Appunti per il 1° Anno - 1° Semestre - Gruppo C2

Algebra

Dalle lezioni del prof. Cutolo Giovanni

Anno 2023/24 - Di Tota Gaetano

Algebra - a.a. 2023/2024

Simboli

Simboli

$\cup$ unione

$\cap$ intersezione

$\forall$ per ogni

$\exists$ esiste

$\in$ appartiene

$\notin$ non appartiene

$\vee$ o disgiunzione

$\wedge$ e congiunzione

$\Leftrightarrow$ equivalente

$\neg$ negazione

$\Rightarrow$ implica

$\subseteq$ inclusione

$\subset$ inclusione propria

$\triangle$ differenza simmetrica

$\setminus$ differenza insiemistica

$\bigcup$ unione unaria

$\bigcap$ intersezione unaria

$\simeq$ isomorfo

Siete pregati di segnalare ogni tipo di errore!

Calcolo proposizionale

Il calcolo proposizionale studia delle proposizioni di cui è possibile determinarne il valore di verità, usando le "tabelle di verità" per descriverne in modo sintetico i valori e ottenerne una definizione semantica completa.

Definizione - Formula chiusa o proposizione

Espressioni a cui è possibile attribuire valori di verità. (Possono anche essere chiamate "sentenze" o "affermazioni".)

Definizione - Forma proposizionale

Una formula di formule, ossia l'unione di più formule chiuse attraverso l'utilizzo dei connettivi proposizionali.

Esempio - Proposizioni

1+1=3 *Falsa*
1+1=2 *Vera*
1+x=2 *Non è una proposizione perché nella formula è contenuta una variabile*

Connettivi proposizionali

- **Negazione**: inverte il valore di verità di una formula (Simbologia $\neg$).
- **Congiunzione**: risulta vero se e solo se entrambe le forme sono vere (Simbologia $\wedge$).
- **Congiunzione Negata**: negazione della congiunzione (Simbologia ($\uparrow$), (NAND)).
- **Disgiunzione (inclusiva)**: risulta vero se almeno una delle forme è vera (Simbologia $\vee$).
- **Disgiunzione Negata (inclusiva)**: negazione della disgiunzione (Simbologia ($\downarrow$), (NOR)).
- **Disgiunzione (esclusiva)**: risulta vera se e solo se una delle due forme è vera (Simbologia ($\veebar$), (XOR)).
- **Bicondizionale**: risulta vero se e solo se entrambe le formule hanno stesso valore di verità (Simbologia $\Leftrightarrow$).
- **Condizionale**: risulta falsa se e solo se l'antecedente è vero e il conseguente falso (Simbologia $\Rightarrow$).

Proprietà dei connettivi proposizionali

- **Commutativa**: poter scambiare l'ordine delle proposizioni senza alterarne il risultato.
  $(p \wedge q) \Leftrightarrow (q \wedge p)$
  $(p \vee q) \Leftrightarrow (q \vee p)$
  $(p \text{ XOR } q) \Leftrightarrow (q \text{ XOR } p)$
  $(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p)$
- **Associativa**: Poter modificare l'ordine di verifica senza alternarne il risultato.
  $((p \wedge q) \wedge r) \Leftrightarrow (p \wedge (q \wedge r))$
  $((p \vee q) \vee r) \Leftrightarrow (p \vee (q \vee r))$
  $((p \text{ XOR } q) \text{ XOR } r) \Leftrightarrow (p \text{ XOR } (q \text{ XOR } r))$
  $((p \Leftrightarrow q) \Leftrightarrow r) \Leftrightarrow (p \Leftrightarrow (q \Leftrightarrow r))$
- **Distributiva**: distribuiamo ciò che sta fuori dalla parentesi al suo interno (di $\wedge$ rispetto ad $\vee$ (e viceversa) e $\wedge$ rispetto a XOR).
  $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
  $(p \wedge (q \text{ XOR } r)) \Leftrightarrow ((p \wedge q) \text{ XOR } (p \wedge r))$

- **Transitività**: se P è in relazione con Q e Q è in relazione con R allora P è in relazione con R.
  $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
  $((p \Leftrightarrow q) \wedge (q \Leftrightarrow r)) \Leftrightarrow (p \Leftrightarrow r)$

Le forme proposizionali possono essere di 3 tipi:

- **Tautologia**: il valore di verità risulta sempre vero.
- **Contraddizione**: il valore di verità risulta sempre falso.
- **Forma Contingente**: né tautologia, né contraddizione, il valore di verità non è costante.

Nota - Forme logicamente equivalenti

Quando due forme proposizionali assumono sempre lo stesso valore, si dicono logicamente equivalenti. Se p e q sono due forme di questo tipo, $p \Leftrightarrow q$ è un caso particolare di tautologia. In particolare, due tautologie o due contraddizioni sono sempre logicamente equivalenti.

Tautologie, Contraddizioni e Forme Contingenti

Tra le tautologie notevoli abbiamo osservato:

- **Principio di non-contraddizione**: la proposizione P e la sua negazione, cioè non-P, non possano essere entrambe vere allo stesso tempo $(\neg(p \wedge (\neg p)))$.
- **Principio del terzo escluso**: la proposizione P e la sua negazione hanno sempre valori opposti $(p \vee (\neg p))$.
- **Doppia negazione**: la proposizione P negata due volte torna al valore di partenza $(p \Leftrightarrow \neg(\neg p))$.
- **Legge di idempotenza (o iteratività)** (per $\vee$ e $\wedge$): la proposizione composta da molteplici volte P sarà sempre uguale ad P $((p \wedge p) \Leftrightarrow p \Leftrightarrow (p \vee p))$.
- **Tautologia della doppia implicazione**: la congiunzione tra l'implicazione delle proposizioni P e Q ed il viceversa è uguale alla doppia implicazione tra P e Q $((p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \wedge (q \Rightarrow p)))$.
- **Relazione fra implicazione e disgiunzione**: l'implicazione tra P e Q può essere espressa mediante la negazione e la disgiunzione $((p \Rightarrow q) \Leftrightarrow ((\neg p) \vee q))$.
- **Legge di contrapposizione**: l'implicazione tra P e Q è equivalente all'implicazione tra non P e non Q grazie alla commutatività della disgiunzione $((p \Rightarrow q) \Leftrightarrow (\neg(q) \Rightarrow \neg(p)))$.

Definizione - Leggi di De Morgan

Per negare una disgiunzione (o una congiunzione) basta negare i due termini che stiamo disgiungendo (o congiungendo) e, contemporaneamente, scambiare la disgiunzione con la congiunzione (o viceversa).

- **Negazione congiunzione**: $\neg(p \wedge q) \Leftrightarrow ((\neg p) \vee (\neg q))$
- **Negazione disgiunzione**: $\neg(p \vee q) \Leftrightarrow ((\neg p) \wedge (\neg q))$

Interdipendenza semantica

Dalle tautologie e le Leggi di De Morgan è possibile dedurre che basta scegliere uno tra i due connettivi logici *NOR* e *NAND* per ricavare tutti i restanti:

- **Negazione**: $(p\ NOR\ p) \Leftrightarrow (\neg p)$ oppure $(p\ NAND\ p) \Leftrightarrow (\neg p)$.
- **Congiunzione**: $\neg(p\ NAND\ q) \Leftrightarrow (p \wedge q)$ oppure (da De Morgan) $(p \wedge q) \Leftrightarrow (\neg((\neg p) \vee (\neg q)))$.

- **Disgiunzione**: $\neg(p\ NOR\ q) \Leftrightarrow (p \vee q) \Leftrightarrow ((p\ NOR\ q)\ NOR\ (p\ NOR\ q))$.
- **Implicazione**: $((\neg p) \vee q) \Leftrightarrow (p \Rightarrow q)$.
- **Bicondizionale**: $(p \Leftrightarrow q) \Leftrightarrow (((\neg p) \vee q) \wedge ((\neg q) \vee p))$.
- **XOR**: $\neg(p \Leftrightarrow q) \Leftrightarrow (p\ XOR\ q)$.

Logica dei Predicati

Se all'interno di una formula appare una variabile otteniamo delle formule matematiche che indichiamo con la lettera φ alle quali attribuire un valore di verità se e solo se sono proposizioni, una proposizione viene detta **valida** quando è vera per qualsiasi valore si affida alle variabili, le occorrenza di variabili possono essere di due tipi:

- **Vincolata**: Se l'occorrenza della variabile viene introdotta da un quantificatore $\forall x(1 + x = 0)$ oppure $\exists x(x - 1 = 0)$
- **Libera**: Se l'occorrenza della variabile non è vincolata da un quantificatore che la introduce $\forall x(x > y)$

Definizione - Formule chiuse e aperte

- **Formula chiusa** (o proposizione): quando al suo interno ci sono solo occorrenze di variabili vincolate.
- **Formula aperta**: quando al suo interno è presente almeno un'occorrenza di variabile libera.

Nota - Osserva con attenzione!

$$\varphi(x) : \exists z(\exists y(\forall x(x > y)) \wedge x = 7)$$

Notiamo l'occorrenza multipla della variabile x come vincolata e libera, per non incappare in errori possiamo sostituire tutte le occorrenze non vincolate di x con una variabile non in uso, come ad esempio la variabile p.

$$\varphi(p) : \exists z(\exists x(\forall x(x > y)) \wedge p = 7)$$

Definizione - Predicato (unario, binario, ternario...)

Una formula φ è tale solo se ci sono occorrenze libere n-arie delle variabili specificate e non ci sono altre occorrenze libere, un predicato quindi può assumere un valore di verità sostituendo alle occorrenze di variabili libere.

Esempio - Sostituzione

Supponendo il predicato unario in x: $\varphi(x) : x + 10 > 15$, prendiamo in esempio due casi:

1. $\varphi(3) : 3 + 10 > 15$
2. $\varphi(6) : 6 + 10 > 15$

Dove il predicato nel primo esempio ha valore falso mentre il secondo vero.

Osserviamo il caso di un predicato più lungo, come $\varphi(x) : \exists z(\exists y(\forall x(x > y)) \wedge x = 7)$, in questo caso la x non vincolata da $\forall$ è detta libera.

La sostituzione va effettuata soltanto su variabili libere e non vincolate, quindi se supponiamo di avere $\varphi(6)$

$$\varphi(6) : \exists z(\exists y(\forall x(x > y)) \wedge 6 = 7)$$

Quantificatori

Se consideriamo il predicato unario φ nella variabile x possiamo applicare due tipi di quantificatori diversi, ovvero:

- **Universale**: $\forall x(\varphi)$ indica che si ottiene una proposizione vera per ogni sostituzione di x, altrimenti è falsa.
- **Esistenziale**: $\exists x(\varphi)$ indica che si ottiene una proposizione vera per una sostituzione possibile di x, altrimenti è falsa.

Domanda - A quale connettivo logico corrispondono i quantificatori?

Il connettore $\forall$ è equivalente all'implicazione: $(\forall x > 0)(\varphi) \Leftrightarrow \forall x(x > 0 \Rightarrow \varphi)$
Il connettore $\exists$ è equivalente alla congiunzione: $(\exists x > 0)(\varphi) \Leftrightarrow \exists x(x > 0 \wedge \varphi)$

Da questo deduciamo che la negazione del quantificatore $\forall$ (implicazione) è il quantificatore $\exists$ (la congiunzione) e viceversa.

