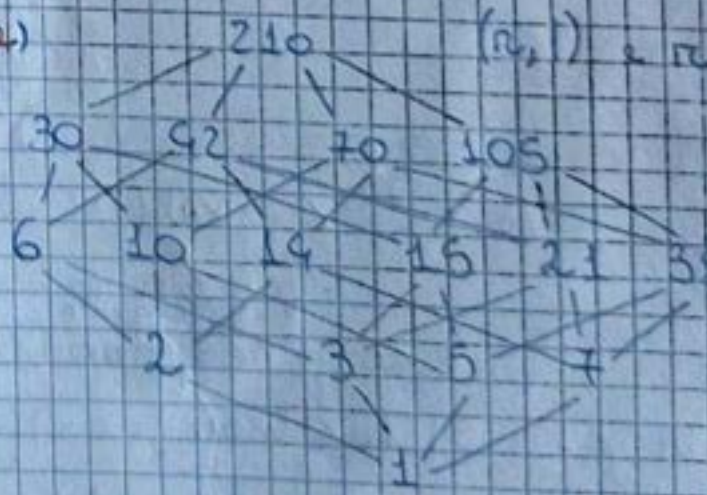
$$\begin{array}{r} 0011 + \\ 0101 = \\ \hline 0110 \end{array}$$

MOLTIPLICAZIONE. Si comporta come l'AND o l'intersezione

$$\begin{array}{r} 0011 \cdot \\ 0101 = \\ \hline 0001 \end{array}$$

Correzione esercizi 30/11/2021 (LEZIONE 29)

4. a) $(R, |)$ e $R = \{n \in \mathbb{N} \setminus \{0\} \mid n | 210\}$



b) $\max(R) = 210$
$\min(R) = 1$

c) $2 \wedge 6 = 2$
$2 \vee 7 = 14$
$7' = 30$

e) $6 + 10 = (6 \wedge 10) \vee (6' \wedge 10) =$
$= (6 \wedge 21) \vee (35 \wedge 10) =$
$= 3 \vee 5 = 15$

DIVISIBILITÀ

Sia $(S, \cdot)$ un semigruppo commutativo. Prendo $x, y \in S$.

x divide y $(x|y)$ se:

$(\exists z \in S)(y = xz)$

L'INSIEME DEI DIVISORI DI X

L'insieme dei divisori di $x \in S$ lo indico con $DIV_S(x)$.

$DIV_S(x) = \{y \in S \mid y|x\}$

L'INSIEME DEI MULTIPLI DI X

L'insieme dei multipli di $x \in S$ lo indico con $MULT_S(x)$.

$MULT_S(x) = \{y \in S \mid x|y\}$

ELEMENTO ASSOCIATO

↳ PER ESEMPIO, IN $\mathbb{Z}$ HO CHE $-5 \in S$ SONO ASSOCIATI PERCHÉ $5|-5$ E $-5|5$ MA $-5 \neq 5$

x e y appartenenti ad S si dicono associati se:

$x \in DIV_S(y)$ e $y \in DIV_S(x)$ ↳ CIOÈ x E y SI DIVIDONO A VICENDA

↳ NON POSSO FARLO SE NON HO L'UNITÀ

L'INSIEME DEGLI ASSOCIATI A X

L'insieme degli elementi associati di x lo indico con $ASSOC_S(x)$

TEOREMA

SE TUTTI GLI ELEMENTI DI X SONO CANCELLABILI ALLORA QUESTA COSA VALE PER TUTTI GLI ELEM.

Sia $(S, \cdot)$ un monoide commutativo.

Se x è cancellabile, $ASSOC_S(x) = \{x \cdot u \mid u \in U(S)\}$*

IL PRODOTTO TRA X E UN ELEMENTO INVERTIBILE

GLI INVERTI.

* Scritto come FBF:

$ASSOC_S(x) = \{x \cdot u \mid u \in U(S)\} = \{y \in S \mid (\exists u \in U(S))(y = x \cdot u)\}$

$u \in U(S) \longleftrightarrow (\exists v \in S)(v * u = 1_S$ AND $u * v = 1_S)$

DIM

$3|3\cdot 4$ $\quad$ $4\cdot 3\cdot \frac{1}{3}=4$

(⊇) Sia $u \in U(S)$. Allora $x | x\cdot u$, ma $(x\cdot u)u^{-1}=x$.
Dunque $x\cdot u | x$. Quindi dato che $x\cdot u \in DIV_S(x)$
e $x \in DIV_S(x\cdot u)$ allora $x\cdot u \in ASSOC_S(x)$

(⊆) Considero $y \in ASSOC_S(x)$, ovvero $x|y$ e $y|x$.
Allora ci sono $w, z \in S$ tali che $y = x\,w$ e $x = y\cdot z$
↳ Di conseguenza $x = x\cdot w\cdot z$, ma dato che
x è cancellabile allora $w\cdot z = 1$. → SIAMO IN UN MONOIDE
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:
$y \in ASSOC(x) \overset{1}{\longleftrightarrow} DIV(x) = DIV(y) \overset{2}{\longleftrightarrow} MULT(x) = MULT(y)$

DIM

1. (→) Per definizione, $y \in ASSOC(x) \longleftrightarrow x \in DIV(y)$ e $y \in DIV(x)$
Ma allora tutti i divisori di x dividono anche y e
tutti i divisori di y dividono anche x.
Cioè per la transitività di "|", $y \in ASSOC(x) \to DIV(x) = DIV(y)$
(←) Dato che $(S,\cdot)$ è un monoide allora
$y \in DIV(y)$. Di conseguenza $y \in DIV(x)$ → DIV(x)=DIV(y) per ipotesi
Stessa cosa vale per x, dunque $y \in ASSOC(x)$

2. (↔) Ogni divisore di x è divisore di y e viceversa.
Se prendo $z \in MULT(x)$, z sarà del tipo
$z = x\cdot k$. Ma $y|x$, quindi $x = y\cdot h$. Ciò significa
che $z = y\cdot h\cdot k$, ovvero $z \in MULT(y)$. Stesso ragionamento
al contrario per l'altro verso.

MASSIMO COMUN DIVISORE

Sia $(S, \cdot)$ un monoide commutativo e $t \subseteq S$

$$MCD_S(t) = \{d \in \bigcap_{x \in t} DIV_S(x) \mid (\forall z \in \bigcap_{x \in t} DIV_S(x))(z \mid d)\}$$

↳ insieme dei divisori comuni di $x \in t$

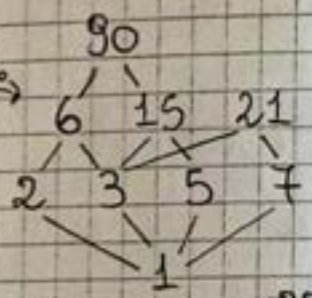
↳ devono essere comuni divisori quindi appartenendo all'intersezione di tutti i divisori di x

↳ soltanto d deve essere diviso da tutti gli altri divisori comuni

ESEMPIO:

Quando vado a fare il MCD, io voglio trovare il massimo dei divisori comuni (cioè il più grande valore che ha come multipli gli elementi di t), ovvero il massimo dei minoranti (l'inf) nella relazione di divisione.

- Se ho $S = \{1, 2, 3, 5, 6, 7, 15, 21, 90\}$



Con $t = \{90\}$, l'inf è 90

Con $t = \{90, 3\}$, l'inf è 3

Con $t = \{90, 7\}$, l'inf è 1 → È IL PIÙ GRANDE DEI DIVISORI COMUNI

In questo caso "|" è una relazione d'ordine

- 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 $\{-5, 1, 5\}$ → CHI È IL SUP DEI MINORANTI? ($DIV(10) \cap DIV(15)$)

↳ Voglio trovare i divisori di 10 e 15 che siano 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

$S = \{-5, 1, 5, 10, 15\}$

$$MCD_S(\{10, 15\}) = MCD_S(10, 15) = \overset{MCD}{\{-5, 5\}} \subseteq \overset{\text{I DIVISORI COMUNI}}{\{-5, 1, 5\}}$$

(PRODOTTI O SUCCESSIVI)

↳ VEDREMO CHE SONO TUTTI E SOLI GLI ASSOCIATI A UN MASSIMO COMUNE DIVISORE

↳ TUTTI E SOLI GLI ASSOCIATI A 5 SONO 5 PER GLI INVERTIBILI (IN $\mathbb{Z}$ SONO -1 E 1)

$-5 \mid 5$ E $5 \mid -5$ MA $5 \nmid -5$

↳ NON È ASIMMETRICO

MINIMO COMUNE MULTIPLO (mcm)

Sia $(S,\cdot)$ un monoide commutativo $t \subseteq S$

$$mcm_S(t) = \left\{ d \in \bigcap_{x \in t} MULT_S(x) \;\middle|\; \left(\forall z \in \bigcap_{x \in t} MULT_S(x)\right)\left(d \mid z\right) \right\}$$

DEVE ESSERE QUELLO CHE DIVIDE TUTTI GLI ALTRI MULTIPLI

ESEMPIO:

- In $\{-5, 1, 5, 10, 15\}$

$mcm(1) = \{1\}$

$mcm(5) = \{-5, 5\}$ → I MULTIPLI DI 5 SONO 5, -5, 10, 15 → PRENDO I MINIMI

MULTIPLI IN $\mathbb{Q}$

Notiamo che in $(\mathbb{Q}, \cdot)$, $MULT_{\mathbb{Q}}(3) = \mathbb{Q}$

↳ Ad esempio, $1 : \frac{1}{3} = 3$, quindi tutti i numeri sono multipli di 3 → 1 È MULTIPLO DI 3

Di conseguenza $mcm_{\mathbb{Q}}$ è inutile perché tutti sono multipli di tutti

DIVISORI BANALI

Sia $(S,\cdot)$ un monoide commutativo e sia $x \in S$. L'insieme dei divisori banali, che indico con $BDIV_S(x)$, è uguale a:

$$BDIV_S(x) = \underbrace{U(S)}_{\text{INVERTIBILI}} \cup \underbrace{ASSOC_S(x)}_{\text{ASSOCIATI DI } x}$$

Li chiamo 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

In $\mathbb{Q}$ tutti sono divisori banali

IRRIDUCIBILE

IN $\mathbb{Z}$ I PRIMI SONO TUTTI E SOLI GLI IRRIDUCIBILI

Sia $(S,\cdot)$ un dominio di integrità e sia $x \in S$, x si dice irriducibile se: $x \notin U(S)$ e $DIV_S(x) = BDIV_S(x)$

NON È INVERTIBILE E TUTTI I DIVISORI SONO QUELLI BANALI

PRIMO

Sia $(S,\cdot)$ un monoide commutativo, e sia $p \in S$, p si dice primo se $(\forall a,b \in S)(p \mid ab \rightarrow p \mid a \vee p \mid b)$

COPRIMI

Se $(S,\cdot)$ un monoide commutativo,

Sia $x, y \in S$, se $1_S \in MCD_S(\{x,y\})$, x e y si dicono coprimi

SE UNO DEI MCD È 1, ALLORA I NUMERI SI DICONO COPRIMI

ESEMPIO: $\rightarrow MCD(\{2,3\}) = \{1,-1\}$

CANCELLATIVI

Un monoide commutativo con tutti elementi cancellabili si dice cancellativo

MONOIDE FATTORIALE

VALE LA FATTORIZZAZIONE PROPRIO COME VALE IN $\mathbb{Z}$ MA NEI MONOIDI

Sia $(m,\cdot)$ un monoide 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 FATTORIALE

Un anello $(a, +, \cdot)$ commutativo unitario si dice fattoriale se $(a \setminus \{0_a\}, \cdot)$ è un monoide fattoriale

↳ BISOGNA TOGLIERE LO ZERO DI a

↳ CHE CE LO 0 IL MONOIDE NON È PROPRIO CANCELLATIVO

ESEMPIO:

- $(\mathbb{N} \setminus \{0\}, \cdot)$
- $(\mathbb{Z} \setminus \{0\}, \cdot)$

↘ SONO MONOIDI FATTORIALI PER IL TEOREMA FONDAMENTALE DELL'ARITMETICA

$(\mathbb{Z}, +, \cdot)$ È UN ANELLO FATTORIALE ANCHE SE C'È LO 0 DATO CHE $(\mathbb{Z} \setminus \{0\}, \cdot)$ È CANCELLATIVO

↳ Non posso scrivere $(\mathbb{Z} \setminus \{0\}, +, \cdot)$ perché altrimenti il $+$ non sarebbe più definito

Correzione esercizi 01/12/2022 (LEZIONE 30)

7. Sia $(S,\cdot)$ un monoide commutativo. Allora
$m \in MCD(x,y) \longleftrightarrow (ASSOC(m) = MCD(x,y))$

DIM

$(\rightarrow)$ $m \in MCD(x,y) \Leftrightarrow$ Per definizione $m|x \wedge m|y \wedge$
$\wedge (\forall z \in S)(z|x \wedge z|y \rightarrow z|m)$

$(\subseteq)$ Considero un $m \in ASSOC(m)$, cioè, per definizione,
$m \in DIV(m)$ e $m \in DIV(m)$, ciò significa che
PER TRANSITIVITÀ DELLA DIVISIBILITÀ $m|x \wedge m|y$ e che $(\forall z \in S)((z|x \wedge z|y \rightarrow z|m) \rightarrow z|m)$ QUINDI m È UN MCD

$(\supseteq)$ Se io prendo un altro massimo comun divisore m', ho che:
PERCHÉ $m' \in MCD(x,y)$ PERCHÉ $m \in MCD(x,y)$
$m' \in MCD(x,y) \rightarrow m|m' \wedge m'|m$ I MASSIMI COMUN DIVISORI SI DIVIDONO TRA LORO
di conseguenza $m' \in ASSOC(m)$

$(\leftarrow)$ $m \in ASSOC(m)$ dato che $(S,\cdot)$ è un monoide, quindi per ipotesi $m \in MCD(x,y)$, dato che per estensionalità $ASSOC(m) = MCD(x,y)$

TEOREMA

Sia $(S,\cdot)$ un monoide commutativo. Allora:
$m \in mcm(x,y) \longleftrightarrow ASSOC(m) = mcm(x,y)$

DIM

La dimostrazione è simile alla precedente
$m \in mcm(x,y) \overset{def}{\Longleftrightarrow} (x|m \wedge y|m) \wedge (\forall z \in S)(x|z \wedge y|z \rightarrow m|z)$

$(\rightarrow)$ $m \in ASSOC(m) \Leftrightarrow m \in DIV(m) \wedge m \in DIV(m)$
Ciò significa che $x|m \wedge y|m \wedge (\forall z \in S)(x|z \wedge y|z \rightarrow m|z) \rightarrow m|z)$ TRANSITIVITÀ
Preso $m' \in mcm(x,y) \rightarrow m'|m \wedge m|m' \rightarrow m \in ASSOC(m)$

$(\leftarrow)$ Essendo $(S,\cdot)$ un monoide, $m \in ASSOC(m)$. Dato che, per ipotesi, $ASSOC(m) = mcm(x,y)$, allora $m \in mcm(x,y)$

TEOREMA

Sia $(m,\cdot)$ un monoide fattoriale. Sia $a \in m \setminus U(m)$, posso scrivere a come prodotto di primi. → CI TROVIAMO IN UN MONOIDE FATTORIALE

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}, \quad \forall k_1, k_2, \ldots, k_m \in \mathbb{N} \text{ e con } p_1, p_2, \ldots, p_m \text{ numeri primi}$$

Notiamo che i divisori di a sono tutti e soli gli associati ad elementi del tipo. → UNO SU ASSOCIATI PERCHÉ IN $\mathbb{Z}$ ABBIAMO ANCHE DIVISORI NEGATIVI

$$p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_m^{l_m} \quad \text{con } 0 \leq l_i \leq k_i \quad \text{e con } 1 \leq i \leq m$$

SE PRENDO UN ESPONENTE MAGGIORE AVRÒ UN DIVISORE DI a

IN UN MONOIDE FATTORIALE $\mathrm{ASSOC}_{\mathbb{Z}}(x) = \{x \cdot u \mid u \in U(\mathbb{Z})\}$

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 $a = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m} \in \mathbb{N}$, allora a ha $m(k_1 + k_2 + \ldots + k_m)$ divisori

↳ SONO TUTTE LE POSSIBILI COMBINAZIONI DI ESPONENTI

↳ GLI ASSOCIATI DI m IN $\mathbb{N}$ È SOLO m PERCHÉ L'UNICO u È 1

COROLLARIO

Se $a = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m} \in \mathbb{Z}$, allora a ha $2m(k_1 + k_2 + \ldots + k_m)$ divisori

↳ ORA DOBBIAMO PRENDERE ANCHE I NUMERI NEGATIVI PERCHÉ IN $\mathbb{Z}$ GLI INVERTIBILI SONO 1 E -1

ESEMPIO:

$6 = 2^1 \cdot 3^1$ IN $\mathbb{N}$ → I divisori di 6 sono $2(1+1) = 4$ ← 1, 2, 3, 6

LA SOMMA DEGLI ESPONENTI

IL NUMERO DI PRIMI

↓

I divisori di 6 in $\mathbb{Z}$ sono:

$2 \cdot 2(1+1) = 8$, infatti $\{n \in \mathbb{Z} \mid n \mid 6\} = \{-1, 1, -2, 2, -3, 3, -6, 6\}$

TEOREMA

NEI MONOIDI FATTORIALI ESISTONO SEMPRE IL mcm E IL MCD

Sia $(m, \cdot)$ un monoide 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:

$$(\forall i \in \mathbb{N})\left(1 \leq i \leq m \rightarrow \underbrace{\alpha_i := MAX(k_i, l_i)}_{\text{E' IL MASSIMO TRA GLI ESPONENTI}} \wedge \underbrace{\beta_i := MIN(k_i, l_i)}_{\text{E' IL MINIMO TRA GLI ESPONENTI}}\right)$$

Allora vale che $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m} \in mcm(a,b)$

e che $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_m^{\beta_m} \in MCD(a,b)$

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:

$a = 2 \cdot 3^2 \cdot 5$ e $b = 3 \cdot 5^2 \cdot 11 \cdot 13$, allora posso riscriverli come $a = 2^1 \cdot 3^2 \cdot 5^1 \cdot 11^0 \cdot 13^0$ e $b = 2^0 \cdot 3 \cdot 5^2 \cdot 11^1 \cdot 13^1$

Avrò che i massimi α saranno:

$\alpha_1 = MAX(1,0) = 1$, $\alpha_2 = MAX(2,1) = 2$, $\alpha_3 = 2$, $\alpha_4 = 1$, $\alpha_5 = 1$

COROLLARIO

Sia $(m, \cdot)$ un monoide 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 $m \in mcm(a,b)$ e $m' \in MCD(a,b)$, allora:

$m \cdot m' \in ASSOC(a,b)$ → QUANDO FACCIO $a \cdot b$ STO SOMMANDO GLI ESPONENTI CHE E' LA STESSA COSA DI SOMMARE IL MASSIMO E IL MINIMO DEGLI ESPONENTI

↳ $a \cdot b = m \cdot m' = p_1^{k_1+l_1} \cdot p_2^{k_2+l_2} \cdots p_m^{k_m+l_m}$

↓ FANNO PARTE DEGLI ASSOCIATI PERCHE' CI PUO' STARE IL −

ESEMPIO:

$a = 2^2 \cdot 3 \cdot 5^0 \rightarrow 12$ e $b = 2 \cdot 5 \cdot 3^0 \rightarrow 10$

mcm: $2^2 \cdot 3 \cdot 5 \in mcm(a,b)$

MCD: $2 \in MCD(a,b)$

$a \cdot b = 2^3 \cdot 3 \cdot 5$

$m \cdot m' = 2^3 \cdot 3 \cdot 5$

$a \cdot b = m \cdot m'$

↓

$m' = \frac{a \cdot b}{m}$ → DAL MCD TROVO IL mcm VICEVERSA

TEOREMA

Se $(a,+,\cdot)$ è un anello commutativo unitario, siano $b,c \in a$ e $d \in DIV_{(a,\cdot)}(b) \cap DIV_{(a,\cdot)}(c)$ → d APPARTIENE AI DIVISORI COMUNI

Allora $(\forall x,y \in a)(d \mid (x\cdot b + y\cdot c))$ → UN DIVISORE COMUNE DI b E C DIVIDE QUALUNQUE COMBINAZIONE DI b E DI C

$b = d\cdot k$, $c = d\cdot h$, METTO IN EVIDENZA d (PER LA DISTRIBUTIVA) E HO CHE $b+c = d(k+h)$, CIOÈ $d \mid (b+c)(k+h)$, CIOÈ $d \mid ((k+h)\cdot b + (k+h)\cdot c)$

VALORE ASSOLUTO

È una funzione $\mathbb{Z} \to \mathbb{N}$ e t.c.:

$|m| = m$ se $m \in \mathbb{N}$

$|m| = -m$ se $m \in \mathbb{Z} \setminus \mathbb{N}$

TEOREMA DELLA DIVISIONE EUCLIDEA (O CON RESTO)

$$(\forall m,n \in \mathbb{Z})(m \neq 0 \to (\exists!(q,r) \in \mathbb{Z}\times\mathbb{N})(n = mq + r \wedge 0 \leq r < |m|))$$

→ NON POSSO DIVIDERE NULLA (TRANNE 0) PER 0

ESEMPIO: • 98 | 13
91 | 7
7

Quindi $98 = 13\cdot 7 + 7$

→ E, INFATTI, $0 \leq 7 < 13$
LA COPPIA È $(13,7)$

DIM → USIAMO L'INDUZIONE DI SECONDA FORMA SU m

• Suppongo $m \geq 0$.

• Se $m = 0$, scelgo $q = 0$ e $r = 0$ → BASE DI INDUZIONE → $0 = 0 \wedge 0 \leq 0 < 0$ ✓

• Se $m = |m|$ allora:

Se $m = m$, $q = 1$ e $r = 0$

Se $m = -m$, $q = -1$ e $r = 0$

• Suppongo che $0 < m < |m|$. Posso scegliere $q = 0$ e $r = m$

• Suppongo $|m| < m$ → DATO CHE PER IPOTESI $|m| \neq 0$

Allora $n - |m| < n$ → DATO CHE HO SUPPOSTO VERO L'ASSERTO $\forall x < n$ → Per ipotesi di induzione, allora

$n - |m| = mq_1 + r_1$ con $0 \leq r_1 < |m|$

Di conseguenza vale che $n = mq_1 + |m| + r_1$

• Visto che $m = mq_1 + |m| + r_1$,

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, l'asserto vale $\forall m \in \mathbb{N}$

• Per i numeri negativi, invece:

Suppongo $m \in \mathbb{Z} \setminus \mathbb{N}$.

ESSENDO $-m$ POSITIVO E AVENDO APPENA DIMOSTRATO L'ASSERTO $\forall m \in \mathbb{N}$

• Vale che $-m = mq_1 + r_1$ con $0 \leq r_1 < |m|$

NON VA BENE PERCHE' NON E' COMPRESO TRA 0 E $|m|$

Di conseguenza $m = m(-q_1) - r_1$, ma $-r_1 \leq 0$

Posso aggiungere e sottrarre $|m|$, quindi avrò che:

$$m = m(-q_1) \underbrace{- r_1 + |m|}_{\text{QUESTA PARTE E' SEMPRE POSITIVA E } < |m|} - |m|$$

• Allora, se $r_1 \neq 0$;

Se $m > 0$, scelgo $q = -q_1 - m$, e $r = m - r_1 < |m|$

Se $m < 0$, scelgo $q = -q_1 + m$, e $r = -m - r_1 < |m|$

• Se $r_1 = 0$, allora va bene avere $m = m(-q_1)$

PER DIMOSTRARE L'UNICITÀ DELLA COPPIA IN $\exists!(q, r) \in \mathbb{Z} \times \mathbb{N}$

• Consideriamo due coppie $(q_1, r_1), (q_2, r_2) \in (\mathbb{Z}, \mathbb{N})$

con $0 \leq \underbrace{r_1 \leq r_2}_{\text{LO SUPPONGO IO}} < |m|$ e $m = mq_1 + r_1$ e $m = mq_2 + r_2$

↳ 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 $|m| \cdot |q_1 - q_2| = |m(q_1 - q_2)| = |r_2 - r_1| < |m|$

Da ciò segue che $\underbrace{q_1 = q_2}_{}$, di conseguenza $r_1 = r_2$

NON POSSO AVERE $|m| \cdot |q_1 - q_2| < |m|$ SE $|q_2 - q_1| \neq 0$

COROLLARIO (FUNZIONE DE(m,n))

Visto che la coppia è unica, posso scrivere una funzione che per ogni coppia (m,n) associa quell'unica coppia

$$DE(m,n) = (q,r)$$

ALGORITMO DELLE DIVISIONI SUCCESSIVE

VOGLIAMO TROVARE IL MCD TRA DUE NUMERI
↓
APPLICO TANTE VOLTE IL TEOREMA DELLA DIVISIONE EUCLIDEA

ESEMPIO:

- MCD(12, 15) , $15 = 12 \cdot 1 + 3$
  $12 = 3 \cdot 4 + 0$

  NON RIESCO A CALCOLARLO IN N E POI METTO L'INVERSO

  MI FERMO CON R=0 E PRENDO IL RESTO CHE STA PRIMA, INFATTI 3|12 E 3|15, MCD=3

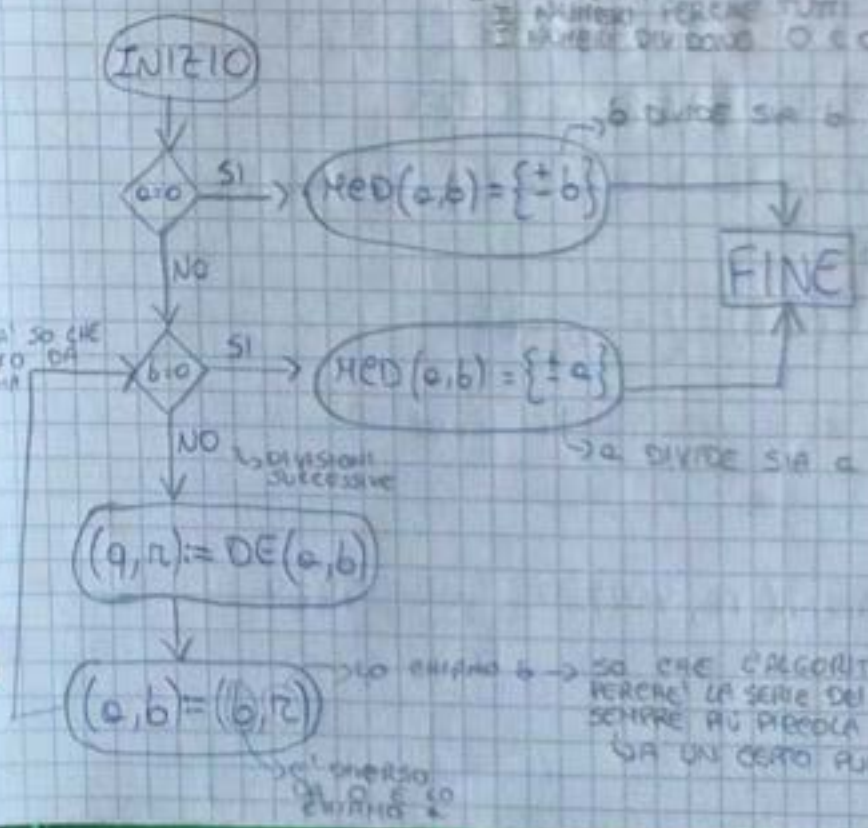
- MCD(111, 17) , $111 = 17 \cdot 6 + 9$ → $111 \mid 111$
  $17 = 9 \cdot 1 + 8$ → $17 \mid 17$
  $9 = 8 \cdot 1 + 1$ → $1 \mid 9$
  $8 = 1 \cdot 8 + 0$ → $1 \mid 8$

  POSSO RISALIRE PER TUTTA LA STRADA

IN GENERALE:

MCD(a,b) con $(a,b) \neq (0,0)$ e $a,b \in \mathbb{N}$

↳ IL MCD(0,0) SONO TUTTI I NUMERI, PERCHÉ TUTTI I NUMERI DIVIDONO 0 E 0



Correzione esercizi 03/12/2021 (LEZIONE 31)

3,4) d) MCD(1111231, 111123)

PUNTO 4 $1111231 = 10 \cdot 111123 + 1 \rightarrow MCD(1111231, 111123) = 1$

$MCD = 1 = 1112311 + 111123 \cdot (-10)$

ALGORITMO DELLE DIVISIONI SUCCESSIVE

$a, b \in \mathbb{N}$

PER $a, b \in \mathbb{Z}$ RICAVIAMO IL MCD ANCHE NEGATIVO

$a = bq_1 + r_1$

$b = r_1 q_2 + r_2$

$r_1 = r_2 q_3 + r_3$

$\vdots$

$r_{t-4} = r_{t-3} \cdot q_{t-2} + r_{t-2}$

$r_{t-3} = r_{t-2} \cdot q_{t-1} + r_{t-1}$

$r_{t-2} = r_{t-1} \cdot q_t + 0 \rightarrow r_t$

$0 = r_t < r_{t-1} < \dots < r_2 < r_1 < b$

a) MCD(72, 402) = 6

$72 = 402 \cdot 0 + 72$

$402 = 72 \cdot 5 + 42$

$72 = 42 \cdot 1 + 30$

$42 = 30 \cdot 1 + 12$

$30 = 12 \cdot 2 + 6$

$12 = 6 \cdot 2 + 0$

SE IL PRIMO È MINORE DEL SECONDO POSSIAMO FARE QUESTO PASSAGGIO IN MODO IMPLICITO

PUNTO 4

DATO CHE SO $42 = 30 \cdot 1 + 12$

TECNICA DI RECUPERO

$6 = 30 - 12 \cdot 2 = 30 - (42 - 30) \cdot 2 =$

$= (72 - 42) - (42 - (72 - 42)) \cdot 2 =$ METTO IN EVIDENZA IL 30

$= 30 + 30 \cdot 2 - 42 \cdot 2 = 30 \cdot 3 - 42 \cdot 2 =$ SCRIVO 30 COME 72 - 42

$= (72 - 42) \cdot 3 - 42 \cdot 2 = 72 \cdot 3 - 42 \cdot 5 =$

$= 72 \cdot 3 - (402 - 72 \cdot 5) \cdot 5 = 402 \cdot (-5) + 72 \cdot 28$

PARTICOLARITÀ

$m \cdot M \in ASSOC(a, b) = \{-ab, ab\}$

$m = \frac{ab}{M}$ SE HO TROVATO M, OVVERO IL MCD, POSSO TROVARE ANCHE IL mcm

Quindi, $mcm(72, 402) = \frac{72 \cdot 402}{6} = 4824$

TEOREMA DI BEZOUT

INSIEME ALL'ALGORITMO DELLE DIVISIONI SUCCESSIVE FA ALGORITMO DELLE DIVISIONI SUCCESSIVE ESTESO

Presa la coppia $(a,b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0,0)\}$ ho che:

$$(\forall (a,b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0,0)\})((\forall d \in MCD(a,b))((\exists u,v \in \mathbb{Z})(d = au + bv)))$$

↳ qualunque sia la coppia e qualunque sia il MCD (a,b), il MCD lo posso scrivere come combinazione lineare di a e b

DIM (INDUZIONE DI SECONDA FORMA SU t)

Sia 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 stesso. Quindi:

  $b \in MCD(a,b)$ e $b = a \cdot 0 + b \cdot 1$ ok

- Se $t = 2$, $r_1 \neq 0$ e $r_2 = 0$

  Allora il MCD è r_1. Quindi:

  $r_1 \in MCD(a,b)$, quindi posso scrivere $r_1 = a \cdot 1 + b(-q_1)$ ok

⋮

- Suppongo vero l'asserto per i r_i con $1 \leq i < t$ → I RESTI MINORI DI t

  ↳ visto che $t > 1$, implica che esiste r_{t-1}.

  In particolare, $r_{t-1} \in MCD(a,b)$

  posso scrivere

  $r_{t-1} = r_{t-3} + r_{t-2} \cdot (-q_{t-1})$

  → STIAMO PROCEDENDO PER INDUZIONE DI SECONDA FORMA PER NON LA FACCIAMO DI MODO MEN RISCHIOSO PERCHÉ NON SO

Tuttavia per ipotesi di induzione $\exists u, v, w, x \in \mathbb{Z}$ tali che $r_{t-3} = au + bv$ AND $r_{t-2} = aw + bx$

Quindi avremo che:

$$r_{t-1} = r_{t-3} + r_{t-2}(-q_{t-1}) = au + bv + (aw + bx)(-q_{t-1}) =$$
$$= a(u - w q_{t-1}) + b(v - x \cdot q_{t-1})$$

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

Siano $a, b, c \in \mathbb{Z}$.

Siano a, b coprimi. → CIOÈ IL MCD IN $\mathbb{Z} = \{-1, +1\}$

Allora, se $a | b \cdot c$, allora $a | c$

ESEMPIO:
SE $a = 3$ E $b = 5$ E $a | 30 \to a | 5 \cdot 6$, ALLORA $a | 6$

DIM

a, b sono coprimi, quindi $1 \in MCD(a, b)$.

Per il teorema di Bezout, trovo $u, v \in \mathbb{Z}$ tale che:

$$1 = au + bv$$

Moltiplico tutto per c e avrò che:

$$c = \underbrace{c \cdot a}_{a|} u + \underbrace{b \cdot c}_{a|} v$$

→ SE $x = c \cdot a$ E $y = b \cdot c$, HO CHE $a \in DIV(x) \cap DIV(y)$ E PER IL TEOREMA PRIMA DEL VALORE ASSOLUTO ALLORA $a | x \cdot u + y \cdot v$, CIOÈ $a | c$

Quindi $a | c$

TEOREMA

→ NUMERI PRIMI

DIMOSTRARE PRIMA QUESTO TEOREMA CI PERMETTE DI 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

→ QUELLI I CUI DIVISORI SONO TUTTI E SOLI QUELLI BANALI

DIM

($\to$) Sia p un numero primo

→ VOGLIAMO DIMOSTRARE CHE p È IRRIDUCIBILE

Siano $a, b \in \mathbb{Z}$ tali che:

$$p = a \cdot b$$

Per ipotesi $p | a \vee p | b$.

Suppongo che $p | a$, cioè:

$p \in DIV(a)$

→ DATO CHE $a | a \cdot b$

Ma vale anche che $a \in DIV(p)$, quindi:

$p \in ASSOC(a) = \{a, -a\}$ → Quindi $p = a \vee p = -a$

→ IN UN MONOIDE COMMUTATIVO $ASSOC(a) = \{x \cdot u \mid u \in U(\mathbb{Z})\}$ MA IN $\mathbb{Z}$, GLI UNICI INVERTIBILI SONO 1 E -1

Segue che $b = 1 \vee b = -1$, quindi p ha solo divisori banali → p è irriducibile

($\Leftarrow$) Sia p irriducibile, cioè $DIV(p) = \{-1, 1, p, -p\}$

Suppongo che $p | ab$ → posso far vedere che $p | a \vee p | b$

Suppongo anche che $p \nmid a$

↳ Visto che $p \nmid a$ e dato che $MCD(p,a) \subseteq DIV(p)$, vuol dire che in $MCD(p,a)$ non ci sono p e $-p$

ALTRIMENTI AVREMMO CHE $p | a$, MA PER IPOTESI $p \nmid a$

Quindi $MCD(p,a) \subseteq (DIV(p) \setminus \{-p, p\})$, cioè $1 \in MCD(p,a)$, cioè p e a sono coprimi

↳ Per il lemma di Euclide, $p | b$

CONGRUENZE MODULO m (con m INTERO)

Preso un $m \in \mathbb{Z}$, definisco che:

$(\forall a, b \in \mathbb{Z})(a \equiv_m b :\Longleftrightarrow m | (a-b))$ → $a \equiv_0 b \Leftrightarrow a = b$ PERCHÉ 0 DIVIDE SOLO 0

SAPPIAMO CHE:

$\equiv_m$ è una relazione di equivalenza

$[a]_{\equiv_m} =: [a]_m$

$[0]_2 = [19]_2$ → DATO CHE $2 | (19-0)$

$\mathbb{Z}_m := \mathbb{Z}/_{\equiv_m}$ e inoltre, $\mathbb{Z}_{(m)} = \mathbb{Z}_{(-m)}$ → INFATTI SE $m | (a-b)$, È OVVIO CHE $-m | (a-b)$

↓ SPESSO CONSIDERIAMO SOLO LE CLASSI DI CONGRUENZA POSITIVE (QUELLE NEGATIVE SONO UGUALI)

$\mathbb{Z}_2 = \{\underset{\text{PARI}}{[0]_2}, \underset{\text{DISPARI}}{[1]_2}\}$

COME POSSO SCRIVERE $[a]_m$ COME INSIEME?