L'ordine dei quantificatori risulta molto importante perché determinano in maniera incisiva la verità di una proposizione:

1. $\forall x(\exists y(x \leq y))$
2. $\exists y(\forall x(x \leq y))$

Possiamo notare che la prima proposizione è vera mentre la seconda è falsa.

Nota - Esiste con n-occorrenze possibili

Il quantificatore esistenziale può simboleggiare anche l'unicità, oppure le n-occorrenze possibili, dove la forma sia vera.

- **N-occorrenze** dove con il pedice n viene indicato l'esatto numero di occorrenze $\exists_n x(\varphi)$
- **Unicità** indicata col simbolo $\exists! x(\varphi) \Leftrightarrow \exists_1 x(\varphi)$

Insiemi

Per insieme si intende un oggetto matematico che trasforma la pluralità in singolarità, in modo che non sia rilevante nell'insieme l'ordine o le ripetizioni, dal quale ricaviamo il seguente assioma:

Definizione - Assioma di estensionalità

Due insiemi uguali rappresentano lo stesso insieme se hanno gli stessi elementi.

$$\forall a, b(a = b \Leftrightarrow \forall x(x \in a \Leftrightarrow x \in b))$$

Questo assioma ci permette di definire due concetti molto importanti, quello di insieme vuoto e singleton di un elemento.

Definizione - Singleton

Insieme composto da un singolo elemento.

$$\forall x(x \in \{a\} \Leftrightarrow x = a)$$

Definizione - Insieme vuoto

Garantisce che esista un'insieme vuoto.

$$\exists y(\forall x(x \notin y))$$

Se prendiamo in considerazione un predicato unario φ nella variabile x, possiamo rappresentare la sua estensione ad un'insieme (ovvero tutti gli oggetti che verificano tale predicato).

Esempio - Numeri naturali minori di 3

Preso il predicato unario $\varphi(x) : x < 3$, esso rappresenta l'estensione all'insieme:

$$\{x \mid x \in \mathbb{N} \land x < 3\} \Leftrightarrow \{0, 1, 2\}$$

Gli insiemi possono essere quindi descritti sulla base di un predicato unario, ma non tutti i predicati unari descrivono un'insieme, questo perché esistono predicati che seppure bene argomentati e logicamente impeccabili non ammettono un insieme di oggetti che lo verificano, quindi questo ci porta a dedurre l'assioma di separazione.

Definizione - Assioma di separazione

Se costruiamo un'insieme degli oggetti che verificano un predicato scegliendoli da un'insieme S, qualsiasi sia la sua estensione otterremo sicuramente un'insieme parte di S.

$$\{x \in S \mid \varphi(x)\}$$

Domanda - Come si descrive un insieme?

Viene descritto come l'insieme di tutti i termini T che verificano φ, espresso in simboli:

$$\{T(x, y, z...) \mid \varphi(x, y, z...)\}$$

Alcuni esempi sono:

- $\{n^2 \mid n \in \mathbb{Z}\}$ Tutti i quadrati di $\mathbb{Z}$
- $\{\{x\} \mid x \in \mathbb{N}\}$ Tutti i singleton di $\mathbb{N}$
- $\{n^2 + m^2 \mid n, m \in \mathbb{Z}\}$ La somma di tutti i termini al quadrato

Teorema - Antinomia di Russell

Supponiamo di avere un'insieme R che contiene tutti gli insiemi che non appartengono a se stessi.

$$R = \{x \mid x \notin x\}$$

La formula per esteso recita:

$$\forall x(x \in R \Leftrightarrow x \notin x)$$

Sostituendo R all'interno della formula otteniamo:

$$R \in R \Leftrightarrow R \notin R$$

Quindi per assurdo si ottiene che R non appartiene a se stesso perché non soddisfa la definizione, quindi R appartiene a se stesso.

Sottoinsieme

Definizione - Inclusione

Per inclusione si intende un'insieme A contenuto ma non appartenente ad un'insieme B, in simboli si esprime con:

$$a \subseteq b \Leftrightarrow \forall x(x \in a \Rightarrow x \in b) \Leftrightarrow \forall x \in a(x \in b)$$

Deduciamo quindi due cose:

1. Ogni insieme è incluso in se stesso: $\forall x(x \subseteq x)$.
2. L'elemento vuoto è incluso in tutti gli insiemi: $\forall x(\emptyset \subseteq x)$:

Esempio - Numeri pari contenuti in $\mathbb{N}$

L'insieme dei numeri pari è contenuto in $\mathbb{N}$ ma non appartiene ad esso, in simboli logici abbiamo: $\{x \in \mathbb{N} \mid 2x\} \subseteq \mathbb{N}$

Insieme delle parti

Definizione - L'insieme delle parti di S

L'insieme delle parti di S, è un insieme che si compone di tutte le parti di S e segue questa definizione:

$$P(S) = \{x \mid x \subseteq S\}$$

Quando non è indicato nessun limite degli elementi che compongono delle parti, è sottintesa ogni possibile combinazione, altrimenti è possibile indicare il limite degli elementi che compongono le parti, come il singleton degli elementi di S:

$$P_1(S) = \{\{x\} \mid x \in S\}$$

Esempio - Tutte le parti di $\{1, 2, 3\}$

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

$P_1(\{1, 2, 3\} = \{\{1\}, \{2\}, \{3\}\}$

Domanda - Quante parti ha $P(S)$?

Dall'esempio sopra possiamo notare che $P(S)$ ha 2^k elementi, dove k è il numero degli elementi di S.

Attenzione! $P(\emptyset)$ ha come elementi solo in singleton dell'insieme vuoto, questo perché ha 0 elementi, quindi $2^0 = 1$, proprio il singleton dell'insieme vuoto.

Da Logica a Teoria degli Insiemi

Definizione - Connettivi insiemistici

Alcuni connettivi logici si possono applicare alla teoria degli insiemi.

- **Unione** (Disgiunzione): $A \cup B = \{x \mid x \in A \vee x \in B\}$
- **Intersezione** (Congiunzione): $A \cap B = \{x \mid x \in A \wedge x \in B\}$
- **Differenza Simmetrica** (Disgiunzione esclusiva): $A \triangle B = \{x \mid x \in A \ XOR \ x \in B\}$
- **Differenza** (Negazione): $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$
- **Inclusione** (Implicazione): $A \subseteq B = \{x \mid x \in A \Rightarrow x \in B\}$
- **Uguaglianza** (Equivalenza): $(A = B) = \{x \mid x \in A \Leftrightarrow x \in B\}$

Nota - Connettivi complementari

I connettivi logici NAND e NOR sono i complementari e non formano insiemi perché non esiste un "insieme esterno" (ovvero un insieme che contiene tutti gli insiemi).

Quali proprietà posso applicare ai connettivi logici?

- **Commutativa**
  $A \cap B = B \cap A$

$A \cup B = B \cup A$
$A \triangle B = B \triangle A$

- **Associativa**
  $(A \cap B) \cap C = A \cap (B \cap C)$
  $(A \cup B) \cup C = A \cup (B \cup C)$
  $(A \triangle B) \triangle C = A \triangle (B \triangle C)$
- **Idempotenza**
  $A \cap A = A$
  $A \cup A = A$
  $A \triangle A = \emptyset$
- **Distributiva**
  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$

Definizione - Tautologie applicate all'insiemistica

Alcune tautologie ci danno la possibilità di ricavarne nozioni insiemistiche

- **Regola della Doppia Implicazione** $A = B \Leftrightarrow (A \subseteq B) \cap (B \subseteq A)$
- **Transitiva** $((A \subseteq B) \cap (B \subseteq C)) \subseteq (A \subseteq C)$

Definizione - Leggi di De Morgan

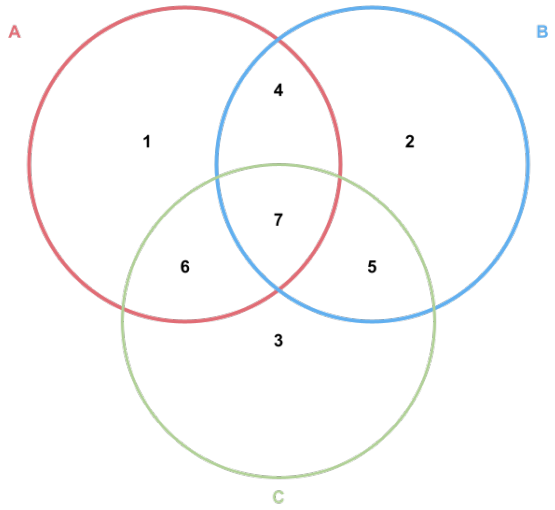
Per negare un'unione (o un'intersezione) basta negare i due termini che stiamo unendo (o intersecando) e, contemporaneamente, scambiando l'unione con l'intersezione.

- **Negazione unione**: $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
- **Negazione intersezione**: $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

Diagramma di Venn

Il diagramma di Venn può essere usato per confrontare le formule, esso però è detto generico se l'insieme che rappresenta i suoi elementi verifica le sue parti.
Prendiamo in esempio il diagramma di Venn a destra, il suo insieme $S = \{A, B, C\}$ verifica $P(S)$, la tabella usata per il confronto è la seguente:

A	1			4		6	7
B		2		4	5		7
C			3		5	6	7
$A \cap B$				4			7
$A \cup B$	1	2		4	5	6	7
$A \triangle B$	1	2			5	6	
$A \setminus B$	1					6	
$B \setminus A$		2			5		
$B \cup C$		2	3	4	5	6	7
$A \cap (B \cup C)$				4		6	7
$A \triangle B \triangle C$	1	2	3				7



Operatori Unari

È possibile ridurre le operazioni binarie di intersezione e di unione alle corrispondenti operazioni unarie.

Definizione - Operazioni Unarie

Unione unaria $\bigcup A = \{x \mid \exists y \in A(x \in y)\}$

Intersezione unaria $\forall A \neq \emptyset : \bigcap A = \{x \mid \forall y \in A(x \in y)\}$

Esempio - Operazioni unarie su un'insieme e le sue parti

Supponiamo di avere un insieme $S = \{\{1;2;3\};\{2;3;4\};\{3;4;5;6\}\}$, le operazioni di unione e intersezione unaria su questo insieme avrebbero come risultato:

- $\bigcup S = \{1;2;3;4;5;6\}$ rappresenta l'unione di tutti gli elementi degli elementi di S.
- $\bigcap S = \{3\}$ rappresenta l'intersezione di tutti gli elementi degli elementi di S.

Altre applicazione di questi operatori unari sono, per ogni insieme S arbitrario:

- $\bigcup P(S) = S$
- $\bigcap P(S) = \emptyset$

Teorema - Associatività generalizzata

$\forall a, b\ a \neq \emptyset \neq b\ (\bigcup a) \cup (\bigcup b) = \bigcup \{x \cup y \mid x \in a \wedge y \in b\} = \bigcup (a \cup b)$

$\forall a, b\ a \neq \emptyset \neq b\ (\bigcap a) \cap (\bigcap b) = \bigcap \{x \cap y \mid x \in a \wedge y \in b\} = \bigcap (a \cup b)$

Teorema - Distributività generalizzata

$b \neq \emptyset \; a \cap \bigcup b = \{x \mid \exists y \in b(x \in y \wedge x \in a)\} = \bigcup_{y \in b}(a \cap y)$

$b \neq \emptyset \; a \cup \bigcap b = \{x \mid \forall y \in b(x \in y \wedge x \in a)\} = \bigcap_{y \in b}(a \cup y)$

Definizione - Leggi sulla generalizzazione di De Morgan

Unione unaria

$$\forall a, b \; b \neq \emptyset \Rightarrow a \setminus \bigcup b = \bigcap_{y \in b}(a \setminus y)$$

Dimostrazione

$$a \setminus \bigcup b \Leftrightarrow \forall x(x \in a \wedge \neg(\exists y \in b \mid x \in y)) \Leftrightarrow \forall x(x \in a \wedge \forall y \in b(x \notin y)) \Leftrightarrow \forall x(\forall y \in b(x \in a \wedge x \notin b)) \Leftrightarrow \bigcap_{y \in b}(a \setminus y)$$

Intersezione unaria

$$\forall a, b \; b \neq \emptyset \Rightarrow a \setminus \bigcap b = \bigcup_{y \in b}(a \setminus y)$$

Dimostrazione

$$a \setminus \bigcap b = \forall x(x \in a \wedge \neg(\forall y \in b(x \in y)) \Leftrightarrow \forall x(x \in a \wedge \exists y \in b(x \notin y)) \Leftrightarrow \forall x(\exists y \in b(x \in a \wedge x \notin y)) \Leftrightarrow \bigcup_{y \in b}(a \setminus y)$$

Corrispondenza

Per definire una corrispondenza dobbiamo prima capire cosa è una coppia ordinata, una terna ordinata e un prodotto cartesiano, definiamo quindi questi tre concetti.

Definizione - Coppia ordinata

Dati due insiemi a e b, diremo coppia ordinata (a, b) dove la **1° coordinata** è a e la **2° coordinata** è b.

- **Proprietà di unicità**: $\forall a, b, c, d \; (a, b) = (c, d) \Leftrightarrow a = c \wedge b = d$
- **Definizione di Kuratowski**: $(a, b) = \{\{a\}, \{a, b\}\}$

Definizione - Terna ordinata

Dati tre insiemi a, b, c, diremo terna oridnata (a, b, c) dove la **1° coordinata** è a, la **2° coordinata** è b e la **3° coordinata** è c.

- **Proprietà di unicità**: $\forall a, b, c, d, e, f \; (a, b, c) = (d, e, f) \Leftrightarrow (a, b) = (d, e) \wedge c = f \Leftrightarrow a = d \wedge b = e \wedge c = f$
- **Definizione di Kuratowski**: $(a, b, c) = \{\{c\}, \{c, \{\{a\}, \{a, b\}\}\}\}$

Definizione - Prodotto Cartesiano

Il prodotto cartesiano tra due a e b è l'insieme di tutte le coppie ordinate formata dagli elementi di a associati agli elementi di b.

$$\forall a, b \; a \times b = \{(x, y) \mid x \in a \wedge y \in b\}$$

Esempio - Prodotto Cartesiano

Siano dati gli insiemi $a = \{1, 2\}$ e $b = \{1, 3\}$.
$a \times b = \{(1,1), (1,3), (2,1), (2,3)\}$
$b \times a = \{(1,1), (1,2), (3,1), (3,2)\}$

Definizione - Corrispondenza

Siano dati a e b insiemi, una corrispondenza γ è una terna ordinata (a, b, g) tale che $g \subseteq a \times b$, possiamo quindi indicare con $Corr(a, b)$ è l'insieme di tutte le corrispondenze da a a b, dove:

- g è il grafico della corrispondenza.
- $\forall x \in a$ e $\forall y \in b$ diremo che y è una corrispondenza di x in $\gamma \Leftrightarrow (x, y) \in g$

Esempio - Corrispondenza

Data la corrispondenza $\gamma \in Corr(a, b)$ possiamo riscriverla come $\forall x \in a(\forall y \in b(x \ \gamma \ y \Leftrightarrow x < y))$ dove il grafico è $g = \{(x, y) \in a \times b \mid x < y\}$.

Nota - Relazione binaria

Le $Corr(a, a)$ sono relazioni binarie in a, ovvero $Rel(a) = Corr(a, a)$.

Esempio - Relazione binaria in A

Dato l'insieme $A = \{n \in \mathbb{N} \mid n < 4\}$ con $\sigma \in Rel(a)$

σ è definito da $\forall x, y \in a(x \ \sigma \ y \Leftrightarrow y = x + 1)$

Definizione - Corrispondenza Relazionale

Dati degli insiemi a, b, c ed avere le corrispondenze $a \xrightarrow{\alpha} b \xrightarrow{\beta} c$, chiamati gli elementi nelle corrispondenze $\alpha \in Corr(a, b)$ e $\beta \in Corr(b, c)$, esse sono dette corrispondenze componibili e possiamo definire un'unica corrispondenza con $\alpha\beta \in Corr(a, c)$ ponendo:

$$\forall x \in a(\forall z \in c(x \ \alpha\beta \ z \Leftrightarrow \exists y \in b(x \ \alpha \ y \wedge y \ \beta \ z)))$$

Teorema - Associatività

Dati gli insiemi a, b, c, d e date le corrispondenze $a \xrightarrow{\alpha} b \xrightarrow{\beta} c \xrightarrow{\gamma} d$, chiamati gli elementi nelle corrispondenze $\alpha \in Corr(a, b)$, $\beta \in Corr(b, c)$, $\gamma \in Corr(c, d)$, otteniamo che $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ secondo tale definizione:

$$\forall x \in a \text{ e } \forall t \in d \text{ otteniamo } x \ ((\alpha\beta)\gamma) \ t \Leftrightarrow x \ (\alpha(\beta\gamma)) \ t$$

Dimostrazione: $\exists z \in c(x \ (\alpha\beta) \ z \wedge z \ \gamma \ t) \Leftrightarrow \exists y \in b(\exists z \in c(x \ \alpha \ y \wedge y \ \beta \ z \wedge z \ \gamma \ t)) \Leftrightarrow \exists y \in b(x \ \alpha \ y \wedge y \ (\beta\gamma) \ t)$

Domanda - Come è strutturata la notazione di una corrispondenza?

Quando otteniamo una corrispondenza da A a B con grafico $\{(x, y) \in A \times B \mid x \in A\}$ la possiamo scrivere con $x \in A \longrightarrow y \in B$, ottenendo la terna:

$$(A, B, \{(x, y) \in A \times B \mid x \in A\})$$

Generalizzando la formula otteniamo $S(x,y,z...) \in A \longmapsto T(x,y,z...) \in B$ che corrisponde alla terna:

$$(A, B, \{(S(x,y,z...), T(x,y,z...)) \in A \times B \mid x,y,z... \in A\})$$

Applicazioni

Definizione - Applicazione

Siano a e b due insiemi, chiamato il dominio a e codominio b, un'applicazione è una corrispondenza $\alpha \in Corr(a,b)$ che ad ogni elemento di a associa un singolo elemento di b, in simboli: $\forall x \in a(\exists! y \in b(x\ \alpha\ y))$.

- Indichiamo con $Map(a,b)$ l'insieme di tutte le applicazioni con dominio a e codominio b.
- **Applicazione costante** ad ogni elemento di A fa corrispondere un solo elemento di B.
- **Applicazione identica** in A si ha un'applicazione da A ad A che si indica con id_A, in simboli: $id_A := (A, A, \Delta A) = (A, A, \{(x,x) \mid x \in A\}$.
- **Immersione** dato l'insieme A e l' insieme $B \subseteq A$, l'applicazione $x \in B \hookrightarrow x \in A$ è detta immersione di B in A.

Domanda - Come è strutturata la notazione di una applicazione?

Quando otteniamo un'applicazione da A a B con grafico $\{(x, f(x)) \in A \times B \mid x \in A\}$ la possiamo scrivere con $x \in A \longmapsto f(x) \in B$, ottenendo la terna:

$$(A, B, \{(x, f(x)) \in A \times B \mid x \in A\})$$

Esempio - Applicazioni

$n \in \mathbb{N} \longmapsto n+1 \in \mathbb{Z} \Leftrightarrow (\mathbb{N}, \mathbb{Z}, \{(n, n+1) \in \mathbb{N} \times \mathbb{Z} \mid n \in \mathbb{N}\})$

$x \in \mathbb{R}^+ \longmapsto \log(x) \in R \Leftrightarrow (\mathbb{R}^+, \mathbb{R}, \{(x, \log(x)) \in \mathbb{R}^x \times \mathbb{R} \mid x \in \mathbb{R}^+\})$

$\{x\} \in P_1(\mathbb{N}) \longmapsto x+1 \in \mathbb{Z} \Leftrightarrow (P_1(\mathbb{N}), \mathbb{Z}, \{(\{x\}, x+1) \in P_1(\mathbb{N}) \times \mathbb{Z} \mid x \in P_1(\mathbb{N})\})$

Definizione - Applicazioni Composte

Sono chiamate Applicazioni Composte l'unione di più Applicazioni, dati gli insiemi A, B, C, D e le Applicazioni $A \xrightarrow{\alpha} B \xrightarrow{\beta} C \xrightarrow{\gamma} D$ possiamo ottenere l'Applicazione $A(\alpha\beta\gamma)D$, ovvero: $(\alpha\beta\gamma) \in Map(A, D)$, in simboli:

$$\forall x \in A(\exists! z \in D(x(\alpha\beta\gamma)z)$$

Proprietà Associativa può essere applicata alle Applicazioni Composte $\alpha(\beta\gamma) = (\alpha\beta)\gamma$, oltre a questa notazione si usa anche $\gamma_o\beta_o\alpha$ che indica l'applicazione $x \in A \longmapsto \gamma(\beta(\alpha(x)))$.

Definizione - Restrizione

Dati due insiemi A e B, un'applicazione in $Map(A,B)$ e il sottoinsieme $C = \{x \mid x \in P(A)\}$, chiamiamo una restrizione di f a C:

$$f_{|C} : x \in C \longmapsto f(x) \in B$$

Definizione - Riduzione

Dati due insiemi A e B, un'applicazione in $Map(A, B)$ e il sottoinsieme delle immagini di f contenuto in D, possiamo ottenere una riduzione di f a D:

$$f^{|D} : x \in A \longmapsto f(x) \in D$$

Esempio - Applicazioni Composte

Date l'applicazione $f : n \in \mathbb{Z} \longmapsto n^2 \in \mathbb{Z}$ e l'applicazione $g : n \in \mathbb{Z} \longmapsto n + 1 \in \mathbb{Z}$, possiamo vedere le composte si comportano in maniera diversa.