Sappiamo che, preso $b \in \mathbb{Z}$ tale che $m | (a-b)$, $b = a + km$.

$[a]_m = \{b \in \mathbb{Z} \mid m | (a-b)\}$, quindi posso riscrivere $[a]_m$

$[a]_m := \{a + km \mid k \in \mathbb{Z}\}$

↳ TUTTI GLI ELEMENTI IN RELAZIONE $\equiv_m$ CON a

↓

$[0]_2 = \{0 + k \cdot 2 \mid k \in \mathbb{Z}\}$

$[1]_2 = \{1 + k \cdot 2 \mid k \in \mathbb{Z}\}$

ARITMETICA → È UN FUNTORE $\mathbb{Z}/\mathbb{Z}$

OPERAZIONE (PARZIALE) MOD

$$(\forall (a,m) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))(a \text{ MOD } m := \text{MIN}([a]_m \cap \mathbb{N}))$$

↳ IL PIÙ PICCOLO NELLA CLASSE DI EQUIVALENZA

ESEMPIO:

$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ → INFATTI $[3]_3 = [0]_3$ DATO CHE IN $[x]_3$ HO $x+3k$

↳ $[3]_3$ HO $3+3k$ CHE POSSO AVERE ANCHE IN $[0]_3$ CON $0+3(2k)$

- $0 \text{ MOD } 3 = 0$
- $\text{ MOD } 3 = 1$
- $2 \text{ MOD } 3 = 2$
- $3 \text{ MOD } 3 = 0$

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 $r = a + (-q)m$, CIOÈ $r \in [a]_m$ 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 $|\mathbb{Z}_m| = m$

↳ ORDINE DI $\mathbb{Z}_m$

DIM

- Sia $a \in \mathbb{Z}$.

DE$(a,m) = (q,r)$, cioè $a = qm + r$ e $0 \leq r < |m|$, quindi $[a]_m = [r]_m$ → QUALUNQUE NUMERO IO PRENDA, POSSO TROVARE UN RAPPRESENTANTE DELLA CLASSE CHE È UN RESTO DEL NUMERO

STESSO RAGIONAMENTO DI PRIMA*

Cioè ho fatto vedere che $\mathbb{Z}_m \subseteq \{[0]_m, [1]_m, \dots, [m-1]_m\}$.

QUALUNQUE SIA a, LA SUA CLASSE È UGUALE A UNO DI QUESTI

- Siano $0 \leq i \leq j < |m|$ e $[i]_m = [j]_m$ → VOGLIAMO DIMOSTRARE CHE TUTTE QUELLE CLASSI SONO DISTINTE, QUINDI GLI i E j DEVONO ESSERE UGUALI SE $[i]_m = [j]_m$

↳ Dato che $0 \leq i \leq j < |m|$, segue che $0 \leq j - i < m$

↳ Visto che $[i]_m = [j]_m$, allora $(\exists k \in \mathbb{Z})(j = i + k \cdot m)$

Quindi $j - i$ è un multiplo di m $\xrightarrow{\text{non che } j-i<m}$ $j - i = 0 \to i = j$ → I E J UGUALI

CLASSI UGUALI SONO

CONGRUENZE

UNA RELAZIONE:
- RIFLESSIVA
- SIMMETRICA
- TRANSITIVA

COMPATIBILE A SINISTRA

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 UGUALI

$(\forall a,b,c,d \in S)((\forall i \in \mathbb{N})(0 \leq i \leq m \rightarrow (a \sim b \wedge c \sim d \rightarrow a *_i c \sim b *_i d)))$

CONTINUO AD AVERE SEMPRE LA STESSA CLASSE DI EQUIVALENZA

ALLORA ANCHE FARE IL PRODOTTO DEI SINGOLI RAPPRESENTANTI NON CAMBIA LA RELAZIONE DI EQUIVALENZA

Se $\sim$ è congruenza in $(S, *_1, *_2, \dots, *_m)$, allora sono ben poste:

ABBIAMO L'OPERAZIONE SU S E VOGLIAMO RIPORTARLA SULL'INSIEME QUOZIENTE

- $(*_i)_\sim : ([X]_\sim, [Y]_\sim) \in S/\sim \times S/\sim \longmapsto [X *_i Y]_\sim \in S/\sim$
- $\pi \quad X \in S \longmapsto [X]_\sim \in S/\sim \rightarrow \pi$ è un epimorfismo tra $(S, *_1, *_2, \dots, *_m)$ e $(S/\sim, (*_1)_\sim, (*_2)_\sim, \dots, (*_m)_\sim)$

LE STRUTTURE NON SONO TANTO DIVERSE, POSSO PORTARMI LE OPERAZIONI DA S A S/~ SE IL ~ SI COMPORTA BENE RISPETTO ALLE OPERAZIONI → CIOÈ SE VALE 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

↳ SE $(S, *_1, *_2, \dots, *_n)$ È UNA STRUTTURA CON n OPERAZIONI INTERNE

DIM

Suppongo ci sia un'unica operazione $*$ in $(S,*)$

$(\rightarrow)$ Per ipotesi ho $a \sim b$. Dato che $\sim$ è una relazione di equivalenza, allora vale anche $c \sim c$. Quindi $c*a \sim c*b$

STESSO RAGIONAMENTO PER LA COMPATIBILITÀ A DESTRA

↳ 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, $b*c \sim b*d$
- 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

↳ SI PUÒ VEDERE CHE SONO CONGRUENZE IN $(\mathbb{Z},+,\cdot)$

↳ $(\mathbb{Z},+,\cdot) \xrightarrow{\pi} (\mathbb{Z}_m,+,\cdot)$ → POSSIAMO SOMMARE E MOLTIPLICARE LE CLASSI DI EQUIVALENZA COME ABBIAMO DEFINITO PRIMA

$[1]_3 \cdot [2]_3 = [1 \cdot 2]_3 = [2]_3$

ANELLI QUOZIENTE DI $(\mathbb{Z},+,\cdot)$

$(\mathbb{Z}_m,+,\cdot)$ lo chiamo anello quoziente di $(\mathbb{Z},+,\cdot)$, infatti:

- $(\mathbb{Z}_m,+)$ è un gruppo → $[1]_3 \overset{\text{OPPOSTO DI } [1]_3}{+} [2]_3 = [3]_3 = [0]_3$ → ELEMENTO NEUTRO IN $(\mathbb{Z}_m,+)$
- $(\mathbb{Z}_m,\cdot)$ è un gruppo → $[2]_3 \overset{\text{INVERSO DI } [2]_3}{\cdot} [2]_3 = [4]_3 = [1]_3$ → ELEMENTO NEUTRO IN $(\mathbb{Z}_m,\cdot)$

PROVA CHE ANELLO QUOZIENTE È UN GRUPPO

↳ ALTRI $(\mathbb{Z}_m,\cdot)$ NON HANNO L'INVERSO!

ESEMPIO:

In $\mathbb{Z}_6$, $[2]_6 \cdot [3]_6 = [0]_6$ → $\mathbb{Z}_6$ NON È UN DOMINIO DI INTEGRITÀ

DIVISORI DI 0 CON $\cdot$

TEOREMA

Sia $m \in \mathbb{Z} \setminus \{0\}$ sono equivalenti:

1) $(\mathbb{Z}_m, +, \cdot)$ è un campo
2) $(\mathbb{Z}_m, +, \cdot)$ è un dominio di integrità
3) m è primo

DIM

1) $\to$ 2) È ovvio perché ogni campo è un dominio di integrità

VOGLIO FAR VEDERE CHE m HA SOLO DIVISORI BANALI

2) $\to$ 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:

$[a]_m = [0]_m \vee [b]_m = [0]_m \to$ ho che $[a]_m [b]_m = [0]_m$

Suppongo $a \equiv_m 0$, cioè $(\exists x \in \mathbb{Z})(a = km)$ $\to$ cioè $a - 0 = km$

↳ Allora $m = a \cdot b = k \cdot m \cdot b$, quindi, dato che m è cancellabile, $1 = k \cdot b$

↳ Allora $b = \pm 1$ e $a = \pm m \to$ Allora m è irriducibile, quindi primo.

3) $\to$ 1) Considero $[a]_m \neq [0]_m \to$ VOGLIO FAR VEDERE TUTTI GLI ELEMENTI NON NULLI SONO INVERTIBILI AFFINCHÉ SIA UN CAMPO

Posso scegliere $0 < a' < |m|$ (resto di a)

m è irriducibile, cioè $DIV(m) = \{1, -1, m, -m\}$

Quindi $MCD(a, m) = \{-1, 1\}$

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

Quindi $[1]_m = [a \cdot u + \widetilde{m \cdot v}]_m = [a \cdot u]_m = [a]_m \cdot [u]_m$

Quindi $[a]_m$ è invertibile $\to (\mathbb{Z}_m, +, \cdot)$ è un campo

EQUAZIONI DIOFANTEE

Siano $a, b, c \in \mathbb{Z}$

$\ell[a,b,c] : (m, n) \in \mathbb{Z} \times \mathbb{Z} \longmapsto a \cdot m + bn - c \in \mathbb{Z}$

ESEMPIO:

- $\ell[1,2,3](10,-2) = 1 \cdot 10 + 2(-2) - 3 = 3$

$\ell[a,b,c]$ si chiama equazione diofantea di 1° grado a due incognite con termini a, b, c.
Sinteticamente scrivo "$ax + by = c$"

SOLUZIONE DI $\ell[a,b,c]$

Se $\ell[a,b,c](m,n) = 0$, la coppia $(m,n) \in \mathbb{Z} \times \mathbb{Z}$ si dirà soluzione di $\ell[a,b,c]$

ESEMPIO:

- $2u - 1 = k \cdot 3$

$2u + (-k) \cdot 3 = 1 \rightarrow u = 2$

$(u, k) = (2, -1)$

TEOREMA

Siano $a, b \in \mathbb{Z} \setminus \{0\}$ e sia $d \in MCD(a,b)$.
Allora sono equivalenti:

1) Il teorema di Bezout
2) a e b sono coprimi se e solo se:
   $(\exists u, v \in \mathbb{Z})(1 = a \cdot u + b \cdot v)$
3) $\langle a, b \rangle = d \cdot \mathbb{Z}$ in $(\mathbb{Z}, +)$
   sottogruppo generato da a e b — sottogruppo di ordine d
4) L'equazione diofantea $ax + by = c$ ha soluzioni se e solo se $d \mid c$

DIM

1) -> 2)

(->) Per Bézout, dato che se a e b sono coprimi (per il teorema di Bézout), vuol dire che $1 \in MCD(a,b)$ e quindi $1 = a \cdot u + b \cdot v$

(<-) $d|a \wedge d|b$ (dal teorema prima del valore assoluto ho che $d|(au+bv)$), quindi $d|1$, quindi $1 \in MCD(a,b)$, (dal teorema di Bezout)

per ipotesi $d \in MCD(a,b)$ cioè sono coprimi

visto che $au+bv=1$

2) -> 3)

($\subseteq$) $a, b \in d\mathbb{Z}$ dato che $d \in MCD(a,b)$

$\langle a,b \rangle$ è il più piccolo sottogruppo che contiene a, b, ma $d\cdot\mathbb{Z}$ è un sottogruppo di $\mathbb{Z}$, quindi $\langle a,b \rangle \subseteq d\mathbb{Z}$

($\supseteq$) Scrivo $a = a_1 \cdot d$ e $b = b_1 \cdot d$

Poiché $d \in MCD(a,b)$, ho che a_1 e b_1 sono coprimi -> Per 2), trovo due numeri $u, v \in \mathbb{Z}$ tale che $1 = a_1 u + b_1 v$ -> moltiplico tutto per d

tutti i divisori comuni sono in d

Quindi $d = au + bv \in \langle a,b \rangle$, ossia $d\mathbb{Z} \subseteq \langle a,b \rangle$

essendo $au+bv$ somme di a e b varie volte

$d \in \langle a,b \rangle$, quindi d e tutti i suoi multipli appartengono a $\langle a,b \rangle$

3) -> 4)

(->) Ci sono $m, n \in \mathbb{Z} : am + bn = c$

Ma dato che $d|a$ e $d|b$ ($d \in MCD(a,b)$), allora $d|c$ -> perché $d|(am+bn)$ dal teorema prima del valore assoluto

(<-) Sia $d|c$, allora $c \in d\mathbb{Z}$ ma $d\mathbb{Z} = \langle a,b \rangle$ per 3). Cioè $(\exists m, n \in \mathbb{Z})(am + bn = c)$ -> l'equazione diofantea ha soluzioni

così si scrivono gli elementi del sottogruppo generato da a e b

4) -> 1) Se prendo $d = c$, per la 4), vuol dire che $ax + by = d$ ha soluzioni, cioè $(\exists m, n \in \mathbb{Z})(am + bn = d)$

-> è proprio Bezout

TEOREMA

Sia $ax+by=c$ una equazione diofantea con soluzione (x_0, y_0).
Allora, se $d \in MCD(a,b)$, l'insieme delle soluzioni dell'equazione è: $\left\{\left(x_0+\frac{b}{d}k,\ y_0-\frac{a}{d}k\right) \mid k \in \mathbb{Z}\right\}$

POSSO FARLO PERCHÉ $d \in MCD(a,b)$

AL VARIARE DI K IN $\mathbb{Z}$

DIM

L'insieme delle soluzioni dell'equazione $ax+by=c$ lo chiamo S e l'insieme $\left\{\left(x_0+\frac{b}{d}k,\ y_0-\frac{a}{d}k\right) \mid k \in \mathbb{Z}\right\}$ lo chiamo H → VOGLIO FAR VEDERE CHE $H=S$

($\subseteq$)

Sostituendo si vede che $H \subseteq S$

$$a\left(x_0+\frac{b}{d}k\right)+b\left(y_0-\frac{a}{d}k\right)=ax_0+by_0+\cancel{\frac{ab}{d}k}-\cancel{\frac{ab}{d}k}=c$$

↳ (x_0, y_0) È SOLUZIONE PER IPOTESI E LE HO TROVATE SOSTITUENDO LA COPPIA DI H NELL'EQUAZIONE

($\supseteq$)

Sia $(x,y) \in S$, cioè $ax+by=c=ax_0+by_0$, quindi
$a(x-x_0)=b(y_0-y)$ → CIOÈ, $ax+by=ax_0+by_0 \rightarrow ax-ax_0=by_0-by$ E METTO IN EVIDENZA

↳ Visto che $d \in MCD(a,b)$, 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 $\frac{a}{d}$ e $\frac{b}{d}$ sono coprimi, $(\exists k, h \in \mathbb{Z})\left(\begin{cases} h\cdot\frac{a}{d}=y_0-y \\ k\cdot\frac{b}{d}=x-x_0 \end{cases}\right)$ DATO CHE $\frac{a}{d} \mid y_0-y$ E ↳ $\frac{b}{d} \mid x-x_0$

h E k SONO UGUALI?

Sostituisco il sistema in $\frac{a}{d}(x-x_0)=\frac{b}{d}(y_0-y)$ e ho che:

$$\frac{a}{d}\left(k\cdot\frac{b}{d}\right)=\frac{b}{d}\left(h\cdot\frac{a}{d}\right) \rightarrow h=k$$

Quindi $x=x_0+k\cdot\frac{b}{d}$ e $y=y_0-k\cdot\frac{a}{d}$

↳ La soluzione generica è proprio uguale alla copia di H

Correzione esercizi 07/12/2021 (LEZIONE 32)

1) $[41]_5 \cap \{m \in \mathbb{Z} \mid m^2 \leq 20\}$

Ovvero:

- $[41]_5 = [1]_5 = \{1 + k \cdot 5 \mid k \in \mathbb{Z}\}$
- $\{m \in \mathbb{Z} \mid m^2 \leq 20\} = \{0, -1, 1, -2, 2, -3, 3, -4, 4\}$ → DOBBIAMO TROVARE QUI QUELLI CHE POSSO SCRIVERE COME $1 + k \cdot 5$ o CHE $DE(m,5) = (q,1)$

$[41]_5 \cap \{m \in \mathbb{Z} \mid m^2 \leq 20\} = \{1, -4\}$, infatti:

- $DE(-1,5) = (-1,4)$ → PERCHÉ $0 \leq r < |m|$, QUINDI → IL RESTO NON PUÒ ESSERE NEGATIVO

Quindi dai passaggi ridotti: SAL SECONDO RIGO IN NEG. $1 = 0 \cdot 5 + 1$

$-1 = 0 \cdot 5 - 1 = (0 \cdot 5 - 5) + (5 - 1) = \underline{(-1)} \cdot 5 + \underline{4}$ ← AGGIUNGO E SOTTRAGGO $|m|$

- Inoltre, $[-1]_5 = [4]_5$
  $[-2]_5 = [3]_5$
  $[-3]_5 = [2]_5$
  $[-4]_5 = [1]_5$

  BASTA AGGIUNGERE (O SOTTRARRE) 5 FINCHÉ NON ARRIVIAMO A UNA CLASSE CON RESTO $0 \leq r < |m|$

4) $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$

$\underbrace{[30]_3 = [0]_3}_{3 \mid 30-0}$; $[2]_3 = [11]_3$; $\underbrace{[-8]_3 = [1]_3}_{\text{AGGIUNGO 9 A } -8}$ SI

5) $\underbrace{[30]_5 = [0]_5}_{30 \text{ È UN MULTIPLO DI } 5}$; $[2]_5$; $[11]_5 = [1]_5$; $[-8]_5 = [-8+10]_5 = [2]_5$; $[3]_5$

Quindi abbiamo: $[0_5]$, $[2]_5$, $[1]_5$, $[3]_5$ ma manca $[4]_5$, quindi questo insieme non $\mathbb{Z}_5$

6) $4842893740982793 40! \text{ MOD } 3879374 = 0$ perché essendo il primo numero un fattoriale è maggiore del secondo, tra i prodotti dei fattoriali c'è anche il secondo numero.

EQUAZIONI CONGRUENZIALI

- Sia $m \neq 0$ appartenente a $\mathbb{Z}$ $(m \in \mathbb{Z} \setminus \{0\})$

Siano $a, b \in \mathbb{Z}$.

Sia $ec[a, b, m] : [m]_m \in \mathbb{Z}_m \mapsto [a \cdot m - b]_m \in \mathbb{Z}_m$

- $ec[a, b, m]$ 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 la scriveremo come: $aX \equiv_m b$

- $m \in \mathbb{Z}$ si dice soluzione di $ec[a, b, m]$ se $ec[a, b, m]([m]_m) = [0]_m$.