- $f_o g = n \xrightarrow{g} n + 1 \xrightarrow{f} (n + 1)^2 \Leftrightarrow n \in \mathbb{Z} \longmapsto (n + 1)^2 \in \mathbb{Z}$
- $g_o f = n \xrightarrow{f} n^2 \xrightarrow{g} n^2 + 1 \Leftrightarrow n \in \mathbb{Z} \longmapsto n^2 + 1 \in \mathbb{Z}$

Suriettività, Iniettività e Biettività

Definizione - Suriettività

Un'applicazione si definisce suriettiva quando le immagini del dominio corrispondono al codominio, ovvero:

$$f \text{ è suriettiva} \Leftrightarrow im\ f = B \Leftrightarrow \forall y \in B(\exists x \in A(y = f(x)))$$

Applicazione Componibile per definirne la suriettività vanno osservate due cose:

1. Se α e β sono suriettiva allora $\beta_o\alpha$ è suriettiva.
2. Se $\beta_o\alpha$ è suriettiva allora sicuramente β sarà suriettiva.

Esempio - Applicazioni suriettive

$n \in \mathbb{N} \longmapsto n^2 \in \mathbb{N}$ non è suriettiva.

$n \in \mathbb{Z} \longmapsto |n| \in \mathbb{N}$ è suriettiva.

Teorema - Dimostrazione Suriettività

Assumiamo f e g suriettive e dimostriamo $g_o f$ suriettiva: $\forall z \in C(\exists x \in A((g_o f)(x) = z))$

- g è suriettiva $\forall z \in C(\exists y \in B(g(y) = z))$
- f è suriettiva $\forall y \in B(\exists x \in A(f(x) = y))$

Fissato un x con questa proprietà, andiamo a calcolare $(g_o f)(x) \Rightarrow g(f(x)) \Rightarrow g(y) = z$.
Assumiamo $g_o f$ suriettiva e dimostriamo g suriettiva: $\forall z \in C(\exists y \in B(g(y) = z))$

- $g_o f$ è suriettiva $\forall z \in C(\exists x \in A((g_o f)(x) = z))$

Fissato un x con questa proprietà, poniamo $y = f(x)$ (con $f(x) \in B$) e allora $z = g(f(x)) \Rightarrow z = g(y)$

Definizione - Iniettività

Un'applicazione si definisce Iniettiva quando elementi distinti del dominio hanno immagini distinte, ovvero:

$$f \text{ è iniettiva} \Leftrightarrow (f(x) = f(y) \Rightarrow x = y)$$

Applicazione Componibile per definirne l'iniettività vanno osservate due cose:

1. Se α e β sono iniettive allora $\beta_o\alpha$ è iniettiva.
2. Se $\beta_o\alpha$ è iniettiva allora sicuramente α sarà iniettiva.

Esempio - Applicazioni iniettive

$n \in \mathbb{N} \longmapsto n^2 \in \mathbb{N}$ è iniettiva.

$n \in \mathbb{Z} \longmapsto |n| \in \mathbb{N}$ non è iniettiva.

Teorema - Dimostrazione Iniettività

Assumiamo f e g iniettive e dimostriamo g_of iniettiva: $\forall x, y \in A(g(f(x)) = g(f(y)) \Rightarrow x = y)$

- g è iniettiva $g(f(x)) = g(f(y)) \Rightarrow f(x) = f(y)$
- f è iniettiva $f(x) = f(y) \Rightarrow x = y$

Assumiamo g_of iniettiva e dimostriamo f iniettiva: $\forall x, y \in A(f(x) = f(y) \Rightarrow x = y)$

- g_of è iniettiva $g(f(x)) = g(f(y)) \Rightarrow x = y$

Definizione - Biettività

Un'applicazione si definisce Biettiva quando è sia suriettiva che iniettiva: $\forall y \in B(\exists! x \in A(y = f(x))$
Applicazione Componibile per definire la biettività vanno osservate due cose:

1. Se α e β sono biettive allora $\beta_o\alpha$ è biettiva.
2. Se $\beta_o\alpha$ è biettiva allora α è iniettiva e β è suriettiva.

Teorema - Biettività

$\forall a, b \quad \forall f \in Map(a, b)$

1. f è biettiva
2. f ha una sezione e una retrazione
3. f ha un'inversa
4. f ha un'unica sezione
5. $\forall y \in b(\exists! x \in a(f(x) = y))$
6. $\forall y \in b(|\overleftarrow{f}(\{y\})| = 1)$

(Queste proprietà si dimostrano a vicenda)

Esempio - Applicazioni biettive

$n \in \mathbb{Z} \longmapsto n + 1 \in \mathbb{Z}$

$x \in P(S) \longmapsto S \setminus x \in P(S)$

Applicazioni immagine e anti-immagine

Definizione - Applicazione Immagine

L'insieme degli elementi che hanno immagine tramite la funzione, in simboli: $\overrightarrow{f} : P(A) \longmapsto P(B)$ che compone l'insieme $\overrightarrow{f}(X) = \{f(x) \mid x \in X\}$

Definizione - Applicazione anti-immagine

L'insieme degli elementi del dominio che vengono mandati nel codominio dalla funzione, in simboli: $\overleftarrow{f} : P(B) \longmapsto P(A)$ che compone l'insieme $\overleftarrow{f}(Y) = \{f^{-1}(y) \mid y \in Y\}$

Esempio - Applicazione immagine e anti-immagine

$\forall c \in P(A)$ la funzione immagine agisce in questo modo $\overrightarrow{f}(c) = im\, f_{|c} = \{f(x) \mid x \in c\}$

$\forall c \in P(B)$ la funzione anti-immagine agisce in questo modo $\overleftarrow{f}(c) = \{x \in A \mid f(x) \in c\}$

Domanda - Che altra definizione possiamo dare di applicazioni iniettive e suriettive?

Data la funzione $f : A \to B$

- Un'applicazione è suriettiva quando: $\forall y \in B(\overleftarrow{f}(\{y\}) \neq \emptyset)$
- Un'applicazione è iniettiva quando: $\forall y \in B(|\overleftarrow{f}(\{y\})| \leq 1)$
- Un'applicazione è biettiva quando: $\forall y \in B(|\overleftarrow{f}(\{y\})| = 1)$

Sezioni e Retrazioni

Definizione - Sezione e Retrazioni

Date le applicazioni $f : A \longmapsto B$ e $g : B \longmapsto A$.

- **Sezione** Possiamo definire g una sezione di f quando $f_o g = id_B$ quindi $B \xrightarrow{g} A \xrightarrow{f} B$.
- **Retrazione** Possiamo definire g una retrazione di f quando $g_o f = id_A$ quindi $A \xrightarrow{f} B \xrightarrow{g} A$.

Da qui ricaviamo che tutte le sezioni sono iniettive e tutte le retrazioni sono suriettive.

Teorema - Suriettiva $\Rightarrow$ avere una sezione

$f : a \longmapsto b$ data come applicazione, f è suriettiva $\Leftrightarrow$ f ha almeno una sezione, cioè $\exists g \in Map(b, a)(f_o g = id_b)$.

Dimostrazione

Poiché f è suriettiva $\forall y \in b(\exists x \in a(f(x) = y))$, per ciascuna $y \in b$ fissiamo una x.

Sia $g : y \in b \longmapsto x \in a$. Allora $\forall y \in b(f_o g)(y) = f(g(y)) = f(x) = y$

Teorema - Iniettiva $\Rightarrow$ avere una retrazione

$f : a \longmapsto b$ data come applicazione, f è iniettiva $\Leftrightarrow$ $a = \emptyset$ o f ha una retrazione, cioè $\exists g \in Map(b, a)(g_o f = id_a)$.

Dimostrazione

Poiché f è iniettiva $\forall y \in im\ f(\exists! x \in a(f(x) = y))$, fissiamo un elemento $h \in a$, se $a \neq \emptyset$.

Sia $g : y \in b \longmapsto \begin{cases} x, \text{ se } y \in im\ f \\ h, \text{ se } y \notin im\ f \end{cases} \in a$ otteniamo che $\forall x \in a(g_o f)(x) = g(f(x)) = f(x) = x$

Esempio - Sezione e Retrazione

Date le applicazioni $i : \mathbb{N} \longmapsto \mathbb{Z}$ e $v : n \in \mathbb{Z} \longmapsto |n| \in \mathbb{N}$ osservando le composte:

- $v_o i = id_{\mathbb{N}}$ quindi i è una sezione di v e v è una retrazione di i
- $i_o v : n \in \mathbb{Z} \longmapsto |n| \in \mathbb{Z}$ che non è una $id_{\mathbb{Z}}$

Applicazione inversa

Definizione - Applicazione inversa

Sia $f : a \longmapsto b$ un'applicazione, la sua inversa (indicata con f^{-1}) è un'applicazione $g : b \longmapsto a$ che sia contemporaneamente una sezione e una retrazione, così da rendere f biettiva.

Nota - Sull'applicazione inversa

Sia $n \in \mathbb{N}^*$ e l'applicazione composta $f^n = f_o f_o f_o \ldots_o f = id$, allora se $n > 1$ con f biettiva, la sua inversa sarà $f^{n-1} = f^{-1}$ perché $f_o f^{-1} = id$.

Esempio - Applicazioni Inverse

$f : x \in \mathbb{Z} \longmapsto x + 5 \in \mathbb{Z}$
Per trovare l'inversa poniamo $x + 5 = y$ e risolviamo l'equazione in x ottenendo $x = y - 5$
$f^{-1} : x \in \mathbb{Z} \longmapsto x - 5 \in \mathbb{Z}$

$\alpha : x \in \mathbb{Q} \longmapsto \frac{2x+1}{3} \in \mathbb{Q}$
Per trovare l'inverso poniamo $\frac{2x+1}{3} = y$ e risolviamo l'equazione in x ottenendo $x = \frac{3y-1}{2}$
$\alpha^{-1} : x \in \mathbb{Q} \longmapsto \frac{3x-1}{2} \in \mathbb{Q}$

$f : x \in P(\mathbb{Z}) \longmapsto \mathbb{Z} \setminus x \in P(\mathbb{Z})$
Se facciamo la composta $f_o f = id_{P(\mathbb{Z})}$ vuol dire che f è l'inversa di se stessa
$f^{-1} : x \in P(\mathbb{Z}) \longmapsto \mathbb{Z} \setminus x \in P(\mathbb{Z})$

Teorema - Unicità dell'inversa

Se f ha una sezione s e una retrazione r, allora:

1. $s = r$
2. s è un'inversa di f
3. s è l'unica sezione di f

4. s è l'unica retrazione di f
5. s è l'unica inversa di f

Dimostrazione $r = r_o id_b = r_o(f_o s) = (r_o f)_o s = id_{a_o} s = s$

Nota - sull'unicità dell'inversa

Se vale la prima proprietà e $a = \emptyset$, allora $b = \emptyset$ perché f è suriettiva, quindi $f = id_\emptyset$ ed ha se stessa come inversa.

Operazioni Binarie

Definizione - Operazione Binaria

Sia a un'insieme, un'operazione binaria (ovunque definita) in a è un'applicazione $a \times a \longmapsto a$.

Definiamo una generica operazione $* : (x, y) \in a \times a \longmapsto x * y \in a$, può avere le seguenti proprietà:

- **Commutativa**: $\forall x, y \in a(x * y = y * x)$.
- **Associativa**: $\forall x, y, z \in a(x * (y * z) = (x * y) * z)$.

Teorema - Associatività

Se un'operazione è associativa, presi n elementi, qualsiasi sia l'ordine delle operazioni, il risultato sarà sempre lo stesso.

Teorema - Commutatività

Se un'operazione è commutativa, dati n elementi, qualsiasi sia l'ordine degli elementi, il risultato sarà sempre lo stesso.

Definizione - Parti Chiuse

Sia $* : S \times S \longmapsto S$ e $T \subseteq S$, possiamo dire che T è una parte chiusa in una struttura $(S, *)$ se presi due elementi da T e eseguita l'operazione binaria, il risultato è sempre un elemento di T, in simboli:

$$T \text{ è una parte chiusa nella struttura } (S, *) \Leftrightarrow (\forall x, y \in T(x * y \in T))$$

Definizione - Operazione Indotta

Data l'operazione $* : S \times S \longmapsto S$ e preso $T \subseteq S$, l'operazione indotta è un'operazione binaria definita nel sottoinsieme della struttura originale, ereditando le proprietà di commutatività e Associatività.

$$\text{Operazione indotta da } * \text{ a } T\text{: } (x, y) \in T \times T \longmapsto x * y \in T$$

Definizione - Operazione Opposta

Sia $* : S \times S \longmapsto S$ la sua opposta sarà $*^{op} : (x, y) \in S \times S \longmapsto y * x \in S$, in simboli:

$$\forall x, y \in S(x *^{op} y = y * x)$$

Da dove possiamo dedurre le seguenti proprietà:

- $(*^{op})^{op} = *$
- Se $*$ è commutativa : $*^{op} = *$

- $*^{op}$ è associativa $\Leftrightarrow$ $*$ è associativa

Elementi Neutri, Simmetrici e Cancellabili

Definizione - Elementi Neutri

Sia $* : S \times S \longmapsto S$ un'operazione binaria e $t \in S$ possiamo dire:

- t è un elemento neutro-a-sinistra in $(S, *) \Leftrightarrow \forall x \in S(t * x = x)$
- t è un elemento neutro-a-destra in $(S, *) \Leftrightarrow \forall x \in S(x * t = x)$
- t è un elemento neutro in $(S, *) \Leftrightarrow \forall x \in S(t * x = x = x * t)$

Teorema - Unicità dei Neutri

Data l'operazione binaria $* : a \times a \longmapsto a$ se nella struttura $(S, *)$ esistono un neutro-a-sinistra "s" e un neutro-a-destra "d", allora:

1. $d = s$
2. d è un neutro in $(S, *)$
3. d è l'unico neutro-a-destra in $(S, *)$
4. d è l'unico neutro-a-sinistra in $(S, *)$
5. d è l'unico neutro in $(S, *)$

Dimostrazione: $\forall x \in a \begin{cases} s * x = x \\ x * d = x \end{cases} \Rightarrow s = s * d = d$

Nota - Non esiste più di un neutro se unico

Se un'operazione binaria ha un neutro, è unico, se ha più di un neutro-a-sinistra non ha neutro-a-destra e viceversa.

Definizione - Elementi Simmetrici

Sia $(S, *, t)$ un monoide e $x, y \in S$ possiamo dire:

- y è un simmetrico-a-sinistra di x in $(S, *) \Leftrightarrow \exists y \in S(y * x = t)$
- y è un simmetrico-a-destra di x in $(S, *) \Leftrightarrow \exists y \in S(x * y = t)$
- y è un simmetrico di x in $(S, *) \Leftrightarrow \exists y \in S(y * x = t = x * y)$

Nota - Simmetrico non vuol dire simmetrizzabile

Un elemento simmetrizzabile è un elemento che ha un simmetrico!

Teorema - Unicità dei Simmetrici

Data l'operazione binaria $* : a \times a \longmapsto a$ se nel monoide $(S, *, t)$ esistono un simmetrico-a-sinistra "s" e un simmetrico-a-destra "d", allora:

1. $d = s$

2. d è un simmetrico in $(S, *)$
3. d è l'unico simmetrico-a-destra in $(S, *)$
4. d è l'unico simmetrico-a-sinistra in $(S, *)$
5. d è l'unico simmetrico in $(S, *)$

Dimostrazione: $d = t * d = (s * x) * d = s * (t * d) = s * t = s$

Nota - Non esiste più di un simmetrico se unico

Se un'operazione binaria ha un simmetrico, è unico, se ha più di un simmetrico-a-sinistra non ha simmetrico-a-destra e viceversa.

Definizione - Elementi Cancellabili

Sia $* : S \times S \longmapsto S$ un'operazione binaria nell'insieme S.

$$\text{Fissato } a \in S \begin{cases} \sigma_a : x \in S \longmapsto a * x \in S \text{ Traslazione sinistra definita da } a \in (S, *) \\ \delta_a : x \in S \longmapsto x * a \in S \text{ Traslazione destra definita da } a \in (S, *) \end{cases}$$

Possiamo quindi dire:

- a è cancellabile a sinistra in $(S, *) \Leftrightarrow \sigma_a$ è iniettiva $\Leftrightarrow \forall x, y \in S((a * x = a * y) \Rightarrow (x = y))$
- a è cancellabile a destra in $(S, *) \Leftrightarrow \delta_a$ è iniettiva $\Leftrightarrow \forall x, y \in S((x * a = y * a) \Rightarrow (x = y))$
- a è cancellabile in $(S, *) \Leftrightarrow \sigma_a \wedge \delta_a$ sono iniettiva $\Leftrightarrow \forall x, y \in S((a * x = a * y \wedge x * a = y * a) \Rightarrow (x = y))$

Trasformazioni e Permutazioni

Definizione - Trasformazioni di un'insieme

Definite le applicazioni da a ad a : $\{M = Map(a, a) = T(a)\}$ e l'operazione binaria $_o : M \times M \longmapsto M$, questa operazione non è commutativa se a ha almeno due elementi.

Domanda - Perché non è commutativa?

Se $x, y \in a$ e $x \neq y$, siano:

- $C_x : t \in a \longmapsto x \in a$.
- $C_y : t \in a \longmapsto y \in a$.

Allora si ottiene: $\forall t \in a \quad (C_x \, {}_o C_y)(t) = C_x(C_y(t)) = x \neq y = C_y(C_x(t)) = (C_y \, {}_o C_x)(t)$

Definizione - Gruppo delle Permutazioni di un'insieme

Dato un'insieme a il gruppo degli invertibili è $U(T(a), {}_o, id_a) = Sym(a) = \{\text{insieme delle trasformazioni biettive di } a\}$, allora possiamo dire:

- $f \in Sym(a)$ ha simmetrici destri (sezione) e simmetrici sinistri (retrazioni)
- È chiamato gruppo abeliano $\Leftrightarrow |a| \leq 2$

Domanda - Perché il gruppo delle permutazioni è abeliano solo se l'insieme ha al massimo 2 elementi?

La commutatività si verifica $\Leftrightarrow Sym(a) = \{id_a, \alpha\}$, supponiamo l'insieme $a = \{0, 1\}$, allora:

$$id_a : a \longmapsto a \begin{cases} 0 \longmapsto 0 \\ 1 \longmapsto 1 \end{cases}$$

$$\alpha : a \longmapsto a \begin{cases} 0 \longmapsto 1 \\ 1 \longmapsto 0 \end{cases}$$

Quindi $\forall x, y \in Sym(a)(x * y = y * x)$

Permutazioni Cicliche

Definizione - Permutazioni Cicliche

Dati n elementi una permutazione è detta ciclica quando partendo da x_1 si arriva ad x_n per poi ripetersi.

$$\underbrace{x_1 \longmapsto x_2 \longmapsto x_3 \longmapsto ..... \longmapsto x_n}_{\longleftarrow}$$

Tavola di Cayley

Definizione - Tavola di Cayley

Questa tavola permettere di rappresentare tramite una tabella tutti i risultati di un'operazione binaria e ricavarne tante informazioni utili, ad esempio preso l'insieme $S = \{t, a, b\}$ con tre elementi diversi fra loro, dunque $(t \neq a \neq b \neq t)$:

$*$	t	a	b
t	$t * t$	$t * a$	$t * b$
a	$a * t$	$a * a$	$a * b$
b	$b * t$	$b * a$	$b * b$

Domanda - Cosa riusciamo a leggere dalla Tavola di Cayley?

- **Elemento Neutro**: se poniamo t come l'elemento neutro, noteremo nella sua riga e nella sua colonna come risultato dell'operazione l'elemento con il quale è stato messo in operazione.
- **Simmetrico**: un elemento ha un simmetrico se nella sua riga o colonna appare l'elemento neutro.
- **Cancellabilità**: non sono presenti ripetizioni nella riga e colonna di un elemento cancellabile.
- **Commutatività**: se l'operazione binaria è commutativa le operazioni rispetto alla linea diagonale avranno gli stessi risultati.

Potenze

Definizione - Potenze di un elemento

Dato il semi-gruppo $(S, *)$ con $x \in S$, diamo la seguente definizione $x^1 = x$, quindi: $\forall n \in \mathbb{N}^* \; x^{n+1} := x^n * x$.

Se $(S, *, t)$ è un monoide abbiamo che $x^0 = t$.

Se $(S, *, t, ')$ è un gruppo otteniamo che $x^{-n} := (x')^n$, ovvero il simmetrico di x^n.

Le potenze di stessa base commutano
$\forall x \in S\ \forall n, m \in \mathbb{Z}$ le potenze di uno stesso intero che appiano nelle formule hanno la proprietà commutativa:

$$x^{n+m} = x^n * x^m = x^m * x^n = x^{m+n}$$
$$x^{n \cdot m} = (x^n)^m = (x^m)^n = x^{m \cdot n}$$

Multipli

Definizione - Multipli

Dato il semi-gruppo $(S, *)$ con $x \in S$ possiamo dire che $1x = x$ e dare la seguente definizione:

$$\forall n \in \mathbb{N}^*\ (n+1)x = nx * x$$

Se $(S, *, t)$ un monoide abbiamo che $0x = t$

Se $(S, *, t, ')$ un gruppo otteniamo che $(-n)x := n(x')$, ovvero il simmetrico di nx.

I multipli di stesso elemento commutano
$\forall x \in S\ \forall n, m \in \mathbb{Z}$ i multipli di uno stesso intero che appiano nelle formule hanno la proprietà commutativa:

$$(n+m)x = nx + mx = mx + nx = (m+n)x$$
$$(n \cdot m)x = nm \cdot mx = mx \cdot nx = (m \cdot n)x$$

Strutture Algebriche

Definizione - Struttura Algebrica

Sia a un'insieme e data l'operazione $* : a \times a \longmapsto a$, $(a, *)$ è una struttura algebrica con operazione binaria.

Semi-Gruppo
La struttura algebrica $(a, *)$ è un semi-gruppo $\Leftrightarrow * : a \times a \longmapsto a$ è associativa, se tutti gli elementi sono cancellabili è chiamato **cancellativo**.

Monoide
Il semi-gruppo $(a, *, t)$ è un monoide se ha t come elemento neutro.

Sotto-Monoide
Per definizione $(b, *, t)$ è un sotto-monoide di $(a, *, t)$ se b è una parte chiusa rispetto a $(a, *, t)$ e $t \in b$ (hanno quindi lo stesso neutro).

Gruppo
Monoide $(a, *, t, ')$ in cui ogni elemento ha un simmetrico, se commutativo è chiamato **Abeliano**.