Ovvero se $a \cdot m \equiv_m b$

↓

Se m è soluzione, tutti gli interi in $[m]_m$ sono soluzioni

ESEMPIO:

- $2x \equiv_5 4$ $\quad 2 \cdot 2 \equiv_5 4 \leftrightarrow 2 \cdot \overbrace{(2 + k \cdot 5)}^{\text{UN ALTRO MEMBRO DELLA CLASSE DI EQUIVALENZA } [2]_5} = 4 + 2k \cdot 5 \equiv_5 4$ → $5 \mid (4 + 2k \cdot 5 - 4)$, $5 \mid 2k \cdot 5$ essendo $2k5 \in \mathbb{N} \cup \{0\}$

- $4x \equiv_2 3$ non ha soluzione dato che $[4x]_2 = [0]_2$ (4x è sempre pari) e $[3]_2 = [1]_2$. Quindi siamo dicendo che $0 \equiv_2 1$ → FALSO

- Trovare soluzioni di $aX \equiv_m b$ equivale a trovare le soluzioni di $aX + mY = b$ → cioè noi stiamo 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 diofantee e le equazioni congruenziali

TEOREMA

Siano $a, b \in \mathbb{Z}$, $m \in \mathbb{Z} \setminus \{0\}$ e $d \in MCD(a, m)$, allora $aX \equiv_m b$ ha soluzione x se solo se $d | b$

↳ 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 e m sono coprimi. ↳ cioè $d | 1$ con $d = MCD(a, m)$

COROLLARIO 2

Se $m \in \mathbb{Z} \setminus \{0\}$, $[a]_m \in U(\mathbb{Z}_m)$ se e solo se $[a]_m$ non è $\underbrace{\text{divisore dello zero}}$ → POSSO FARE UN ALGORITMO PER TROVARE IL DIVISORE DELLO 0 ASSOCIATO A $[a]_m$ SE NON INVERTIBILE

↓ NELL'ESERCIZIO A PROSSIMA PAGINA

DIM $[a]_m$ È DIVISORE DELLO ZERO $\leftrightarrow (\exists [b]_m \in \mathbb{Z}_m)([a]_m [b]_m = [0]_m)$

($\rightarrow$) 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 cancellabile quindi $[b]_m = [0]_m$ ↯

($\leftarrow$) Per Assurdo, $[a]_m$ non è invertibile.

Per il corollario 1, a ed m non sono coprimi, allora prendo $d \in \mathbb{Z}$ con $d \neq 1$ (ciò che non sono coprimi) : $a \cdot d = K \cdot m$

Quindi $[a]_m [d]_m = [a \cdot d]_m = [m]_m = [0]_m$

ESEMPIO:

- $a = 6$
  $m = 10$
  $2 \in MCD(6, 10)$

DIVIDO m PER IL MCD → $\frac{10}{2} = 5 \neq 1$ e $0 \leq 5 < 10$

E' IL NUMERO TALE CHE DIVISORI DELLO 0

$[5]_{10} \neq [0]_{10}$ → POSSIAMO CHE $[3]_{10}$ $[6]_{10}$ SIANO DEI DIVISORI DELLO ZERO

→ $[6]_{10} \cdot [5]_{10} = [3 \cdot 2]_{10} \cdot [5]_{10} = [3]_{10} \cdot [2 \cdot 5]_{10} =$
$= [3]_{10} \cdot [10]_{10} = [0]_{10} = 0$

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:

  - $100x \equiv_{11} 2$ → DEVO TROVARE UN NUMERO CHE MOLTIPLICATO PER 100 MI DIA $[0]_{11}$

    $1 \in [100]_{11}$ → DATO CHE $100 = 9 \cdot 11 + 1$

    Cerco la soluzione di $1 \cdot x = x \equiv_{11} 2$ → $[x]_{11} = [2]_{11}$

- Se $k \in \mathbb{Z} \setminus \{0\}$, l'equazione $a \cdot k \cdot x \equiv_{m \cdot k} b \cdot k$ ha lo stesso insieme di soluzioni di "e"

  ↳ In effetti, nelle equazioni diofantee,
  $ax + my = b \leftrightarrow akx + mky = bk$ → DATO CHE LE EQ SONO MOLTO SIMILI ALLE E, ALLORA LO STESSO RAGIONAMENTO PUO' ESSERE RIPORTATO

  ESEMPIO:

  MOLTIPLICO PER -1 — SIAMO $\equiv_3$ E' UGUALE A $\equiv_3$

  - $-4x \equiv_3 -1 \leftrightarrow 4x \equiv_{-3} 1 \leftrightarrow 4x \equiv_3 1$

- Se esiste $k \in \mathbb{Z}$: $a = a'k$, $b = b'k$ e $m = m'k$, l'equazione $a'x \equiv_{m'} b'$ ha lo stesso insieme di soluzione di "e"

  ↳ $ax + my = b \leftrightarrow akx + mky = bk$

  ESEMPIO:

  - $2x \equiv_6 4 \leftrightarrow x \equiv_3 2$

Per ogni K coprimo con m, l'equazione $aKx \equiv_m bK$ ha lo stesso insieme di soluzione di "a"

1) Ovviamente $[a \cdot x]_m = [b]_m \rightarrow [a \cdot K \cdot x]_m = [b \cdot K]_m$ → MOLTIPLICO A SINISTRA PER UNA CLASSE DI EQUIVALENZA PER $[K]_m$

2) $[a \cdot K \cdot x]_m = [b \cdot K]_m \rightarrow [a \cdot x]_m = [b]_m$ perché vale l'inverso di K, QUESTO PERCHÉ ESSENDO K E m COPRIMI, ALLORA K È INVERTIBILE, CIOÈ POSSIAMO TROVARE UN NUMERO h TALE CHE $h \cdot K = 1$

ESEMPIO: RISOLVERE ESSERE

$\cdot\ 5x \equiv_{19} 3 \rightarrow [5]_{19} [x]_{19} = [3]_{19}$

TROVO L'INVERSO

$[5]_{19} \cdot [4]_{19} = [20]_{19} = [1]_{19} \rightarrow [4]_{19}$ è l'inverso di $[5]_{19}$

Quindi $[5]_{19} \cdot [x]_{19} = [3]_{19} \leftrightarrow [5]_{19} \cdot [x]_{19} [4]_{19} = [3]_{19} \cdot [4]_{19} \leftrightarrow [x]_{19} = [12]_{19}$ è la soluzione

METODO DI RISOLUZIONE DI $aX \equiv_m b$

1) Ridurre a e b a numeri compresi tra 0 e $m-1$ (ESSI LA CONDIZIONE COPRIMA)

2) Prendere $d \in MCD(a, m)$

↳ Se $d \nmid b$, l'equazione non ha soluzioni

↳ Se $d \mid b$ procedo al passo 3

3) Scrivo $a = a' \cdot d$, $b = b' \cdot d$ e $m = m' \cdot d$ → DATO CHE: $d \mid b \wedge d \mid m \wedge d \mid a$

Passo all'equazione $a'x \equiv_{m'} b'$ (EQUIVALENTE ALLA PRIMA)

4) Trovo l'inverso in $(\mathbb{Z}_{m'}, \cdot)$ di $[a']_{m'}$ con l'algoritmo delle divisioni successive estesa e lo chiamo $[K]_{m'}$ → DA QUI TROVIAMO CHE $aK + mh = 1$

POSSO FARLO PERCHÉ a' E m' SONO COPRIMI AVENDO TOLTO IL $MCD(a, m)$

5) L'insieme delle soluzioni è $[b' \cdot K]_{m'}$

↳ È una classe di resto modulo m/d con $d \in MCD(a, m)$

PERIODICO

{ • È ASSOCIATIVA
CE 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 priodico se:

$(\exists m \in \mathbb{N}\setminus\{0\})(\underbrace{x^m = 1_g}) \rightarrow$ SAREBBE $\underbrace{x\cdot x\cdot x\cdot x\cdot x}_{m \text{ VOLTE}} = 1_g \rightarrow$ ELEMENTO NEUTRO

! In $(\mathbb{Z},+)$ è come dire "$m\cdot x = 0$" $\rightarrow$ PERCHÉ È COME DIRE $\underbrace{x+x+x+x+x}_{m \text{ VOLTE}} = 0$

ESEMPIO:

$(\mathbb{Z},+)$ non ha elementi periodici diversi da 0 perché solo $0+0+0+0+\dots+0=0$

PERIODO DI X

Il minimo $m \in \mathbb{N}\setminus\{0\} : x^m = 1$ si dice periodo di x e si scrive $|x| = m$

Equivale 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:

$(\forall a,b \in \mathbb{Z})(x^a = x^b \Leftrightarrow a \equiv_m b)$

DIM → L'ALTRO VERSO SI DIMOSTRA CON LO STESSO RAGIONAMENTO AL CONTRARIO

L'INVERSO DI x^b → ESISTE PERCHÉ $(g,\cdot)$ È UN GRUPPO

$(\rightarrow)$ $x^a = x^b$ se e solo se $x^{a-b} = x^a \cdot x^{-b} = x^b \cdot x^{-b} = 1_g = x_0$

Prendo $DE(a-b, m) = (q, r)$

Quindi $1_g = x^{a-b} = x^{qm+r} = x^{qm}\cdot x^r = (x^m)^q \cdot x^r$

DATO CHE r È DATO DALLA DE$(a-b,m)$ Per ipotesi $x^m = 1_g$, quindi $(x^m)^q \cdot x^r = 1_g^q \cdot x^r = x^r$

So che $0 \leq r < m$, quindi $r = 0$

↳ Infatti mi sono trovato che $1_g = x^r$, cioè r è il periodo di x, ed essendo il minimo dei valori compresi tra 0 e m, allora $r = 0$

Ciò significa che $a \equiv_m b$ dato che $r = 0$ ↳ DATO CHE $a-b = q\cdot m + r$, cioè $a-b = q\cdot m$

POLINOMI

Sia A un anello commutativo unitario (ACU)
e dico $0 = 0_A$ → 0 DELL'ANELLO

SUCCESSIONE

Una funzione da $\mathbb{N}$ ad A viene detta successione di elementi di A.
Scrivo $(a_n)_{n \in \mathbb{N}}$ per indicare che l'immagine di 0 è a_0, che l'immagine di 1 è a_1 ecc... L'IMMAGINE DI n È a_n

POLINOMIO A COEFFICIENTI IN A

Dico $(a_n)_{n \in \mathbb{N}}$ un polinomio a coefficienti in A se
$(\exists k \in \mathbb{N})((\forall n \geq k)(a_n = 0))$ → SONO DELLE SUCCESSIONI CHE DA UN CERTO PUNTO IN POI DANNO SEMPRE IMMAGINE UGUALE A 0

COEFFICIENTI DEL POLINOMIO

Gli a_i di $(a_n)_{n \in \mathbb{N}}$, 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, $0 := (0)_{n \in \mathbb{N}}$, ovvero, $(\forall n \in \mathbb{N})(a_n = 0)$ → SUCCESSIONE NULLA

GRADO DI f

Sia $f \in A[X] \setminus \{0\}$.
Il minimo $k \in \mathbb{N} : (\forall n \geq k)(a_n = 0)$ lo dico grado di f. Lo scrivo come $gr(f)$

SAPPIAMO CHE ESISTE PER DEFINIZIONE

COEFFICIENTE DIRETTORE

Se $f \in A[X] \setminus \{0\}$, $a_{gr(f)}$ è detto coefficiente direttore e lo scrivo $cd(f)$ → sempre diverso da 0

a_0 lo dico termine noto

ESEMPIO:

$(0, 1, a, 0, 0, b, \overbrace{0, 0, 0, \ldots, 0}^{\text{sempre } 0})$ ha grado 5

↳ scrivo $1x + ax^2 + bx^5$

PER LA SUCCESSIONE NULLA

Definisco $cd(0) = 0$ e $gr(0) = -\infty$

↳ Cioè ma pongo in $(\mathbb{N} \cup \{-\infty\}, \leq)$ dove $-\infty$ è il valore più piccolo di tutti

POLINOMIO MONICO

Se $a_{gr(f)} = 1$, f lo dico polinomio monico

SOMMA E PRODOTTO

Se $(a_n)_{n \in \mathbb{N}}$ e $(b_n)_{n \in \mathbb{N}}$ appartengono a $A[X]$, definisco:

- $(a_n + b_n)_{n \in \mathbb{N}} =: (a_n)_{n \in \mathbb{N}} + (b_n)_{n \in \mathbb{N}}$ è la somma → sommo componente a componente
- $\left(\sum_{i+j=n} a_i \cdot b_j\right)_{n \in \mathbb{N}} =: (a_n)_{n \in \mathbb{N}} \cdot (b_n)_{n \in \mathbb{N}}$ è il prodotto → è scritto sopra il prodotto dei singoli a_i e b_j tali che la somma dei pedici faccia n e poi sommo i prodotti

ESEMPIO:

- $(1+x) \cdot (2+x^2) \rightarrow (1, 1, 0, 0, \ldots) \cdot (2, 0, 1, 0, 0, \ldots)$

$2 + x^2 + 2x + x^3$ $\qquad (2, \underbrace{2+0}, \underbrace{1+0+0}, \ldots)$

$n = 2 \rightarrow i + j = 2$

Per $n=0$ ho che $i+j=0$ e sono finite la somma di quando $i=0$ e $j=0$ e di quando $i=1$ e $j=0$

TUTTE LE COMBINAZIONI DI i E j PER CHE $i+j=1$

$i=0$ e $j=1 \rightarrow 1 \cdot 2$

$i=1$ e $j=0 \rightarrow 1 \cdot 0$

Faccio la somma $\rightarrow 2+0=2$

QUINDI:

$0+2 = 1 \cdot 1 = 1$

$1+1 = 1 \cdot 0 = 0$

$2+0 = 0 \cdot 2 = 0$

$\sum = 2$

la somma

TEOREMA [illegible]

$(A[X],+,\cdot)$ è un anello commutativo unitario

- l'opposto additivo di $(a_n)_{n\in\mathbb{N}}$ è $-(a_n)_{n\in\mathbb{N}}$
- 0 è neutro rispetto a $+$
- $(1,0,0,0,\dots)$ è neutro rispetto a $\cdot$ [illegible]

↳ $(a_0,a_1,a_2,\dots)(1,0,0,0,\dots)=(a_0,a_1,a_2,\dots)$

POLINOMIO COSTANTE

Un polinomio del tipo $(a,0,0,0,\dots)$ si dice polinomio costante

MONOMORFISMO DI ANELLI

- $\mu: a\in A \longrightarrow (a,0,0,0,\dots)\in A[X]$ è un monomorfismo di anelli. ↳ è un omomorfismo iniettivo → non somma e prodotto non alterano gli elementi polinomio costante
- In particolare $A \underset{\text{è isomorfo}}{\simeq} \operatorname{Im}\mu$ — non confondere i polinomi come anelli
- Per ogni $a\in A$, pongo $\bar{a} := (a,0,0,0,0,\dots)$ → anche indeterminate
- Pongo $X := (0,1,0,0,0,\dots)$

↳ $X^2 = ?$

$$(0,1,0,0,0,\dots)\cdot(0,1,0,0,0,\dots)=(0,0,1,0,0,\dots)$$

Quindi $X^2=(0,0,1,0,0,0,0,\dots)$

- È facile provare per induzione che:

$$X^m=(\underbrace{0,0,0,\dots,0}_{m \text{ volte}},1,0,0,0,0,\dots)$$

- Anche facile vedere che:

$$a\cdot X^m=(a,0,0,0,0,\dots)\cdot(\overbrace{0,0,0,\dots,0}^{m \text{ volte}},1,0,0,\dots)=$$
$$=(\underbrace{0,0,0,0,\dots,0}_{m \text{ volte}},a,0,0,0,\dots)$$

• Se $m \in \mathbb{N}$ e $gr(f)=m$ con $f=(a_0, a_1, \dots, a_m, \underbrace{0, 0, \dots}_{\text{SEMPRE } 0})$
ho scritto che $f = a_0 + a_1 X + \dots + a_m X^m$.
$a_m \neq 0$ per definizione di $gr(f)$ → a_m è QUELLO CHE ANCORA NON È 0

PROPRIETÀ

Dalla distributività in $(A[X], +, \cdot)$, segue che se:

- $f, g \in A[X]$
- $m = gr(f)$
- $n = gr(g)$
- $M = MAX\{m, n\}$

Allora:

- $f+g = \sum_{i=0}^{M} (a_i + b_i) X^i$
- $f \cdot g = \sum_{i=0}^{m+n} \left(\sum_{j=0}^{i} a_j \cdot b_{i-j} \right) \cdot X^i$ → LA SOMMA DI $\overset{\text{POTENZE DI } a}{j}$ E $\overset{\text{POTENZE DI } b}{i-j}$ FARÀ i, CHE È PROPRIO L'ESPONENTE DI X, CHE NON È ALTRO CHE LA POSIZIONE i^{ma} $(0, 0, 0, \dots, 0, 1, 0, 0 \dots)$ DEL POLINOMIO

POSSO FARE L'ANELLO DEI POLINOMI SU:

$\mathbb{Z}[X] \longrightarrow \mathbb{Z}_m[X]$ e è un epimorfismo → QUELLO CHE A UN CERTO POLINOMIO ASSOCIA I COEFFICIENTI CHE STANNO TUTTI NELLE CLASSI DI CONGRUENZA ASSOCIATE

ESEMPIO:

- $(a_n)_{n \in \mathbb{N}} \longrightarrow ([a_n]_m)_{n \in \mathbb{N}}$

GRADO NELLA SOMMA DI POLINOMI

Siano $f, g \in A[X] \setminus \{0\}$ allora: • Se $gr(f) = gr(g)$ e $cd(f) = -cd(g)$ allora $gr(f+g) < gr(f) = gr(g)$ → È OVVIO PERCHÉ SE IL cd È OPPOSTO QUEL GRADO SI CANCELLA E CI SARÀ 0

• Se $gr(f) \neq gr(g)$ oppure $cd(f) \neq -cd(g)$ allora:
$gr(f+g) = MAX\{gr(f), gr(g)\}$ → IL MASSIMO DEI GRADI

GRADO NEL PRODOTTO DI POLINOMI

ESEMPIO: In $\mathbb{Z}_4[X]$:

$$\underbrace{([1]_4 + [2]_4 X)}_{gr(f)=1}\underbrace{([2]_4)}_{gr(g)=0} = [2]_4 + \underbrace{[4]_4 X}_{\text{è } 0} = \underbrace{[2]_4}_{gr(f \cdot g)=0}$$

→ IN $\mathbb{Q}$ NON SUCCEDE, IL GRADO È LA SOMMA DEI GRADI

1) Se $cd(f) \cdot cd\, g = 0$, allora $gr(f \cdot g) < gr(f) + gr(g)$

↳ SE IL COEFFICIENTE DIRETTORE DIVENTA 0, IL POLINOMIO A QUELLA POSIZIONE AVRÀ 0

2) Se $cd(f) \cdot cd(g) \neq 0$, allora

$gr(f \cdot g) = gr(f) + gr(g)$ e $cd(f\, g) = cd(f) \cdot cd(g)$

FORMULA DI ADDIZIONE DEI GRADI (F.A.G.)

QUESTA FORMULA VALE ANCHE PER LA SUCCESSIONE NULLA

• $f = 0$	$gr(f\, g) = gr(0) = -\infty = -\infty + gr(g)$
	$cd(f\, g) = 0 = cd(f) \cdot cd(g)$

3) Se $cd(f)$ è cancellabile, anche f è cancellabile. In particolare per f vale la formula di addizione dei gradi

DIM

Essendo $cd(f)$ 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 ↳

(→) SE $A[X]$ È UN DOMINIO DI INTEGRITÀ, A STA DENTRO AD $A[X]$, QUINDI È OVVIO CHE A È UN DOMINIO DI INTEGRITÀ

(←) SEGUE DALLA 3, SE A È UN DOMINIO DI INTEGRITÀ ALLORA LO È ANCHE L'ANELLO DI INTEGRITÀ

5) Se $f \in A[X]$ è cancellabile e il grado di f è strettamente maggiore di 0 ($gr(f) > 0$) allora f non è invertibile

DIM

Per Assurdo, sia f invertibile e sia $g = f^{-1}$ → $gr(f) + gr(g) = 0$, QUINDI $gr(f)$ O È 0 O È $-\infty$

Per 2) ho che $\underbrace{gr(f) + gr(g)}_{} = gr(f \cdot g) = gr(1) = 0$

Quindi $gr(f) = 0$ ↯

FALSO VALE PERCHÉ f È CANCELLABILE

CIOÈ SUCCESSIONE $(1, 0, 0, 0, \ldots)$ → COSTANTE

6) Se A è dominio di integrità, $U(A[X]) = U(A)$

↳ SEGUE DA 5), PERCHÈ GLI INVERTIBILI DA 5) SONO SOLO QUELLI CON GRADO 0, CIOÈ QUELLI CHE STANNO IN A

↳ INVERTIBILI

ESEMPIO:

$$\cdot([1]_4 + [2]_4 X)([1]_4 + [2]_4 X) = [1]_4 + [2]_4 X + [2]_4 X + ([2]_4 X)^2 =$$

$$= [1]_4 + \underbrace{[4]_4}_{0} X + \underbrace{[4]_4}_{0} X^2 = [1]_4$$

→ $\mathbb{Z}_4$ NON È UN DOMINIO DI INTEGRITÀ → $[2]_4 \cdot [2]_4 = [4]_4 = [0]_4$

E HO TROVATO DELLI ELEMENTI INVERTIBILI CHE NON SONO IN $U(A)$ PERCHÈ CON GRADO MAGGIORE DI 0

7) Il polinomio X non è mai invertibile (perché il $ed(X) = 1$ che è sempre cancellabile)* → $\frac{1}{X} \notin A[X]$

In particolare $A[X]$ non è mai un campo

TEOREMA (DIVISIONE LUNGA) → LA DIVISIONE TRA I POLINOMI

Sia A un anello commutativo unitario e siano $f, g \in A[X]$. Se $\boxed{ed(g) \in U(A)}$, esiste una ed una sola coppia $(q, r) \in A[X] \times A[X]$ tale che:

$f = gq + r$ e $gr(r) < gr(g)$

DIM INDUZIONE DI II FORMA SU $m := gr(f)$

(ESISTENZA) Pongo $m := gr(g)$ e $n := gr(f)$.

- Se $n < m$, è ovvio perché pongo $q = 0$ e $r = f$
- Se $n \geq m$, $m \neq 0$ per ipotesi su $ed(g)$

Pongo $a := ed(f)$ e $b := ed(g)$ → USO INDUZIONE DI SECONDA FORMA SU m

Sia $k = ab^{-1} \cdot X^{n-m} \cdot g$. → POSSO FARLO PERCHÈ HO CHE $n \geq m$

Tra $a \cdot b^{-1} \cdot X^{n-m}$ e g vale la formula di addizione dei gradi per 2).

Di conseguenza $gr(k) = gr(ab^{-1} \cdot X^{n-m}) + gr(g) =$

$= n - m + m = n$ e $ed(k) = a$.

Dico $h := f - k$, dunque $gr(h) < n$. → PERCHÈ HO TOLTO AD f UN POLINOMIO CHE HA IL GRADO DI f E IL SUO STESSO COEFFICIENTE DIRETTORE

Per induzione ci sono q_1 e r_1

Per induzione ci sono q_1 e r_1 tali che:

$f - K = g \cdot q_1 + r_1$ con $gr(r_1) < gr(g)$.

Scrivo $f = g \cdot q_1 + r_1 + ab^{-1} \cdot x^{m-m} \cdot \underset{\substack{\uparrow \\ \text{MESSO IN} \\ \text{EVIDENZA } g}}{g} = g(q_1 + ab^{-1} \cdot x^{m-m}) + r_1$

(UNICITÀ) Siano (q_1, r_1) e (q_2, r_2) come da ipotesi.

Quindi $g(q_1 - q_2) = r_2 - r_1$.

↳ $\underline{gr(r_2 - r_1) < (gr(g) = m)}$

Poi da 2) segue che $gr(g(q_1 - q_2)) = gr(g) + gr(q_1 - q_2) =$

$= m + \underbrace{gr(q_1 - q_2)}_{\text{↳ NON CI INTERESSA QUALE SIA}}$ ~~il grado è sicuramente $\geq m$, $gr(q_1 - q_2) \geq m$~~

DATO CHE $gr(g(q_1 - q_2)) = gr(r_2 - r_1)$, GIUNGO HO CHE $m + gr(q_1 - q_2) = gr(r_2 - r_1) < m$

Quindi $m + gr(q_1 - q_2) < m$. ↗ ALTRIMENTI NON AVREMMO MAI $gr(q_1 - q_2) < m$

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:

$\mathbb{Z}[x] \ldots \mathbb{Q}[x], \mathbb{R}[x]$

7)* Inoltre, se X fosse invertibile allora varrebbe la formula di addizione dei gradi

↳ CHI È IL GRADO DI $\frac{1}{X}$?

Il grado di X è 1 $(gr(X) = 1)$

Se faccio una cosa tipo $X \cdot f = 1$, visto che $cd(X) = 1$ allora vale la formula di addizione dei gradi, essendo cancellabile. Allora avrei che: $gr(X) + gr(f) = gr(1) = 0$, ma $gr(X) = 1$ e dato che $gr(X) \leq gr(X) + gr(f)$ io sto dicendo che $1 \leq 0$ ↯

SE X HA COD INVERTIBILE ALLORA CD È CANCELLABILE E TROVO CON COD CANCELLABILE DO ANCHE SE CANCELLABILI E PER LORO VALE LA FAG

Correzione esercizi 08/12/2021 (LEZIONE 33)

3) • $(g, \cdot)$ è un gruppo ciclico di ordine 19: $g = \langle x \rangle$
↳ È DI 19 ELEMENTI

Per definizione, $g = \langle x \rangle = \{x^m \mid m \in \mathbb{Z}\}$, di conseguenza $g = \{x^0, x^1, x^2, \dots, x^{18}\}$

↳ DOPO x^{18} C'È x^0 PERCHÉ VOGLIAMO CHE g ABBIA 19 ELEMENTI
↳ $x^{19} = x^0 = 1_g$

↳ $x^0 = 1_g$ (l'elemento neutro di g)

$x^m \cdot x^0 = x^{m+0} = x^m$

$x^m = x^n \iff m \equiv_{19} n$ ↳ DATO CHE $x^a = x^b \iff a \equiv_m b$ con $m = |\langle x \rangle|$ DEL 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 VEDIAMO NEGLI ESPONENTI

$x^{23} = x^5 \cdot x^{18} = x^4 (x \cdot x^{18}) = x^4 \cdot x^{19} = x^4 \cdot 1_g = x^4$

↳ Infatti notiamo che $23 \equiv_{19} 4$

Quindi, dire che x ha periodo n vuol dire che $|\langle x \rangle| = n$ → 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^7?

↳ $(x^5)^k = x^7$ → Esiste $k \in \mathbb{N}$: $5k \equiv_{19} 1$

DOMANDA: PERCHÉ $n \in \mathbb{Z}$ MA LI PRENDIAMO SOLO POSITIVI?

Anche se $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$, prendiamo gli esponenti solo positivi perché, in realtà, essendo il gruppo ciclico, ogni esponente negativo può essere riscritto con esponente positivo.

ESEMPIO: $x^{-30} = x^{-30} \cdot (1_g)^2 = x^{-30} \cdot (x^{19})^2 = x^{-30} \cdot x^{38} = x^8$

Infatti, $DE(-30, 19) = (\dots, 8)$

Io voglio sapere se esiste, non chi è → POTREBBE ESSERE DIFFICILE TROVARLO, COME NEL CASO DI: $5k \equiv_{119} 1$

↳ Sì, esiste, perché sappiamo che $[5]_{19} \cdot [k]_{19} = [1]_{19}$ esiste se e solo se 5 e 19 sono coprimi → IN QUESTO CASO $k = 4$ PERCHÉ $4 \cdot 5 = 20$ E $20 - 19 = 1$

CHE VUOL TROVARE L'INVERSO DI $[5]_{19}$

$|\langle x^5 \rangle| = ?$ → CIOÈ QUANTI ELEMENTI CI SONO IN $\langle x^5 \rangle$

$$\langle x^5 \rangle = \{ \underset{1_g}{\underset{\shortparallel}{(x^5)^0}}, x^5, \underset{x_{10}}{\underset{\shortparallel}{(x^5)^2}}, \underset{x_{15}}{\underset{\shortparallel}{(x^5)^3}}, \underset{x_{20} = x^{19} \cdot x = x}{\underset{\shortparallel}{(x^5)^4}}, (x^5)^5, (x^5)^6, \dots$$

↳ IN REALTÀ IN OGNI SOTTOGRUPPO C'È UNA POTENZA CHE DÀ L'UNITÀ PERCHÉ $a \in 19$ SONO COPRIMI QUINDI a È SEMPRE INVERTIBILE

↳ $ax \equiv_{19} 1$ se $a \not\equiv_{19} 0$

$(x^5)^4 = x$, cioè mi sono trovato che:

$x \in \langle x^5 \rangle \rightarrow \langle x \rangle \leq \langle x^5 \rangle \rightarrow g = \langle x^5 \rangle$

↳ 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) $12001 + 47^{202}(5^{36} - 15 \cdot 69) + 5$ P.M. ORE

↳ POST MERIDIEM

Sappiamo che se sono le 5 di pomeriggio, dopo 24 ore saranno ancora le 5 di pomeriggio, dopo 25 ore saranno le 6 di pomeriggio

↓

$[12001 + 47^{202}(5^{36} - 15 \cdot 69)]_{24}$ → Sfruttiamo le proprietà

↳ Così calcoliamo il resto della DE di questo numero con 24, cioè quante ore di differenza ci sono con quella iniziale (5 P.M)

$[a+b] = [a] + [b]$ e

$[a \cdot b] = [a] \cdot [b]$

↓

$[12001]_{24} + [47^{202}]_{24} \cdot ([5^{36}]_{24} - [15]_{24} \cdot [69]_{24})$

• $24 \mid 12000$

↳ $12001 \bmod 24 = 1$, quindi $[12001]_{24} = [1]_{24}$

• $47 \equiv_{24} -1$

↳ $47 = 48 - 1 = 2 \cdot 24 - 1 \leftrightarrow 47 \bmod 24 = 23$, quindi $[47^{202}]_{24} = [-1^{202}]_{24}$

NON RICORDO SUPERE 23 QUINDI CI CONVIENE CONSIDERARE UN RAPPRESENTANTE DELLA CLASSE PIÙ SEMPLICE

INVECE DI ANDARE AVANTI CON IL RAPPRESENTANTE, VAGO INDIETRO

Posso scegliere il rappresentante che voglio, infatti:

$4^2 \equiv_5 16 \equiv_5 1$ ma $4^2 \equiv_5 (-1)^2 = 1$

Quindi:

SONO IN REALTÀ $[3\cdot 5\cdot 8\cdot 8]_{24}$, QUINDI POSSO USARE LA COMMUTATIVITÀ → FACCIO USCIRE UN 24 COSÌ LA CLASSE È 0

$$[1200^1]_{24} + [47^{202}]_{24}\left([5^{36}]_{24} - \overbrace{[15]_{24}\cdot[69]_{24}}\right) =$$

$$= [1]_{24} + [-1^{202}]_{24}\left(\underbrace{[25^{18}]_{24}}_{\text{è } [1^{18}]_{24}} - \underbrace{[3\cdot 8]_{24}}_{\equiv 0}\cdot[5\cdot 8]_{24}\right) = [1]_{24} + [1]_{24}\left([1^{18}]_{24} + [0]_{24}\right) = [2]_{24}$$

Quindi sono le 7 P.M.

Se avessi avuto $[12]_{24}$ sarebbero state le 5 A.M.

13) $4x^4 + 3x^3 + 2x + 1 : x^2 + x + 2$ $\quad \mathbb{Q}[x]$ → POSSO FARE LA DIVISIONE PERCHÉ $cd(x^2+x+2)$ È INVERTIBILE

↳ LO È PERCHÉ IN $\mathbb{Q}$ TUTTI I NUMERI SONO INVERTIBILI

DIVIDO I COEFFICIENTI DIRETTORE E FACCIO $m-n$

$$\begin{array}{l|l}
4x^4 + 3x^3 + 0x^2 + 2x + 1 & x^2 + x + 2 \\
\hline
\underline{4x^4 + 4x^3 + 8x^2} & 4x^2 - x - 7 \\
// \quad -1x^3 - 8x^2 + 2x + 1 & \\
\underline{-x^3 - x^2 - 2x} & \\
// \quad -7x^2 + 4x + 1 & \\
\underline{-7x^2 - 7x - 14} & \\
// \quad 11x + 15 &
\end{array}$$

SOTTRAGGO

SONO I cd E FACCIO $m-n$

↳ L'ALGORITMO SI È FERMATO PERCHÉ IL GRADO DEL RESTO È MINORE DI x^2+x+2

↓ NON POSSO CONTINUARE PERCHÉ x NON È MAI INVERTIBILE

↳ $\frac{1}{x} \notin \mathbb{Q}[x]$

POSSIAMO FARE LA PROVA

$f = g\cdot q + r$

$4x^4 + 3x^3 + 2x + 1 = (x^2+x+2)(4x^2-x-7) + 11x + 15$

TEOREMA

Se un gruppo ciclico ha ordine primo allora tutti i suoi sottogruppi ciclici diversi dall'unità sono tutto quanto il gruppo

↳ PER CAPIRE VEDERE L'ESERCIZIO 3 DI OGGI

OMOMORFISMO DI SOSTITUZIONE

Sia $f \in A[x]$ con $f = a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m$ → UN POLINOMIO

e con $a_m \neq 0$ → CIOÈ a_m È IL COEFFICIENTE DIRETTORE

Sia $c \in A$. Definisco:

$f(c) := a_0 + a_1 c_1 + a_2 c^2 + \dots + a_m c^m \in A$ → CIOÈ VALUTO IL POLINOMIO IN c → APPARTIENE AD A PERCHÉ SONO ANCORA SOMMA E PRODOTTO DI ELEMENTI DI A

Definisco l'omomorfismo di sostituzione:

$f \in A[x] \longmapsto f(c) \in A$ → DIMOSTRARE CHE È UN OMOMORFISMO DI ANELLI PER ESERCIZIO

APPLICAZIONE POLINOMIALE

- Sia $f \in A[x]$, definisco l'applicazione polinomiale di f la funzione:

$\bar{f} : c \in A \longmapsto f(c) \in A$ → È COME VEDIAMO I POLINOMI IN ANALISI → L'APPLICAZIONE POLINOMIALE DI X È $\bar{f} = x$

- Se $f = a_0$ (POLINOMIO COSTANTE), allora $(\forall c \in A)(\bar{f}(c) = a_0)$ ← L'APPLICAZIONE POLINOMIALE È UNA FUNZIONE COSTANTE

RADICE DEL POLINOMIO

- Se $f(c) = 0_A$ (ELEMENTO NEUTRO DELLA SOMMA IN A), c si dice radice di f.
- Si vede facilmente che se $f, g \in A[x]$ e $c \in A$, allora:

$\overline{f+g}(c) = \bar{f}(c) + \bar{g}(c)$ ← METTERLO O NON METTERLO IL SECONDO È UGUALE → INFATTI $\bar{f}(c) = \bar{f}_1(c)$ PER DEFINIZIONE

$\overline{f \cdot g}(c) = \bar{f}(c) \cdot \bar{g}(c)$

APPLICAZIONE POLINOMIALE

L'APPLICAZIONE POLINOMIALE È UN OMOMORFISMO

- 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 $c \in A$.