Sotto-Gruppo
Per definizione $(b, *, t, ')$ è un sotto-gruppo di $(a, *, t, ')$ se abbiamo $\emptyset \neq b \subseteq a$ e accade che $\Leftrightarrow \forall x, y \in b(x * y' \in b)$.

Semi-Gruppo

Teorema - In un **Semi-Gruppo finito** con un elemento cancellabile $\Rightarrow$ Monoide

Sia $(S, *)$ un semi-gruppo finito e sia $x \in S$, allora:

- x cancellabile a destra vuol dire che $\delta_x : a \in S \longmapsto a*x \in S$ è iniettiva, quindi suriettiva, allora esisterà il candidato neutro $\exists b \in S(b * x = x)$ ed ogni elemento di S lo possiamo riscrivere come $\forall y \in S(\exists y' \in S(y' * x = y)$
- x cancellabile a sinistra vuol dire che $\sigma_x : a \in S \longmapsto x * a \in S$ è iniettiva, quindi suriettiva, allora esisterà il candidato neutro $\exists c \in S(x*c = x)$ ed ogni elemento di S lo possiamo riscrivere come $\forall y \in S(\exists y' \in S(x*y' = y)$

Dimostrazione Unendo queste due nozioni posso dire che esiste un neutro perché c'è sia un neutro a destra che a sinistra ed essi coincidono:

- $\forall y \in S(b * y = y)$ perché $b * y = b * (x * y') = (b * x) * y' = x * y' = y$
- $\forall y \in S(y * c = y)$ perché $y * c = (y' * x) * c = y' * (x * c) = y' * x = y$

Monoide

Nota - Non tutti i monoidi hanno sotto-monoidi

1. $(\mathbb{N}, +, 0)$ è un sotto-monoide di $(\mathbb{Z}, +, 0)$
2. $P(\mathbb{N})$ è chiusa nel monoide $(P(\mathbb{Z}), \cap, \mathbb{Z})$ e con l'operazione indotta otteniamo il monoide $(P(\mathbb{N}), \cap, \mathbb{N})$ che non è un sotto-monoide.
3. $\mathbb{N}^*$ è chiusa nel monoide $(\mathbb{N}, +, 0)$ ma la struttura $(\mathbb{N}^*, +)$ ottenuta con l'operazione indotta non è un monoide.

Teorema - Simmetrizzabile è Cancellabile in un Monoide

Sia $(S, *, t)$ un monoide con $a \in S$, allora:

- a è simmetrizzabile a destra $\Rightarrow$ a è cancellabile a destra
- a è simmetrizzabile a sinistra $\Rightarrow$ a è cancellabile a sinistra
- a è simmetrizzabile $\Rightarrow$ a è cancellabile

Dimostrazione: se a è simmetrizzabile a sinistra $\Rightarrow$ a è cancellabile a sinistra, allora:

$$\exists b \in S(b * a = t) \mid a * x = a * y \Rightarrow b * (a * x) = b * (a * y) \Rightarrow (b * a) * x = (b * a) * y \Rightarrow t * x = t * y \Rightarrow x = y$$

Definizione - Gruppo dei simmetrizzabili di un Monoide

Sia $(S, *, t)$ un monoide, poniamo $U(S) = \{x \in S : x \text{ è simmetrizzabile rispetto a } *\}$, allora:

1. $t \in U(S)$
2. $U(S)$ è una parte chiusa e sotto-monoide di $(S, *, t)$
3. $(U(S), *, t)$ è un gruppo

Esempio - Gruppi di simmetrizzabili di Monoidi

$U(\mathbb{Z}, \cdot) = \{-1, 1\}$

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

$U(P(a), \cap) = \{a\}$

$U(\mathbb{Q}, \cdot) = (\mathbb{Q} \setminus \{0\}, \cdot)$

Teorema - In un Monoide finito cancellabile implica simmetrizzabile

Sia $(M, *, t)$ un monoide finito con $x \in M$, allora:

1. x è cancellabile a destra $\Rightarrow$ x è simmetrizzabile sinistra
2. x è cancellabile a sinistra $\Rightarrow$ x è simmetrizzabile destra

Dimostrazione

1. x cancellabile a destra vuol dire che $\delta_x : a \in M \longmapsto a * x \in M$ è un'applicazione iniettiva, ma anche suriettiva essendo in un monoide finito, quindi $t \in im\ \delta_x$ ovvero $\exists a \in M \mid a * x = t$.
2. x cancellabile a sinistra vuol dire che $\sigma_x : a \in M \longmapsto x * a \in M$ è un'applicazione iniettiva, ma anche suriettiva essendo in un monoide finito, quindi $t \in im\ \sigma_x$ ovvero $\exists a \in M \mid x * a = t$.

Monoide Fattoriale

Definizione - Monoide Fattoriale

Sia $(M, \cdot, t)$ un monoide commutativo, è detto fattoriale se e solo se:

- M è cancellativo (ogni suo elemento è cancellabile)
- $\forall a \in M \setminus U(M)$ abbiamo che a è un prodotto irriducibile, in modo unico a meno di ordine di fattori e sostituzione con associati

Quindi otteniamo che $\forall a \in \mathbb{N}(a > 1)$ sarà prodotto di primi

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$$

!ATTENZIONE! in questo monoide abbiamo sempre MCD e MCM

Esempio - Monodi Fattoriali

Sono monoidi fattoriali $(\mathbb{N}^*, \cdot)$ e $(\mathbb{Z} \setminus \{0\}, \cdot)$

Tutti i gruppi abeliani sono monodi fattoriali!

Domanda - Come faccio a controllare se un numero grande sia primo?

Per semplificare il compito di controllare se un numero con molte cifre è primo non è necessario vedere se tutti i numeri primi che lo precedono lo dividono, ma basta controllare il più piccolo che lo divide, infatti:

$$\forall n \in \mathbb{N}^*((n > 1 \ \wedge \ n \notin \mathbb{P}) \Rightarrow (\exists p \in \mathbb{P}(p \mid n \ \wedge \ p < \sqrt{n})))$$

Se chiamiamo p il più piccolo primo che divide n allora otteniamo due casi possibili:

1. $p = n$ allora sappiamo che n è primo

2. p fa parte della scomposizione di n dove appaiono almeno due fattori, dove appare un un secondo fattore q che è più grande di p allora otteniamo che $p^2 \leq p \cdot q \leq n$

Esempio - Controllare che un numero grande sia primo

Prendiamo $\exists m \in \mathbb{N}^*(m \leq 100)$ basta controllare che esso sia divisibile per $2, 3, 5, 7$ per non essere primo perché ha un primo minore $\sqrt{m} \leq \sqrt{100} = 10$

Domanda - Come trovo i divisori di un elemento di un monoide fattoriale?

Sia $d \in \mathbb{N} \ \wedge \ d \mid a$ allora siamo certi che i divisori di d saranno anche quelli di a perché

$$d = \prod_{i=1}^{k} p_i^{\delta_i} \text{ dove l'esponente } \delta_i \in \mathbb{N} \ \wedge \ \delta_i \leq \alpha_i$$

Il vincolo di δ_i nasce dall'essere sempre un divisore di a ovvero se $d \mid a$ allora per definizione $\exists c \in \mathbb{N}^*(a = d \cdot c)$ cioè scomponendo d e c in fattori primi abbiamo, come in esempio $12 = (2^u \cdot 3^v)(2^h \cdot 3^k) = 2^{u+h} \cdot 3^{v+h}$ quindi in generale

$$d \cdot \prod_{i=1}^{k} p_i^{\alpha_i - \delta_i} = \prod_{i=1}^{k} p_i^{\delta_i} \cdot p_i^{\alpha_i - \delta_i} = \prod_{i=1}^{k} p_i^{\alpha_i} = a$$

Da questo possiamo trarre che se conosciamo la fattorizzazione di a conosciamo anche tutti i suoi divisori, infatti

$$\underset{(\mathbb{N}^*,\cdot)}{\text{Div(a)}} = \{\prod_{i=1}^{k} p_i^{\delta_i} \mid \forall i \in \{1, 2, ..., k\}(\delta_i \leq \alpha_i \in \mathbb{N})\}$$

Sappiamo anche contare il numero di divisori effettuando il prodotto tra le possibili combinazioni di esponenti

$$|\underset{(\mathbb{N}^*,\cdot)}{\text{Div(a)}}| = \prod_{i=1}^{k} (\alpha_i + 1)$$

Esempio - Divisori di un intero

Sia $a = 12$ allora sappiamo che la sua scomposizione in primi è $12 = 2^2 \cdot 3^1$ e i suoi divisori sono:

- $1 = 2^0 \cdot 3^0$
- $2 = 2^1 \cdot 3^0$
- $3 = 2^0 \cdot 3^1$
- $4 = 2^2 \cdot 3^0$
- $6 = 2^1 \cdot 3^1$
- $12 = 2^2 \cdot 3^1$

Se consideriamo i divisori in $\mathbb{Z}$ includiamo gli associati.

Se vogliamo contare la cardinalità, basta guardare la scomposizione in fattori primi, ad esempio

- $12 = 2^2 \cdot 3^1$
  - In $\mathbb{N}$ abbiamo che $|Div(12)| = (2+1) \cdot (1+1) = 3 \cdot 2 = 6$
  - In $\mathbb{Z}$ abbiamo che $2|Div(12)| = 2 \cdot 6 = 12$ ovvero raddoppiamo il numero per ottenere gli associati

- $30 = 2^1 \cdot 3^1 \cdot 5^1$
  - In $\mathbb{N}$ abbiamo che $|Div(30)| = (1+1)\cdot(1+1)\cdot(1+1) = 2\cdot 2\cdot 2 = 8$
  - In $\mathbb{Z}$ abbiamo che $2|Div(30)| = 2\cdot 8 = 16$ perché aggiungiamo ancora una volta gli associati

Domanda - Sfruttando la scomposizione in fattori primi posso trovare anche MCD e MCM?

Certamente che posso, perché anche se due numeri hanno una scomposizione con fattori diversi, aggiungere i fattori non in comune con esponente 0 e non avere variazioni nella loro scomposizione o descrizione dei divisori.

Quindi se considero i numeri a e b dove i loro esponenti $\alpha_i, \beta_i \in \mathbb{N}$ possono sceglierli con gli stessi primi e quindi trovare i divisori in comune.

- Per trovare i divisori in comune basta scegliere un numero $d \mid a \ \wedge \ d \mid b \Leftrightarrow \forall i \in \{0,1,2,\dots,k\}\ \delta_i \leq \min\{\alpha_i, \beta_i\}$
- Per trovare l'MCD basta scegliere $d := \prod_{i=1}^{k} p_i^{\sigma_i}$ dove l'esponente $\sigma := min\{\alpha_i, \beta_i\}\ \forall i \in \{1,2,\dots,k\}$
- Per trovare l'MCM basta scegliere $m := \prod_{i=1}^{k} p_i^{\mu_i}$ dove l'esponente $\mu := max\{\alpha_i, \beta_i\}\ \forall i \in \{1,2,\dots,k\}$

Nota - A cosa equivale il prodotto dell'MCD e l'MCM?

Sappiamo che l'MCD e il prodotto dei fattori con esponente minore tra i due numeri e l'MCM invece e il prodotto dei fattori con esponente maggiore tra i due, quindi otteniamo che

$$d \cdot m = \prod_{i=1}^{k} p_i^{\sigma_i} \cdot p_i^{\mu_i} = \prod_{i=1}^{k} p_i^{\sigma_i+\mu_i} = \prod_{i=1}^{k} p_i^{\alpha_i+\beta_i} = a \cdot b$$

Quindi sappiamo che nei monoidi fattoriali esiste sempre l'MCD e l'MCM ed è sempre associato al prodotto tra a e b

Esempio - MCD e MCM

Siano $a = 12$ e $b = 45$, ovvero due numeri con scomposizioni diverse, io posso aggiungere i fattori primi non in comune con esponente zero ottenendo

- $a = 12 = 2^2 \cdot 3^1 \cdot 5^0$
- $b = 45 = 2^0 \cdot 3^2 \cdot 5^1$

Quindi trovo i divisori comuni, l'MCD e l'MCM

- Divisori comuni
  - $1 = 2^0 \cdot 3^0 \cdot 5^0$
  - $3 = 2^0 \cdot 3^1 \cdot 5^0$
- $MCD = 3 = 2^0 \cdot 3^1 \cdot 5^0$
- $MCM = 180 = 2^2 \cdot 3^2 \cdot 5^1$

Teorema - Bézout

Siano $a, b \in \mathbb{Z}$ e $d = MCD(a, b)$ noi sappiamo che

1. d è una combinazione lineare di a e b, ovvero $d \in \{au + bv \mid u, v \in \mathbb{Z}\}$ ma quindi ogni multiplo di d è una combinazione lineare quindi $d\mathbb{Z} \in \{au + bv \mid u, v \in \mathbb{Z}\}$
2. Essendo $d = MCD(a, b)$ allora $d\mathbb{Z} = \{au + bv \mid u, v \in \mathbb{Z}\}$
3. a e b sono comprimi $\Leftrightarrow \exists u, v \in \mathbb{Z}(1 = au + bv) \Leftrightarrow$ l'$MCD(a, b) = 1$
4. Sia data un'equazione diofantea $ax + by = c$, essa ha soluzione solo se c è combinazione lineare di a e b
5. Sia data un'equazione congruenziale $ax \underset{b}{\equiv} c$, essa ha soluzione solo se $d = MCD(a, b) \ \wedge \ d \mid c$

Dimostrazione

1. Questo perché $\forall k \in \mathbb{Z}((d = au + bv) \Rightarrow (dk = a(uk) + b(vk)))$
2. Essendo che $d \mid a \ \wedge \ d \mid b$ allora otteniamo la doppia inclusione $d\mathbb{Z} \subseteq \{au + bv \mid u, v \in \mathbb{Z}\} \subseteq d\mathbb{Z}$
3. Se 1 e combinazione lineare di a e b deve essere multiplo dell'$MCD(a, b)$ ma 1 e multiplo solo di $\{1, -1\}$
4. Ponendo c come combinazione lineare di a e b allora abbiamo che $d = MCD(a, b) \ \wedge \ d \mid c$ e quindi $c \in d\mathbb{Z}$
5. Riformuliamo l'equazione congruenziale come combinazione lineare e la dimostrazione è analoga

Sotto-gruppo

Teorema - Dimostrazione Sotto-Gruppo

Sia $(G, *, t, ')$ un gruppo e sia $\emptyset \neq H \subseteq G$, allora H è un sotto-gruppo di $G \Leftrightarrow \forall x, y \in H(x * y' \in H)$.
Definiamo l'operazione binaria $\# : (x, y) \in H \longmapsto x * y' \in H$, allora possiamo dimostrare che:

1. H e sotto-monoide di G: abbiamo $H \neq \emptyset$ allora $\exists a \in H(a \ \# \ a = t \in H)$.
2. H è un sotto-gruppo di G: abbiamo $\forall a \in H(t \ \# \ a = a' \in H)$.
3. H è chiuso rispetto a $*$: abbiamo $\forall a, b \in H(a \ \# \ b' = a * b \in H)$.

Intersezione Unaria di parti chiuse

Teorema - Intersezione unaria delle parti chiuse

Sia $(S, *)$ una struttura algebrica dove $* : S \times S \longmapsto S$ e $\emptyset \neq L \subseteq P(S)$, allora $\forall x \in L(x$ è chiusa rispetto a $*)$ abbiamo che $\bigcap L$ è chiusa rispetto a $*$.

Dimostriamo quindi che $\forall x, y \in \bigcap L(x * y \in \bigcap L)$:

- fissiamo $x, y \in \bigcap L$
- Sia $a \in L$
- sappiamo che a è chiusa rispetto a $*$ e inoltre $x, y \in a$, quindi anche $x * y \in a$

Infine abbiamo che: $\forall x, y \in \bigcap L(\forall a \in L(x * y \in a))$

Definizione - Parte chiusa generata da una parte

Sia $T \subseteq S$ e chiamato $L_T = \{x \in P(S) \mid T \subseteq x \text{ con } x \text{ chiusa rispetto a } *\}$, possiamo dire:

- $S \subseteq L_T$ quindi $L_T \neq \emptyset$.
- $\bigcap L_T$ è chiusa rispetto a $*$.
- $T \subseteq \bigcap L_T$ e quindi $\bigcap L_T \in L_T$.

$\bigcap L_T$ è la parte chiusa generata da T in $(S, *)$ (l'intersezione di tutte le parti chiuse contenenti T).

Esempio - Parti chiuse generate da una parte

Per un generico $\{x\}$:

- Parte chiusa generata dal $\{x\}$ è l'insieme $\{x^n \mid n \in \mathbb{N}^*\}$
- Sotto-monoide generato dal $\{x\}$ è l'insieme $\{x^n \mid n \in \mathbb{N}\}$
- Sotto-gruppo generato dal $\{x\}$ è l'insieme $\{x^n \mid n \in \mathbb{Z}\}$

Per il $\{2\}$:

- Parte chiusa generata dal $\{2\}$ è l'insieme $\{2n \mid n \in \mathbb{N}^*\}$
- Sotto-monoide generato dal $\{2\}$ è l'insieme $\{2n \mid n \in \mathbb{N}\}$
- Sotto-gruppo generato dal $\{2\}$ è l'insieme $\{2n \mid n \in \mathbb{Z}\}$

Gruppo Ciclico

Definizione - Gruppo Ciclico

Dato il gruppo $(S, *)$ è detto ciclico $\Leftrightarrow \exists x \in S(S$ è il sottogruppo di S generato dal $\{x\})$, in questo caso $S = \{x^n \mid n \in \mathbb{Z}\}$

Esempio - Gruppo ciclico

$\mathbb{Z} = \{1^n \mid n \in \mathbb{Z}\}$

Cardinalità

Definizione - Prinicipio di buon ordinamento dei numeri naturali

Per ogni parte non vuota $x \in \mathbb{N}$, esiste il minimo di x, ovvero $\exists a \in x(\forall b \in x(a \leq b))$

Teorema - Due insieme equipotenti hanno un'applicazione biettiva tra loro

$\forall n \in N \quad I_n = \{i \in N^* \mid i \leq n\}$
$\forall n, m \in N \quad n \neq m \Rightarrow$ non esistono applicazioni biettive da $I_n \longmapsto I_m$.

Infatti se chiamiamo $C = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N} \setminus \{n\}(\exists f \in Map(I_n, I_m)(f \text{ è biettiva}))\}$ e dimostriamo che $C = \emptyset$.

Dimostrazione: se $C \neq \emptyset$ e $C \subseteq \mathbb{N}$ possiamo dire che esiste il minimo elemento di C che chiamiamo h, allora:

$$\exists m \in \mathbb{N} \quad \exists f : I_h \longmapsto I_m \text{ con } f \text{ applicazione biettiva}$$

Poniamo $a = f(h)$ e analizziamo i due casi possibili

1. $a = m$, quindi effettuiamo la restrizione eliminando h dal dominio:

   $$f_{I_{h-1}} : x \in I_{h-1} \longmapsto f(x) \in I_m \text{ con } f \text{ iniettiva}$$

   Quindi $im\ f_{I_{h-1}} = I_m \setminus \{a\}$ ed effettuando anche la riduzione eliminando a dal codominio:

   $$f_{I_{h-1}}^{I_{m-1}} : x \in I_{h-1} \longmapsto f(x) \in I_{m-1} \text{ con } f \text{ biettiva}$$

   Allora $g : I_{h-1} \longmapsto I_{m-1}$ è biettiva, quindi $h-1, m-1 \in \mathbb{N}$ e per la definizione di C sappiamo che $h-1 \in C$.
   Conclusione: è assurdo perché h è il minimo di C.

2. Sia $\sigma : I_m \longmapsto I_m$ biettiva.

   Definiamola $\begin{cases} \sigma(a) = m \\ \sigma(m) = a \\ \forall x \in I_m \setminus \{a, m\} = \sigma(x) = x \end{cases}$ e la sua composta $\sigma_o f : I_h \longmapsto I_m$ è biettiva.

   Conclusione: $(\sigma_o f)(h) = m$ verifica il Caso 1 dove $a = m$

Domanda - $h-1$ può essere minore di 0?

Analizziamo i casi possibili:

1. Se $n \neq 0$ e $m \neq 0$ allora $h-1 \geq 0$ e $m-1 \geq 0$
2. Se $n = 0$ allora il teorema è già dimostrato perché da $\emptyset$ a $\emptyset$ esiste un unica biettiva

Definizione - Insiemi equipotenti

Indico con $|a|$ la cardinalità dell'insieme, e uso la notazione $|a| = n \Leftrightarrow$ esiste $f : I_n \longmapsto a$ ed è biettiva.

Due insiemi a e b sono detti equipotenti $\Leftrightarrow \exists f \in Map(a, b)$ ed è biettiva (ed anche la sua inversa f^{-1} è biettiva).

Nota - Insiemi infiniti equipotenti

Gli insiemi "infiniti" (ricordiamo che infinito è un aggettivo e non una cardinalità) equipotenti sono $|\mathbb{N}^*| = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{N} \times \mathbb{N}|$ che differiscono da $|\mathbb{R}| = |P(\mathbb{N})|$.

Definizione - Cardinalità di insiemi finiti disgiunti

Supponiamo di avere gli insiemi A e B con cardinalità $a = |A|$ e $b = |B|$.

1. $\forall A, B, C, \ldots$ insiemi finiti e disgiunti tra loro, allora $A \cap B = \emptyset \Rightarrow |A \cup B| = |A| + |B|$
2. Se F è un insieme finito costituito da insiemi finiti disgiunti tra loro, ovvero $\forall x, y \in F(x \neq y \Rightarrow x \cap y = \emptyset)$, quindi $|\bigcup F| = \sum_{A \in F} |A|$
3. Dati gli insiemi A e B, gli elementi del prodotto cartesiano $|A \times B| = |A| \cdot |B| = \sum_{y \in B} |P_y|$ $(\forall y \in B(P_y = A \times \{y\}))$

Principio di Inclusione - Esclusione

Definizione - Principio di Inclusione - Esclusione

Generalizzando la cardinalità di insiemi, quindi senza assumere che essi siano disgiunti, allora otteniamo che:

- Dati gli insiemi A e B, gli elementi della loro unione saranno $|A \cup B| = |A| + |B| - |A \cap B|$
- Dati gli insiemi A, B e C allora gli elementi della loro unione saranno $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap B| - |B \cap C| + |A \cap B \cap C|$ (quindi come regola generale le intersezioni con numero di insiemi dispari ha segno positivo, con numero di insiemi pari ha segno negativo)

Domanda - Sommare le intersezioni con insiemi dispari e sottrarre con insiemi pari?