Allora $f(c)$ è il resto della divisione lunga tra f e $(X-c)$

↳ POSSO FARE LA DIVISIONE PERCHE' IL COEFFICIENTE DIRETTORE DI $X-c$ E' 1, CHE E' CANCELLABILE

NON POSSO FARE $3X : 5$ IN $\mathbb{Z}[X]$ PERCHE' CON DI 5 NON E' INVERTIBILE IN $\mathbb{Z}[X]$

<u>DIM</u> CIOE' FACCIO LA DIVISIONE LUNGA

Parto $f = \overline{(X-c)} \cdot \bar{q} + \bar{r}$ con $gr(r) < \overbrace{gr(X-c)}^{1}$,

allora dato che $gr(r) < 1$, r è un polinomio costante. Quindi: $f(c) = \underbrace{(c-c)}_{=0} q(c) + \underbrace{r(c)}_{\text{E' COSTANTE QUINDI LO CHIAMO } r_0} = r_0$ ↳ QUINDI $f(c) = r_0$

TEOREMA DI RUFFINI

Sia A un anello commutativo unitario, $f \in A[X]$ e $c \in A$

Allora c è radice di f se e solo se $(X-c) \mid f$ ↳ $\overset{\text{DIM}}{=}$ DEL TEOREMA DEL RESTO

$(\rightarrow)$ QUINDI $r=0$, CIOE' $(X-c) \mid f$

$(\leftarrow)$ CIOE' $r=0$ QUINDI c E' RADICE

TEOREMA DI RUFFINI GENERALIZZATO

Sia A un dominio di integrità, sia $f \in A[X]$ ↳ UN POLINOMIO DI $A[X]$ e siano $c_1, c_2, \dots, c_m \in A$ $\underbrace{\text{a 2 a 2 distinti}}_{(\forall i,j \in \mathbb{N})(1 \leq i,j \leq m \rightarrow (c_i = c_j \leftrightarrow i = j))}$ → CIOE' $c_i \neq c_j$

Allora $c_1, c_2, \dots, c_m$ sono radici di f se e solo se $\prod_{i=1}^{m} (X-c_i)$ divide f.

↳ si legge: il prodotto, i da 1 a m di $X-c$ con i

↳ CIOE', $(X-c_1) \cdot (X-c_2) \cdot (X-c_3) \cdot \dots \cdot (X-c_m)$

<u>DIM</u> Per dimostrarlo useremo l'induzione di I forma

$(\rightarrow)$ su m

Caso Base) $m=1$ → Per $m=1$ si ha il teorema di Ruffini

Passo Induttivo)

Suppongo $m > 1$ e vero l'asserto per $m-1$

Dato che e_m è radice, ho $f(e_m)=0$, allora per Ruffini abbiamo che $f=(X-e_m)\,g$, cioè $X-e_m \mid f$

- Se $1 \leq i < m$, $f(e_i)=(e_i-e_m)\,g(e_i)$. Allora:

Dato che siamo in un dominio di integrità e che i e m sono a due a due distinti, ovvero $(e_i-e_m)\neq 0$, essendo $f(e_i)=0$ perché e_i è una radice di f (per ipotesi), allora, per la legge di annullamento del prodotto, $g(e_i)=0$

Quindi $(\forall i \in \mathbb{N})(1 \leq i \leq m-1 \rightarrow g(e_i)=0)$ → cioè tutti i e_i sono zeri di g

Per ipotesi di induzione, allora abbiamo che:

$$g = h \cdot \prod_{i=1}^{m-1}(X-e_i), \quad \text{quindi} \quad f = \underbrace{(X-e_m)\cdot g}_{\text{ez. ipotesi}} = h \prod_{i=1}^{m}(X-e_i)$$

PERCHÉ g È MULTIPLO DI $\prod_{i=1}^{m-1}(X-e_i)$

↳ QUESTA È LA TESI

($\Leftarrow$) Esiste $h \in A[X]$: $f = h \cdot \prod_{i=1}^{m}(X-e_i)$ → cioè $\prod_{i=1}^{m}(X-e_i)$ 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 arriveremo ad avere nel prodotto un fattore uguale a 0.

ESEMPIO:

- Siano e_1, e_2, e_3 radici di f.

Allora il polinomio $(X-e_1)(X-e_2)(X-e_3) \mid f$ e viceversa.

TEOREMA

Se A è un dominio di integrità, $f \in A[x] \setminus \{0_A\}$ (POLINOMIO NULLO) e f ha n radici distinte, allora $n \leq gr(f)$

↳ NON POSSO AVERE PIÙ RADICI DEL GRADO

<u>DIM</u>

Dico $e_1, e_2, \dots, e_n$ le n radici distinte di f e dico $\prod_{i=1}^{n}(x-e_i) = g \rightarrow g$ è IL PRODOTTO DI TUTTI GLI $(x-e_i)$

Per il teorema di Ruffini generalizzato, ho che $\exists h \in A[x]$ tale che $f = h \cdot g$

Ma A è un dominio di integrità e $g \neq 0$, dunque vale la formula di addizione dei gradi.

↳ $gr(f) = gr(g) + gr(h)$, ovviamente $gr(g) + gr(h) \geq gr(g)$.
Ma $gr(g) = n$ perché è il prodotto di n polinomi di grado 1, quindi ho che $gr(f) \geq gr(g) \rightarrow n \leq gr(f)$

ATTENZIONE!

Se non siamo in un dominio di integrità, non vale.

- $f = [2]_4 X \in \underbrace{\mathbb{Z}_4(X)}_{\text{NON È UN DOMINIO DI INTEGRITÀ}}$

$f([0]_4) = [4]_4 = [0]_4$ e $f([2]_4) = [0]_4$, cioè f ha più radici distinte anche se $gr(f) = 1$ 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 O I POLINOMI È LA STESSA COSA

PER QUESTO IN DI DEFINISCO I POLINOMI COME APPLICAZIONI POLINOMIALI

DIM

($\rightarrow$) È ovvio per la definizione di applicazione polinomiale

($\leftarrow$) Definiamo $h = f - g$.

Poiché $\bar{f} = \bar{g}$ (IPOTESI), cioè $(\forall c \in A)(h(c) = \bar{h}(c) = \overline{f-g}(c) = \overbrace{\bar{f}(c) - \bar{g}(c)}^{\text{SONO UGUALI}} = 0)$

Poiché A è infinito, h ha infinite radici. Per il teorema precedente, allora, $h = 0$. Infatti, trovandoci in un dominio di integrità, se non fosse 0 dovrebbe avere il grado maggiore delle radici (CHE È INFINITE). Quindi $f = g$.

ESEMPIO:

- $f = x^3 - x \in \mathbb{Z}_3[x]$

$\bar{f}([0]_3) = [0]_3^3 - [0]_3 = [0]_3$

$\bar{f}([1]_3) = [1]_3^3 - [1]_3 = [0]_3$

$\bar{f}([2]_3) = [2]_3^3 - [2]_3 = [2]_3 - [2]_3 = [0]_3$

Quindi $\bar{f} = \bar{0}$, questo perché essendo $\mathbb{Z}_3$ finito qualche applicazione polinomiale deve coincidere, anche se i polinomi sono infiniti → VA DA $\mathbb{Z}_3 \to \mathbb{Z}_3$

Correzione esercizi 14/12/2021 (LEZIONE 30)

5) a. $x \in ASSOC(y) \leftrightarrow x \in DIV(y) \wedge y \in DIV(x)$

Se x è cancellabile allora $ASSOC(x) = \{ux \mid u \in U(a)\}$

↳ $\left.\begin{matrix} x = ky \\ y = hx \end{matrix}\right\}$ $x = khx$

GIUSTO DAR ESEMPIO DI ANELLI TALI CHE ↳ ALMENO UNO NO!

$\mathbb{Z}_9$ è integro? NO → Quindi nemmeno $\mathbb{Z}_9[x]$ è integro

↳ $[3]_9 \cdot [3]_9 = [9]_9 = [0]_9$

CON $\bar{m}$ INDICO $[m]_9$

$f = \bar{2}x^3 + \bar{2}x^2 \in \mathbb{Z}_9[x]$ → BISOGNA TROVARE UN POLINOMIO MONICO E ASSOCIATO

↳ $f = \bar{2}(x^3 + x^2)$

Se $cd(f)$ è cancellabile → f è cancellabile → Allora gli ASSOC sono del tipo $\{ux \mid u \in U(a)\}$ → QUINDI C'È ANCHE QUELLO MONICO SE PONGO $u = 1$

↓ $\bar{2}$ è invertibile perché invertibile ($\bar{2} \cdot \bar{5} = \bar{10} = \bar{1}$) ↳ 2 è COPRIMO CON 9

- Se ho $x^3 + x^2$, $(x^3 + x^2)\bar{2} = f$ → Quindi $x^3 + x^2 \in DIV(f)$
- Se faccio $f \cdot \bar{5} = x^3 + x^2$ → Quindi $f \in DIV(x^3 + x^2)$ ↳ INVERSO DI $\bar{2}$

Quindi $x^3 + x^2$ è un polinomio monico ed è un associato di f perché si dividono reciprocamente

b. $\bar{4}x^2 + \bar{8}$ → Anche 4 è invertibile perché cancellabile

↳ L'inverso di $\bar{4}$ è $\bar{7}$ dato che:

$\bar{7} \cdot \bar{4} = \overline{28} = \bar{1}$

$\bar{7}(\bar{4}x^2 + \bar{8}) = x^2 + \bar{2}$ → [Se moltiplico il polinomio con l'inverso del coefficiente direttore trovo il polinomio monico associato a quel polinomio]

Per trovare l'inverso di $[4]_9$ avrei potuto fare la divisione Euclidea

↳ $DE(4, 9)$ → $9 = 2 \cdot 4 + 1$

↳ $9 - 2 \cdot 4 = 1$ → $[9 - 2 \cdot 4]_9 = [1]_9$ → $[-2]_9 \cdot [4]_9 = [1]_9$

$[-2 + 9]_9 \cdot [4]_9 = [1]_9$ → $[7]_9 \cdot [4]_9 = [1]_9$

FATTORIZZAZIONE IN UN ANELLO DI POLINOMI

Sappiamo che i divisori banali di f sono gli invertibili e gli associati di f.

ESEMPIO:

- $f = \bar{2}x \in \mathbb{Z}_4[x]$ è irriducibile?

DATO CHE $\bar{2}$ È INVERTIBILE, È CANCELLABILE. È CARATTERISTICO $\text{Assoc}(f) = \{u \cdot x \mid u \in U(a)\}$

$$\text{BDIV}(f) = U(\mathbb{Z}_4[x]) \cup \text{Assoc}(f)$$

$$U(\mathbb{Z}_4[x]) = \{\bar{1}, \bar{2}\} \qquad \text{Assoc}(f) = \{\bar{1}f, \bar{2}f\}$$

ESSENDO $\mathbb{Z}_4$ UN CAMPO, GLI INVERTIBILI SONO TUTTI TRANNE LO 0

Quindi $\text{BDIV}(f) = \{\bar{1}, \bar{2}, f, \bar{2}f\}$ → Un polinomio è irriducibile se non è invertibile e ha solo divisori banali

Preso $f = h \cdot g$ (UN CERTO DIVISORE DI f), per la formula di addizione dei gradi abbiamo che: $1 = gr(f) = gr(g) + gr(h)$ → ALMENO UNO DEI DUE È VERO $gr(g) = 1$ E $gr(h) = 0$ O VICEVERSA

In $\mathbb{Z}_4[x]$ i polinomi:

- DI GRADO 1: $x, \bar{2}x, x+\bar{1}, x+\bar{2}, \bar{2}x+\bar{1}, \bar{2}x+\bar{2}$ → QUESTI NON POSSONO ESSERE DIVISORI DI f PERCHÉ NON C'È IL TERMINE NOTO IN f
- DI GRADO 0: $\bar{1}, \bar{2}$ → QUESTI SONO I DIVISORI DI f → INFATTI SONO PROPRIO I $\text{BDIV}(f)$

TEOREMA

Se $(a, +, \cdot)$ è un campo e se x è cancellabile, allora:

$$\text{Assoc}(x) = \{u \cdot x \mid u \in a \setminus \{0\}\}$$

→ INOLTRE, DATO CHE IN QUESTA COSA IN a SONO TUTTI INVERTIBILI TRANNE LO 0

COROLLARIO

Se $(a, +, \cdot)$ è un campo, ogni polinomio non nullo di $a[x]$ è associato ad un <u>unico</u> polinomio monico. Questo polinomio viene detto rappresentante monico della classe di f

SAPPIAMO CHE QUESTO POLINOMIO ESISTE PERCHÉ, ESSENDO $(a, +, \cdot)$ UN CAMPO, ALLORA IL $cd(f)$ È SICURAMENTE INVERTIBILE. MOLTIPLICANDO f PER L'INVERSO DI $cd(f)$ OTTENGO L'UNICO POLINOMIO MONICO E ASSOCIATO A

UNICITÀ DATA DALL'UNICITÀ DELL'INVERSO

TEOREMA

Sia A un campo $(A,+,\cdot)$ 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

$\Rightarrow$ 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 anelli fattoriali e dall'unicità del polinomio monico associato $\Rightarrow$ COROLLARIO DI PRIMA

Dobbiamo dimostrare l'esistenza (DELLA SCOMPOSIZIONE) per induzione di prima forma su $gr(f)$ (che chiamo n).

- Se $gr(f) = 0$, è ovvio che f si decompone come un certo $c \in A$
- Suppongo $n > 0$ e vero l'esistenza per $n-1$

$\downarrow$

ESSENDO $A[X]$ è fattoriale, quindi prendo una decomposizione irriducibile di f, avrò $f = h_1 \cdot h_2 \cdots h_m$ irriducibili (HO POSTO PRIMA)

Scrivo:

$$\left.\begin{aligned} g_i &:= cd(h_i)^{-1} \cdot h_i \\ c &:= \prod_{i=0}^{n} cd(h_i) \end{aligned}\right\}$$

IO FACCIO DIVENTARE TUTTI GLI $h_1 \cdot h_2 \cdots h_m$ MONICI E HO RAGGRUPPATO TUTTI I LORO COEFFICIENTI DIRETTORI IN c, CHE È IL PRODOTTO DI TUTTI I $cd(h_1), cd(h_2), \dots, cd(h_m)$ $\Rightarrow$ CIOÈ LI HO MESSI IN EVIDENZA

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'asserto è vero $\forall m \in \mathbb{N}$

ESEMPIO:

$f = (\bar{2}x+1)(\bar{3}x+\bar{2}) \in \mathbb{Z}_5[x]$ → È UN CAMPO → ABBIAMO L'IPOTESI

- $(\bar{2}x+\bar{1}) = \bar{2}(x+\bar{3})$ → METTO IN EVIDENZA IL $\bar{2}$ → $\bar{2} := [2]_5$
- $(\bar{3}x+\bar{2}) = \bar{3}(x+\bar{4})$ → METTO IN EVIDENZA IL $\bar{3}$ → $\bar{3} := [3]_5$

Quindi posso scrivere $f = \bar{2}\cdot\bar{3}\cdot(x+\bar{3})(x+\bar{4}) = \bar{1}\cdot(x+\bar{3})(x+\bar{4}) = (x+\bar{3})(x+\bar{4})$

UNA DECOMPOSIZIONE IN POLINOMI MONICI E IRRIDUCIBILI

TEOREMA

Sia A un campo, $f \in A[x] \setminus \{0\}$ e consideriamo $m = gr(f)$

f è irriducibile se e solo se $m > 0$ e vale:

1) $(\forall g, h \in A[x])(f = g\cdot h \rightarrow gr(g) = m \text{ XOR } gr(h) = m)$
2) $(\forall g, h \in A[x])(f = g\cdot h \rightarrow gr(g) = 0 \text{ XOR } gr(h) = 0)$

EQUIVALENTE → DEVE ESSERE ALMENO UNA DELLE DUE

DIM

(←) Se $gr(f) > 0$, allora $f \notin U(A[x])$. Infatti, se A è un campo gli invertibili di $A[x]$ sono tutti gli invertibili di A (E CIOÈ PERÒ HANNO gr 0)

Se $f = g\cdot h$, dato che vale 1), posso supporre $gr(g) = m$ e, di conseguenza, per la formula di addizione dei gradi, $gr(h) = 0$ → CIOÈ PROPRIO QUELLI CON gr UGUALE A 0 (CIOÈ g E h SONO DIVISORI DI f)

MA IN UN CAMPO, LE COSTANTI SONO QUELLI INVERTIBILI.

↳ $h \in U(A[x])$ → ci sono solo divisori banali → INFATTI h È INVERTIBILE → E g È ASSOCIATO

(→) Se $f \notin (U(A[x]) = U(A) = A \setminus \{0\})$ e $DIV(f) = BDIV(f)$, allora $gr(f) > 0$ dato che $f \notin A \setminus \{0\}$ → f NON È UNA COSTANTE

DEFINIZIONE DI IRRIDUCIBILE

VOGLIAMO DIMOSTRARE CHE VALE LA 1) O LA 2)

Sia $f = g\cdot h$. A è un campo, quindi f è cancellabile.

→ Di conseguenza, $BDIV(f) = \{u\cdot f \mid u \in A \setminus \{0\}\} \cup A \setminus \{0\}$ → ASSOCIATI → INVERTIBILI

TUTTI I DIVISORI SONO SOLO QUELLI BANALI

↓ Im questo caso, $gr(g) = 0 \vee gr(h) = 0 \overset{\text{PER FAG}}{\longleftrightarrow} gr(g) = m \vee gr(h) = m$

VALE XOR PERCHÉ ESISTE UN SOLO DIVISORE DI GRADO m → f NON È INVERTIBILE

TEOREMA

Sia A un campo e $f \in A[X]$ → f È UN POLINOMIO

f ha radici in A se e solo se ha almeno un divisore di grado 1 in A[X]

DIM

(→) È vero per il teorema di Ruffini

(←) È vero perché sappiamo che ogni polinomio di 1 grado ha radici in un campo. Infatti se ho $kX+h$, posso prendere:

↳ $c = -hk^{-1}$ che è radice del polinomio.

→ $f = g(kX+h)$ ha radice perché $kX+h$ ce l'ha.

TEOREMA → PER L'IRRIDUCIBILITÀ DI UN POLINOMIO ANDIAMO A VEDERE SE HA RADICI, PERCHÉ CERCARE TUTTI I DIV(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 $(X-c) \in DIV(f)$ perché vale la 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

(→) Se ha delle radici allora per il teorema di prima non è irriducibile

(←) Se f non è irriducibile allora è diviso da qualcosa RUFFINI, ma per la FAG è un divisore di grado 1 o 2, cioè non ha radici

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 f 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

↳ f non è irriducibile → PERCHÉ HA DUE DIVISORI (x^2+1) E (x^2+1) CHE NON SONO RADICI e non ha radici in $\mathbb{Q}$

- $2 \in \mathbb{Z}[X]$ → $\mathbb{Z}[X]$ NON È UN CAMPO, QUINDI 2X PUR AVENDO GRADO 1 NON È IRRIDUCIBILE → GLI IRRIDUCIBILI SONO SOLO I PRIMI E X

$2 \notin U(\mathbb{Z}[X])$ perché 2 non è invertibile in $\mathbb{Z}$

2 è irriducibile in $\mathbb{Z}[X]$ perché non invertibile e divisibile ha solo

2X ha grado 1 e non è irriducibile perché è un prodotto di irriducibili

TEOREMA FONDAMENTALE DELL'ALGEBRA

NO DIM

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 → NO DIM

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

$\Delta = b^2-4ac \rightarrow$ Se $\Delta \geq 0$ $\quad x_{1,2} = \frac{-b \pm \sqrt{\Delta}}{2a}$

RADICI IN $\mathbb{Q}[x]$

ESEMPIO

- $3x^4 + \frac{1}{90}x + \frac{3}{4} = \frac{1}{180}(540x^4 + 2x + 135)$

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 IRRIDUCIBILITA' DI EISENSTEIN → NO DIM

Sia $f = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \in \mathbb{Z}[x]$ con $a_n \neq 0$

↓ cioè, per trovare una radice in $\mathbb{Q}$ moltiplico il polinomio per il minimo comune denominatore e trovo un polinomio in $\mathbb{Z}[x]$

↳ il coefficiente direttore

Se esiste un numero primo p:

1) p divide $a_0, a_1, \dots, a_{n-1}$
2) $p \nmid a_n$
3) $p^2 \nmid a_0$

Allora f è irriducibile in $\mathbb{Q}[x]$

ESEMPIO:

- $\frac{1}{10}x^4 + \frac{3}{10} = f$

f ha radici in $\mathbb{Q}[x] \Leftrightarrow 10 \cdot f$ ha radici in $\mathbb{Q}[x]$

$x^4 + 3 = 10f \in \mathbb{Z}[x]$ e trovo il primo p:

$p = 3 \to a_0 = 3,\ a_1 = 0,\ a_2 = 0,\ a_3 = 0,\ \underline{a_4 = 1}$ → $3 \nmid a_4$

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

↳ Questa 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 DIM

f È UN POLINOMIO IN $\mathbb{Z}[X]$ NON NULLO

Sia $f \in \mathbb{Z}[X] \setminus \{0\}$, $cd(f) = a_m$, $f(0) = a_0$ → CIOÈ IL TERMINE NOTO È a_0

Se $e \in \mathbb{Q}$ e $f(e) = 0$, allora $e = \frac{u}{v}$ dove $v | a_m$ e
(e È UNA RADICE RAZIONALE DI f)
$u | a_0$ con a_0 e a_m coprimi

COROLLARIO

Sia $f \in \mathbb{Z}[X] \setminus \{0\}$ monico. Allora tutte le radici razionali di f sono intere

PERCHÉ?

$e = \frac{u}{v}$ per il teorema precedente. Dato che in un polinomio monico $a_m = 1$, allora $v | 1 \rightarrow e = \pm u$
↳ $v = \pm 1$

ESEMPIO:

- $f = X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{R}[X]$ → Scomporre in polinomi irriducibili su $\mathbb{R}[X]$ e su $\mathbb{C}[X]$

So che $(X^3+1) | f$

Faccio la divisione lunga:

$$
\begin{array}{l|l}
X^5 + X^4 + X^3 + X^2 + X + 1 & X^3 + 1 \\
\hline
\text{SOTTRAGO } X^5 + 0 + 0 + X^2 + 0 + 0 & X^2 + X + 1 \\
\quad X^4 + X^3 + 0 + X + 1 & \\
\text{SOTTRAGO } X^4 + 0 + 0 + X + 0 & \\
\quad X^3 + 0 + 0 + 1 & \\
\quad X^3 + 0 + 0 + 1 & \\
\quad 0 &
\end{array}
$$

IN EFFETTI $(X^3+1) | f$

Quindi, $f = (X^2 + X + 1)(X^3 + 1)$ → SU $\mathbb{R}[X]$ NON ESISTONO POLINOMI IRRIDUCIBILI DI GRADO SUPERIORE AL SECONDO

Noto che $(-1)^3 + 1 = 0$, quindi posso ancora scomporre (X^3+1) dato che ha radice -1 → $X+1 | X^3+1$

$(x^3+1)=(x+1)(x^2-x+1)$ per Ruffini

posso farlo con la divisione lunga

$$\begin{array}{rrrr|l} x^3 & +0x^2 & +0x & +1 & x+1 \\ \cline{5-5} x^3 & +x^2 & & & x^2-x+1 \\ \cline{1-2} & -x^2 & & +1 & \\ & -x^2 & -x & & \\ \cline{2-3} & & x & +1 & \end{array}$$

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 DEL DISCRIMINANTE

INFATTI NON HANNO RADICI IN $\mathbb{R}[x]$

↳ Quindi questi due polinomi sono irriducibili su $\mathbb{R}[x]$

↓

$f=(x^2+x+1)(x+1)(x^2-x+1)$ è irriducibile su $\mathbb{R}[x]$

↳ $x+1$ è irriducibile perché di grado 1 e gli altri fattori sono irriducibili

• Scomporre f su $\mathbb{C}[x]$

Per il teorema fondamentale dell'algebra trovo c_1 radice di x^2-x+1 e c_2 radice di x^2+x+1

$x+1$ è irriducibile

↳ Per Ruffini ho che $x-c_1 \mid x^2-x+1$ e $x-c_2 \mid x^2+x+1$

Quindi posso dividere e scriverò che

• $x^2-x+1=(x-c_1)(x-d_2)$

IN REALTÀ NON CI IMPORTA CHI SIANO

CI IMPORTA CHE SAPPIAMO CHE ESISTONO

↳ Deve essere per forza di questo tipo dato che: Visto che x^2-x+1 è monico e $x-c_1$ è monico allora anche $x-d_1$ deve essere monico e deve avere grado 1 per la FAG

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

↳ $c_2=\frac{1+\sqrt{-3}}{2}$ e $d_1=\frac{1-\sqrt{-3}}{2}$

DATO CHE NEI NUMERI COMPLESSI $i=\sqrt{-1}$ e $i^2=-1$

$c_1=\frac{1+i\sqrt{3}}{2}$ e $d_1=\frac{1-i\sqrt{3}}{2}$

ESERCIZI + SPIEGAZIONE

LEZIONE 31

5) Esiste $u \in \mathbb{Z}$ tale che $3 | 2u-1$?

$3 | 2u-1 \leftrightarrow (\exists k \in \mathbb{Z})(2u-1 = \overset{[0]_3}{3k}) \rightarrow$ Quindi $u=2$ è soluzione.

Inoltre, $3 | 2u-1 \leftrightarrow [2]_3 [u]_3 = [1]_3 \rightarrow$ È UN'EQUAZIONE CONGRUENZIALE

$\hookrightarrow [2]_3^{-1}[u]_3 - [2]_3 = [0]_3$

La scrittura della classe di equivalenza è, ad esempio,

$[2]_3 = \{y \in \mathbb{Z} \mid 2 \equiv_3 y\} \leftrightarrow [2]_3 = \{y \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(2-y = 3k)\}$

Quindi $[2]_3$ sono tutte e sole le soluzioni perché 2 è una soluzione di $2u-1=3k$ in $\mathbb{Z}$

6) Esiste $u \in \mathbb{Z}$ tale che $23 | 79u-1$?

Cioè $(\exists k \in \mathbb{Z})(79u + 23k = 1)$?

$\hookrightarrow 79u-1 = 23k$ CON $k \in \mathbb{Z}$

Potrei applicare il teorema di Bezout $\rightarrow$ DEVO VEDERE IL MCD TRA 79 E 23

↳ Già so che il MCD tra 79 e 23 è uno dei divisori banali di 23 (dato che 23 è primo)

↳ Provo lo stesso con l'algoritmo delle divisioni successive

↳ $79 = 23 \cdot 3 + 10$

$23 = 10 \cdot 2 + 3$

$10 = 3 \cdot 3 + 1 \leftarrow$ MCD

$3 = 3 \cdot 1 + 0$

Preso $d | 79$ e $d | 23 \rightarrow d | 10 \rightarrow d | 3 \rightarrow d | 1$

↳ Per Bezout esistono $u, k \in \mathbb{Z}$: $\underset{\text{IL MCD}}{1} = 79u + 23k$, quindi la risposta all'esercizio è sì.

Di conseguenza, per trovare u e k:

$1 = 10 - 3 \cdot 3 = 10 - (23 - 10 \cdot 2) \cdot 3 = 10 + 10 \cdot 6 - 23 \cdot 3 =$

$= 10 \cdot 7 - 23 \cdot 3 = (79 - 23 \cdot 3) \cdot 7 - 23 \cdot 3 = 79 \cdot 7 - 23 \cdot 24$

Quindi $u = 7$ e $k = -24$, → PER TROVARE u E k POTREI ANCHE FARE UN'EQUAZIONE DIOFANTEA O DUE EQUAZIONI CONGRUENZIALI

$[u]_{23} \cdot [79]_{23} = [1]_{23}$

$[k]_{23} \cdot [23]_{23} = [1]_{23}$

infatti $1 = 79 \cdot 7 - 23 \cdot 24 = 553 - 552$

• Chiedere se $(\exists k \in \mathbb{Z})(79u + 23k = 1)$ è come chiedere se $[79]_{23}$ è invertibile

↳ $(\exists k \in \mathbb{Z})(79u + 23k = 1) \Leftrightarrow 79u \equiv_{23} 1 \Leftrightarrow [79]_{23}[u]_{23} = [1]_{23}$

$79u - 1 = 23 \cdot k$

LA CONDIZIONE DI INVERTIBILITÀ IN $(\mathbb{Z}_{23}, +, \cdot)$

$[79]_{23}$ è invertibile

$\Updownarrow$

$[10]_{23}$ è invertibile

↳ $10 \cdot 7 = 70 = 23 \cdot 3 + 1 \rightarrow [10]_{23} \cdot [7]_{23} = [1]_{23}$

LEZIONE 32

4) $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ → SONO PROPRIO LE UNICHE CLASSI IN $\mathbb{Z}_3$

$[0]_3 = [30]_3$, $[1]_3 = [-8]_3$, $[2]_3 = [11]_3$

$[-8]_3 = [1]_3$ perché $8 = 3 \cdot 2 + 2$, → O ANCHE: $-8 + 3 \cdot 3 = 1$

che passando ai negativi sarà $-8 = -3 \cdot 2 - 2$, ma il resto deve essere $0 \leq r < 3$

Quindi $-8 = 3 \cdot (-2) - 3 + 3 - 2$ → AGGIUNGO E ESTRAGGO 3

e $-8 = 3 \cdot (-2) - 3 + (3 - 2) = 3 \cdot (-3) + 1$

↳ METTO IN EVIDENZA

5) $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$

$0 \equiv_5 30 \leftarrow [30]_5$, $[11]_5$, $[-8]_5$

NO PERCHÉ MANCA UNA CLASSE, CIOÈ $[4]_5$

7) $(\forall a,b \in \mathbb{Z})((2 \nmid b) \to a*b = a+b) \wedge (2 \mid b \to a*b = a+\frac{b}{2}))$

$*: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ è un'operazione perché sappiamo sempre qual è l'immagine di una coppia

↳ $10*7=17$ ↳ Le coppie sono quelle che a destra o hanno un numero pari o dispari

↳ $11*8=15$

• Questa operazione non è commutativa, infatti $7*10=12$ che è diverso da $10*7=17$

$(\forall a,b \in \mathbb{Z})(a \equiv_2 b \wedge c \equiv_2 d) \to (a*c \equiv_2 b*d))$ è un'operazione congruenziale

$0 \equiv_2 0$ e $0 \equiv_2 2$ → DATO CHE * TOGLIE UN 2 DAI FATTORI SE b È PARI, QUINDI PER TROVARE UN CONTROESEMPIO USO b CHE HA UN SOLO 2 NELLA SCOMPOSIZIONE

↳ $0*0 = 0+0/2 = 0 \not\equiv_2 0*2 = 0+2/2 = 1$ ↗ SE AVESSI PROVATO CON $0*4 = 0+\frac{4}{2} = 2$, 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 $12 = 7 \cdot 1 + 5$

$[5]_7 \cdot [x]_7 = [3]_7 \iff 12x \equiv_7 3$

$5 \cdot 3 = 7 \cdot 2 + 1$, quindi $[3]_7$ è l'inverso di $[5]_7$

↳ $[5]_7 [3]_7 = [7 \cdot 2]_7 + [1]_7$

$[x]_7 = \underbrace{[3]_7 [5]_7}_{[1]_7} [x]_7 = [3]_7 [3]_7 = [9]_7 = [2]_7$

↳ CIOÈ HO MOLTIPLICATO $[5]_7 \cdot [x]_7 = [3]_7$ PER $[3]_7$

le soluzioni sono

$\{y \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(y = 2 + 7k)\} = [2]_7$

GRAFI

Un grafo è un insieme di punti e di archi.
Ecco un problema che può essere rappresentato tramite un grafo:
ALINGRAD (RUSSIA)
La teoria dei grafi nasce a Königsberg (Germania).
Questa città è attraversata dal fiume Pregel. Ci sono dei ponti che collega i vari punti della città.
Ciò che ci si chiese fu: È possibile attraversare tutti i ponti una sola volta andando su tutti i pezzi di terra?

IN QUESTO CASO I PONTI SONO RAPPRESENTATI DA ARCHI E LA TERRA DA PUNTI

GRAFO SEMPLICE

- Sia V un insieme tale che $V \neq \emptyset$ e ρ una relazione binaria simmetrica e antiriflessiva su V. (V, ρ) si dice grafo (semplice)
  NON È UNA RELAZIONE D'ORDINE PERCHÈ SIMMETRICA
- Gli elementi di V si dicono vertici del grafo.
- Le coppie $\{a,b\} \subseteq V : a\rho b$ si dicono archi o lati
  TALI CHE
  SONO COPPIE NON ORDINATE PERCHÈ $a\rho b = b\rho a$ (SIMMETRIA)

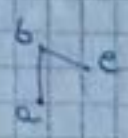
ALTRA DEFINIZIONE EQUIVALENTE DI GRAFO

PARTI CON DUE ELEMENTI DI V

Sia $V \neq \emptyset$ e sia $\ell \subseteq \mathcal{P}_2(V) = \{\{x,y\} \in \mathcal{P}(V) \mid x \neq y\}$.
(V, ℓ) lo dico grafo (semplice)
↳ Posso arrivare dalla prima alla seconda definizione e viceversa.
DALLA PRIMA ALLA SECONDA SI HA SE ρ È LA RELAZIONE DI APPARTENENZA A ℓ (È SIMM. E ANTIRIFL.)
↳ L'INSIEME DEGLI ARCHI È UN SOTTOINSIEME DI $\mathcal{P}_2(V)$

COME RAPPRESENTARLI?

Se $V = \{a,b,c\}$ e $\ell = \{\{a,b\},\{b,c\}\}$, il grafo sarà così fatto:



MULTIGRAFO → PIÙ ARCHI SUGLI STESSI VERTICI

Una terna di insiemi non vuoti (V, ℓ, σ) si dice multigrafo se $\sigma: \ell \to \mathcal{P}_2(V)$ → A ℓ_1 ASSOCIA LA COPPIA $\{a,b\}$, A ℓ_2 ASSOCIA $\{b,c\}$ ECC.

σ È UNA FUNZIONE

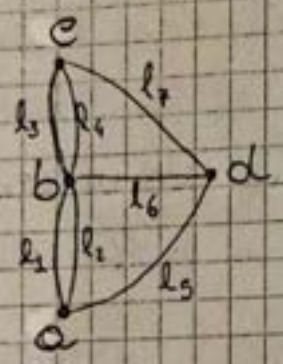
ℓ L'INSIEME DEI LATI

ESEMPIO:

PONTI DI KÖNIGSBERG

$V = \{a, b, c, d\}$

$\ell = \{\ell_1, \ell_2, \ell_3, \ell_4, \ell_5, \ell_6, \ell_7\}$



$\sigma(\ell_1) = \{a, b\} = \sigma(\ell_2)$

$\sigma(\ell_3) = \{b, c\} = \sigma(\ell_4)$

$\sigma(\ell_5) = \{a, d\}$

$\sigma(\ell_6) = \{b, d\}$

$\sigma(\ell_7) = \{c, d\}$

↳ IL PROBLEMA STA NEL VOLER ATTRAVERSARE UNA VOLTA TUTTI GLI ARCHI

TERMINOLOGIA

Sia (V, ℓ) un grafo.

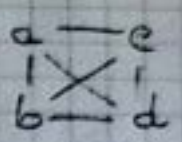
- Se $x, y \in V$ e $\{x, y\} \in \ell$, x e y si dicono estremi di $\{x, y\}$ e diremo che x e y sono adiacenti → C'È UN ARCO TRA LORO
- Archi che hanno vertici in comune, cioè $\cap \neq \phi$, si dicono incidenti → L'INTERSEZ TRA I DUE ARCHI
- Se $x \in V$, si denota con $d(x)$ e si dice grado di x il numero di archi che contiene x → NELL'ESEMPIO DI PRIMA, $d(a) = 3$
- Se $d(x)$ è dispari (o pari), diremo che x è dispari (o pari) → a È DISPARI

- 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 $\ell = \mathcal{P}_2(V)$ → OGNI VERTICE È COLLEGATO CON TUTTI GLI ALTRI

ESEMPIO:

Grafo completo a 4 vertici:



- Un grafo completo su n vertici si denota con K_n → K DI COMPLETO (IN TEDESCO)

- $(V, \mathcal{P}_2(V) \setminus \ell)$ si dice grafo complementare a (V, ℓ)
↳ HA GLI STESSI VERTICI MA GLI ARCHI SONO TUTTI E SOLI QUELLI CHE NON C'ERANO PRIMA

- Se $V' \subseteq V$ e $\ell' \subseteq \ell$, allora (V', ℓ') si dice sottografo di (V, ℓ)
↳ ALCUNI VERTICI E ALCUNI ARCHI DI QUELLI DI PRIMA

- Se l'insieme V è finito, il (multi)grafo si dice finito
↳ Anche se si hanno una quantità infinita di archi, l'importante è che i vertici siano finiti

- Se (V, ℓ) e (V', ℓ') sono grafi, una funzione $f: V \xrightarrow{BI} V'$ si dice isomorfismo tra (V, ℓ) e (V', ℓ') se:
↳ LA FUNZIONE È BIETTIVA

UN VERTICE STA IN UN ARCO SE E SOLO SE STA IN UN ARCO ANCHE DALL'ALTRA PARTE

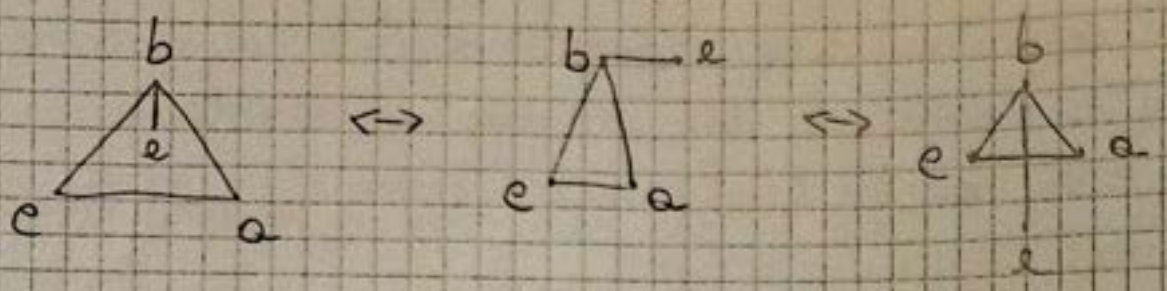
$$(\forall x, y \in V)(\{x, y\} \in \ell \Leftrightarrow \{f(x), f(y)\} \in \ell')$$

→ AUTOMORFISMO SE $(V, \ell) = (V', \ell')$

↳ Si conserva il grado degli elementi di V, il numero di vertici e il numero di lati

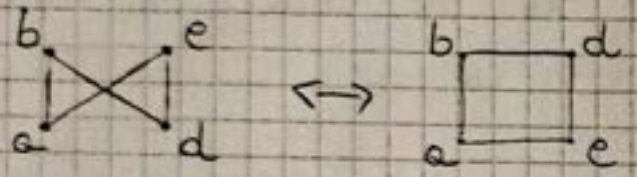
Per quanto riguarda la rappresentazione grafica, ci possono essere dei problemi perché due grafi isomorfi possono essere rappresentati in più modi

RAPPRESENTAZIONE GRAFICA DI GRAFI ISOMORFI



Sono lo stesso grafo!

Ciò può essere anche più complesso, ad esempio:



GRAFO PLANARE

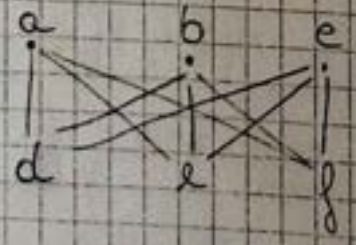
- Un grafo si dice piano o planare se è rappresentabile su un piano senza archi che si intersecano

Il problema dei grafi è che posso avere un grafo apparentemente non planare ma che in realtà lo è, come nei due esempi sopra.

Se ho, ad esempio, questi due grafi:

- K_5
  ↓
  GRAFO COMPLETO SU 5

- $K_{3,3}$
  ↓
  GRAFO BIPARTITO



→ COLLEGO a, b E c CON GLI ALTRI TRE
↓
TUTTI QUELLI IN ALTO O TUTTI QUELLI IN BASSO NON SI TOCCANO MAI

E' possibile riscrivere i grafi in modo da avere un grafo planare? Come faccio a saperlo?

↳ TEOREMA DI KURATOWSKI

TEOREMA DI KURATOWSKI → NO DIM

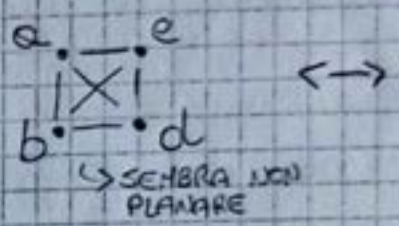
Un grafo finito è planare se e solo se non contiene né K_5 né $K_{3,3}$ come sottografi

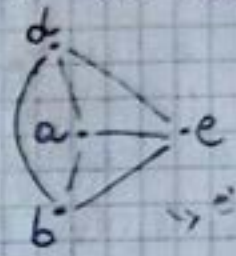
COROLLARIO:

K_5 e $K_{3,3}$ non sono planari

Non è detto che un grafo completo non è planare. → Solo i grafi completi da 5 in su non sono planari

ESEMPIO: K_4





TEOREMA SOMMA

Sia $(V, \mathcal{E})$ un grafo finito. Allora $2|\mathcal{E}| = \sum_{x \in V} d(v)$

IL NUMERO DI LATI

SE CI SONO UN NUMERO FINITO DI VERTICI ALLORA CI SONO UN NUMERO FINITO DI LATI PERCHÉ I LATI SONO UN SOTTOINSIEME DI $\mathcal{P}_2(V)$

x NEI VERTICI

DIM

Sia t il numero di estremi di qualche lato.

Quindi $t = 2|\mathcal{E}|$ → OGNI LATO HA DUE ESTREMI, QUINDI SE HO $|\mathcal{E}|$ LATI, IL NUMERO DI ESTREMI TOTALE È $2 \cdot |\mathcal{E}|$

Ma ogni vertice x è estremo di $d(x)$ lati.

Di conseguenza $t = \sum_{x \in V} d(x)$ → IL NUMERO DI ESTREMI DI QUALCHE LATO È LA SOMMA, PER TUTTI GLI $x \in V$, DEL GRADO DI x

ALTRE DEFINIZIONI

Sia $(V, \mathcal{E})$ un grafo.

- Siano $v_1, v_2, \dots, v_m \in V$ tale che: → CIOÈ, $v_1, v_2, \dots, v_m$ SONO VERTICI

$$(\forall i \in \mathbb{N})((1 \leq i \leq m-1) \rightarrow \{v_i, v_{i+1}\} \in \mathcal{E})$$

→ TRA v_1 E v_2 C'È UN ARCO, TRA v_2 E v_3 C'È UN ALTRO ARCO ecc... → TUTTI COLLEGATI

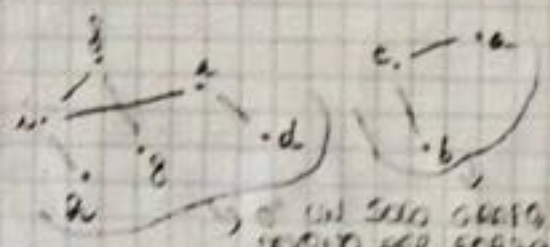
e l'insieme $\{\{v_1, v_2\}, \{v_2, v_3\}, \dots, \{v_{m-1}, v_m\}\}$ ha cardinalità m, la m-upla $(\{v_1, v_2\}, \dots, \{v_{m-1}, v_m\})$ si dice

si dice cammino da v_1 a v_m di lunghezza m.

- Per ogni $x \in V$ aggiungo il cammino nullo c_v da x a x di lunghezza 0 esempio: è un cammino
  ↳ ci dà la riflessività di γ
- Un cammino di lunghezza diversa da 0 da v_1 a v_m si dice circuito se $v_1 = v_m$ esempio:
- Definisco $\gamma = (V \times V, \varrho)$ con $\varrho \subseteq V \times V : (v_1, v_2) \in \varrho$ se e solo se esiste un cammino da v_1 a v_2
  ↳ γ è una relazione di equivalenza su V
  transitività: $(v_1, v_2) \in \varrho$ e $(v_2, v_3) \in \varrho$ → $(v_1, v_3) \in \varrho$ → esiste un cammino da v_1 a v_3
  simmetria: se $(v_1, v_2) \in \varrho$ → $(v_2, v_1) \in \varrho$ → posso percorrere i archi al contrario
- Una classe di equivalenza di γ si dice componente connessa del grafo.

ESEMPIO:

Questo grafo ha due componenti connesse



→ • a, b, c sono in relazione tra di loro esistendo cammini
- anche d, e, f, g, h, i sono in relazione tra di loro esistendo cammini
- nessuno della classe di equivalenza di a è in relazione con la classe di equivalenza di d
- quindi ci sono due componenti connesse

è un solo grafo non sempre per forza essere collegati

CAMMINO SU UN MULTIGRAFO

- Sia (V, l, σ) un multigrafo, siano, inoltre, $v_1, v_2, \dots, v_m, v_{m+1} \in V$ (vertici), siano $l_1, l_2, \dots, l_m \in l$ (un insieme di archi) tutti distinti: $\sigma(l_i) = \{v_i, v_{i+1}\}$ 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 due lati distinti possono passare per lo stesso vertice
- Un cammino $(l_1, l_2, l_3, \dots, l_m)$ è detto sviluppo se $l = \{l_1, l_2, l_3, \dots, l_m\}$ → il cammino copre tutti i possibili lati

ESEMPIO:

- Un cammino euleriano si dice circuito euleriano se, posti $v_1, v_2, \dots, v_n, v_{n+1} \in V$, si ha che $v_1 = v_{n+1}$ [illegible] con l'origine

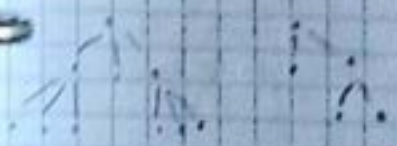
TEOREMA DI EULERO

Sia g un multigrafo finito privo di vertici isolati.
Allora g ha un circuito di Eulero se e solo se tutti i suoi vertici sono pari
↳ Quindi non c'è un circuito euleriano nei ponti di Königsberg perché ogni vertice è dispari

ALBERI E FORESTE

- Un grafo si dice foresta se non ha circuiti
- Un grafo si dice albero se è una foresta ed è connesso

ESEMPIO:



È UNA FORESTA

È UN ALBERO
↳ [illegible] SECONDO

TEOREMA

Un grafo finito (V, E) è una foresta se e solo se per ogni coppia $(x, y) \in V \times V$ e $x \neq x$ esiste al più un cammino da x a y
↳ può anche non esistere un cammino
↳ DIMOSTRAZIONE PROSSIMA PAGINA
↳ se ho $x \in y \in$ ho [illegible] modi per andare, non sapendo che tra x e y c'è un circuito

COROLLARI ALL'ULTIMA PAGINA

$x \subset y$ ←

DIM VOGLIO DIMOSTRARE CHE: $\neg q \to \neg p$

(→) • Siano $(\{u_1, u_2\}, \{u_2, u_3\}, \dots, \{u_{m-1}, u_m\})$ e $(\{v_1, v_2\}, \{v_2, v_3\}, \dots, \{v_{m-1}, v_m\})$ due cammini distinti tra X e Y (cioè $u_1 = v_1 = X$ e $u_m = v_m = Y$)

PRENDIAMO TUTTI GLI INDICI DI U DOVE U E V SI SEPARANO

* • Sia $i = \{h \in \mathbb{N} \mid (\exists k \in \mathbb{N})(u_h = v_k \wedge \{u_h, u_{h+1}\} \neq \{v_k, v_{k+1}\})\}$

• Sia $r = \min(i)$ e sia k_r il relativo k.

• Sia ora $j = \{h \in \mathbb{N}_h \mid (\exists k \in \mathbb{N})(u_{h+1} = v_{k+1})\}$ → PRENDIAMO TUTTI GLI INDICI DI U DOPO IL DOVE U E V SI RICONGIUNGONO

• Sia $s = \min(j)$ e sia k_s il relativo k.

• Certo è che $k_r \neq k_s$ → ALTRIMENTI NON POTREMMO DEFINIRE i E S

↓

Posso supporre, senza ledere la generalità (WLOG), $k_r < k_s$.

Allora, il circuito è il seguente:

VADO AVANTI FINCHÉ U E V SI INCONTRANO

$(\{u_r, u_{r+1}\}, \{u_{r+1}, u_{r+2}\}, \dots, \{u_s, u_{s+1}\}, \{v_{k_s+1}, v_{k_s}\}, \dots, \{v_{k_r+2}, v_{k_r+1}\}, \{v_{k_r+1}, v_{k_r}\})$

↳ È v_{k_r+1} PER LA DEFINIZIONE DI J

TORNO INDIETRO

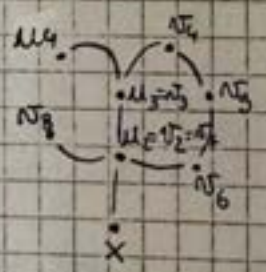
↳ È u_r PER LA DEFINIZIONE DI i

↳ SONO TUTTI DISTINTI PERCHÉ ABBIAMO PRESO I MINIMI DEI → $r < s$ E $k_r < k_s$ RISPETTIVI INSIEMI

---

* Inizialmente ho che $u_1 = v_1 = X$, ma a un certo punto si sdoppiano essendo due cammini distinti, quindi $i \neq \emptyset$

↳ Con r prendo il primo punto in cui si sdoppiano, in questo caso $h = 2$ perché il cammino si sdoppia prima a u_2 e poi a u_3, infatti $\{u_2, u_3\} \neq \{v_1, v_8\}$ ma $u_2 = v_1$



→ IL MINIMO ESISTE PERCHÉ i È UN INSIEME DI NUMERI NATURALI DIVERSO DAL VUOTO

A un certo punto i due cammini dovranno ricongiungersi dato che ho che $u_m = v_m = Y$, quindi di certo $j \neq \emptyset$

↳ Con s prendo il primo punto in cui i due cammini si ricongiungono

---

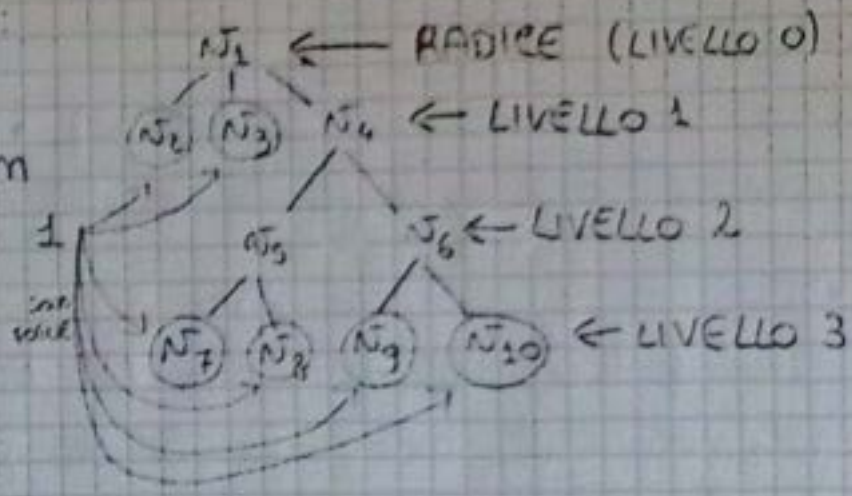
(←) Per Assurdo, ci sia un circuito $(\{v_1, v_2\}, \{v_2, v_3\}, \dots, \{v_{m-1}, v_m\})$ con $v_1 = v_m$. Essendo un circuito, $m > 1$. → NON ESISTONO CIRCUITI SU DI SOLO ELEMENTO

→ CIOÈ NON HO LA FORESTA

Allora $(\{v_1, v_2\})$ e $(\{v_2, v_3\}, \dots, \{v_{m-1}, v_m\}, \{v_1, v_2\})$ SONO DUE CAMMINI DISTINTI TRA v_1 E v_2

RAPPRESENTAZIONE RADICALE DI UN ALBERO

Un esempio di rappresentazione radicale di un albero è:



- In un albero, un vertice di grado 1 si dice foglia
  ↳ 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 $V = \{v_1, v_2, \dots, v_m\}$ e avrò che $|V| = m$ → L'ALBERO È FINITO

- Prendo $l_1 = \{v_1, v_2\}$

Dato che per assurdo non ci sono vertici di grado 1

In questo modo avrò che $d(v_2) \geq 2$

Essendo il grado maggiore di 2, posso trovare v_3 tale che $v_3 \notin \{v_1, v_2\}$ (dato che g è un albero → Quindi non è un circuito) → cioè $v_3 \neq v_2$ e $v_3 \neq v_1$
Dato che v_2 deve essere collegato a v_2 e non ho circuiti

- Dico, allora, $l_2 = \{v_2, v_3\}$, ma $d(v_3) \geq 2$ e così via...

↓

Trovo una successione $l_1, \dots, l_m$ di lati distinti che collegano $m+1$ vertici distinti, ma ciò è un assurdo perché esco dall'insieme V. ↯

TEOREMA (2)

Un albero di n vertici ha $n-1$ lati → cioè $|\ell| = n-1$

DIM

(Per induzione di I forma). • Se $n=1$ allora ciò è ovvio, perché ci sarebbero 0 lati.

• Sia $n>1$ e sia vero l'asserto per $n-1$.
Per il teorema di prima (1) trovo una foglia X. → X HA UN SOLO LATO
Prendo il sottografo S di g in cui tolgo X e il suo unico ramo.
S ha $n-1$ vertici e $|\ell|-1$ lati.

• Per induzione, $|\ell|-1 = n-1-1$, quindi avrò che $|\ell| = n-1$

TEOREMA

Un albero finito con almeno due vertici ha almeno due foglie

DIM

Sia $|V| = n$.
Per il teorema (2), ho che $|\ell| = n-1$. (IL NUMERO DI LATI DI g)
Per il teorema somma ho che $\sum_{x \in V} d(x) = 2(n-1)$.
↳ DOPO KUPATOWSKI
Se per assurdo, ho meno di 2 foglie, allora ho almeno $n-1$ vertici di grado maggiore o uguale a 2. → CON n VERTICI HO SICURAMENTE o 0 o 1 SOLA FOGLIA, QUINDI TUTTI GLI ALTRI VERTICI HANNO GRADO MAGGIORE DI 2

Ovvero $\sum_{x \in V} d(x) \geq 2(n-1)+1$, che è un assurdo perché so che $\sum_{x \in V} d(x) = 2(n-1)$
↳ IL GRADO DI $n-1$ VERTICI È 2 A CUI AGGIUNGO QUELL'UNICA FOGLIA, CHE HA GRADO 1

TEOREMA → NO DIM

Se $g = (V, E, \sigma)$ 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 → NO DIM

Vale che, dato $g = (V, E, \sigma)$ 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) → 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) → 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) → 1) Se vale che g è una foresta e vale che $|V| = |E| + 1$ allora per il teorema di prima abbiamo che "e" è una sola componente connessa, cioè la foresta è un albero

COROLLARI DI 5 PAGINE FA

Dal teorema secondo cui un grafo finito (V, E) è una foresta se e solo se per ogni coppia $(X, Y) \in V \times V$ e $X \neq X$ (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

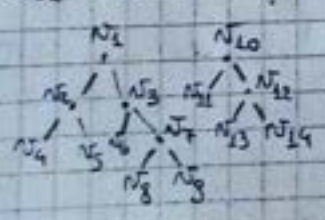
Ogni foresta finita è un grafo planare

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 la foresta:



Non esiste un cammino tra v_1 e v_{10}, ma il grafo è una foresta