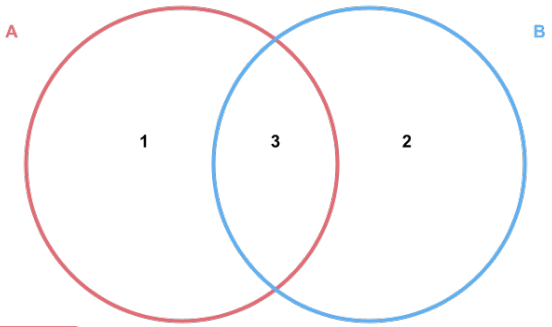
Prendiamo in esempio la cardinalità di due insiemi A e B, non sappiamo se essi sono disgiunti e quindi per evitare di contare più volte elementi che possano essere presenti nell'intersezione, ovvero più volte nella somma della cardinalità di A e B, andiamo a sottrarre l'intersezione tra gli insiemi, per rendere più chiara l'idea:

Se in una settimana vado a cena 4 volte in pizzeria e 7 sere vado al cinema, è possibile che in una settimana ci siano 11 giorni?

La risposta è no! Ovviamente ci saranno state sere in qui si è andati sia a cena in pizzeria che al cinema, per evitare quindi di contare due volte una stessa sera dove si è svolto entrambe le attività si sottrae il numero di sere in cui si sono svolte entrambe.

Osservando il diagramma di Venn a destra, vediamo come sono composti l'insieme $A = (A \setminus B) \cup (A \cap B)$ e l'insieme $B = (B \setminus A) \cup (A \cap B)$, sommando le singole cardinalità conteremmo due volte l'intersezione tra A e B, infatti osservando la tabella otteniamo:

$\|A\|$	1		3	+
$\|B\|$		2	3	+
$\|A \cap B\|$			3	-
$\|A \cup B\|$	1	2	3	=



Calcolo delle applicazioni

Definizione - Numero di applicazioni negli insiemi finiti

Dati gli insiemi A e B, il numero di applicazioni è $|Map(A, B)| = |B|^{|A|}$ (ovvero per ogni elemento del dominio A ho B scelte nel codominio).

Dati gli insiemi A e B, il numero di applicazioni iniettive è:

- Se $a > b$ allora non ne esistono $|InjMap(A, B)| = \emptyset$
- Se $a \leq b$ allora si usa il fattoriale discendente $|InjMap(A, B)| = \prod_{i=0}^{a-1}(b - i) = \frac{b!}{(b-a)!} = b^{\underline{a}}$
- Se $a = b$ allora il numero di applicazioni iniettive coincide con quelle biettive $|InjMap(A, B)| = |Sym(A)| = |A|!$

Teorema - L'esistenza delle funzioni dipende dalla cardinalità degli insiemi

Siano a e b insiemi finiti, allora:

1. Esistono applicazioni iniettive da a verso $b \Leftrightarrow |a| \leq |b|$
2. Esistono applicazioni biettive da a verso $b \Leftrightarrow |a| = |b|$
3. Esistono applicazioni suriettive da a verso $b \Leftrightarrow |a| \geq |b|$ e $b = \emptyset \Rightarrow a = \emptyset$

Dimostrazioni

1. Ritornando al discorso del fattoriale discendente ($b^{\underline{a}}$), se $|a| > |b|$ (il numero di elementi di a supera quello di b) il fattoriale non è definito (alcuni elementi di a non hanno immagine in b) quindi non esistono applicazioni inettive.
2. Se gli insiemi sono equipotenti, quindi $|a| = |b| = n$ posso dire che esistono le applicazioni $f : I_n \longmapsto a$ e $g : I_n \longmapsto b$, posso comporre le applicazioni composte $g_o f^{-1} : a \longmapsto b$ e $f_o g^{-1} : b \longmapsto a$ e ottenere un'applicazione biettiva da a verso b.
3. (a) "$\Rightarrow$" Se esiste l'applicazione suriettiva $f : a \longmapsto b$ allora questa applicazione ha una sezione $g : b \longmapsto a$, che è iniettiva, quindi sappiamo che $|a| \geq |b|$

   (b) "$\Leftarrow$" Se esiste l'applicazione iniettiva $g : b \longmapsto a$ allora osserviamo due casi:

   i. Se $b \neq \emptyset$ allora g ha una retrazione $f : a \longmapsto b$ che è suriettiva

   ii. Se $b = \emptyset$ e anche $a = \emptyset$ allora l'applicazione $g = id_\emptyset$ che è biettiva, altrimenti se $a \neq \emptyset$ non esistono applicazioni ($Map(a, b) = \emptyset$)

Teorema - Negli insiemi finiti equipotenti ogni applicazione è biettiva

Se $|a| = |b|$ allora $\forall f \in Map(a, b)$ vale:

1. f è iniettiva
2. f è suriettiva
3. f è biettiva

Dimostrazione

1. Se f è un'applicazione iniettiva io posso chiamare $c = im\ f$ e ottenere l'applicazione biettiva:

   $$f^{|c} : x \in a \longmapsto f(x) \in c$$

   Quindi sappiamo che $|c| = |a| = |b|$ e quindi $c = b$.
2. Se $f : a \to b$ è suriettiva allora avrà una sezione $g : b \to a$ iniettiva, ma allora anche f che è la retrazione di g (e la sua inversa) sarà biettiva.

Teorema - Negli insiemi finiti equipotenti l'applicazione immagine è biettiva

Siano A e B insiemi finiti ed equipotenti, quindi $f : A \longmapsto B$ è biettiva, allora anche $P(A)$ sarà equipotente a $P(B)$, quindi $\overrightarrow{f} : P(A) \longmapsto P(B)$ è biettiva.

Dimostrazione Date le due funzioni:

- $\overrightarrow{f} : P(A) \longmapsto P(B)$ ottengo che $\forall X \subseteq A\ \overrightarrow{f}(X) = \{f(x) \mid x \in X\}$

- $\overleftarrow{f} : P(B) \longmapsto P(A)$ ottengo che $\forall Y \subseteq B \ \overleftarrow{f}(Y) = \{f^{-1}(y) \mid y \in Y\}$

Proviamo che $\overrightarrow{f} \circ \overleftarrow{f} = id_{P(B)}$ e che $\overleftarrow{f} \circ \overrightarrow{f} = id_{P(A)}$, allora:

1. $(\overleftarrow{f} \circ \overrightarrow{f})(X) = \{f^{-1}(f(x)) \mid x \in X\} = \{x \mid x \in X\} = X$
2. $(\overrightarrow{f} \circ \overleftarrow{f})(Y) = \{f(f^{-1}(y)) \mid y \in Y\} = \{y \mid y \in Y\} = Y$

Calcolo Combinatorio

Funzione Caratteristica

Definizione - Funzione Caratteristica

Dato l'insieme S e l'insieme $T \subseteq S$ definiamo la funzione caratteristica di T in S:

$$\chi_{T,S} : x \in S \longmapsto \begin{cases} 1 \text{ se } x \in T \\ 0 \text{ se } x \notin T \end{cases} \in \{0,1\}$$

Quindi la funzione caratteristica è un'applicazione biettiva tra due insiemi da confrontare, distingue gli elementi che non sono presenti da quelli che sono presenti in T, in questo caso abbiamo che un elemento è presente in T se la funzione caratteristica gli associa 1 altrimenti se non è presente la funzione caratteristica gli associa 0.

Teorema - Biettività della funzione caratteristica

Per dimostrare la biettività di questa funzione definiamo $M = Map(S, \{0,1\})$ e le applicazioni:

- $\alpha : T \in P(S) \longmapsto \chi_{T,S} \in M$
- $\beta : f \in M \longmapsto \overleftarrow{f}(\{1\}) \in P(S)$

Dimostrazione Per dimostrane la biettività dobbiamo far vedere che $\alpha \circ \beta = id_M$ e $\beta \circ \alpha = id_{\chi_{T,S}}$, quindi che α e β sono una l'inversa dell'altra:

- $\alpha \circ \beta : M \longmapsto M$ quindi otteniamo che $\forall f \in M \ (\alpha \circ \beta)(f) = \alpha(\beta(f)) = \alpha(\overleftarrow{f}(\{1\})) = \chi_{T,S}$
- $\beta \circ \alpha : P(S) \longmapsto P(S)$ quindi otteniamo che $\forall T \in P(S) \ (\beta \circ \alpha)(T) = \beta(\alpha(T)) = \beta(\chi_{T,S}) = \{x \in S \mid \chi_{T,S}(x) = 1\} = \{x \in S \mid x \in T\} = S \cap T = T$

Contare l'insieme delle parti

Definizione - Gli elementi di P(S) - Insieme finito

Sia S un'insieme finito, allora $P(S)$ sarà calcolato con $|P(S)| = |Map(S, \{0,1\})| = 2^{|S|}$, ovvero alla cardinalità del codominio (che corrisponde a 2 perché abbiamo la funzione caratteristica) elevato alla cardinalità di S.

Coefficiente binomiale

Definizione - Coefficiente binomiale

Dato un'insieme S vogliamo contare le sue parti che hanno k elementi, dove $\forall k \in \mathbb{N}$, ovvero prendiamo l'insieme $P_k(S) = \{x \subseteq S \mid |x| = k\}$.

La cardinalità viene così calcolata $\forall n, k \in \mathbb{N}$ $\binom{n}{k} = |P_k(S)|$ dove però $n = |S|$.

Nota - Coefficienti binomiali notevoli

- $\binom{n}{0} = 1$ corrisponde all'insieme $P_0(S) = \{\emptyset\}$
- $\binom{n}{1} = n$ corrisponde all'insieme $P_1(S) = \{\{x\} \mid x \in S\}$
- $\binom{n}{n} = 1$ corrisponde all'insieme $P_n(S) = S$
- $\forall k \in \mathbb{N}$ se $k > n$ abbiamo che $\binom{n}{k} = 0$

Teorema - Insiemi equipotenti implica insiemi delle k parti equipotenti

Siano T e S insiemi finiti equipotenti, ovvero $|T| = |S|$ quindi esiste $f : S \longmapsto T$ biettiva, ma questo vuol dire che $\overrightarrow{f} : P(S) \longmapsto P(T)$ è biettiva, ricaviamo che anche $|P_k(T)| = |P_k(S)|$.

Dimostrazione Sappiamo che $\forall k \in \mathbb{N}$ $P_k(S) \subseteq P(S)$ e se applichiamo la restrizione otteniamo un'applicazione iniettiva:

$$\overrightarrow{f}_{|P_k(S)} : P_k(S) \longmapsto P(T)$$

Se applichiamo anche la riduzione a $im\ f$ (che è uguale a $P_k(T)$) otteniamo invece un'applicazione biettiva:

$$\overrightarrow{f}^{|im\ f}_{|P_k(S)} : P_k(S) \longmapsto \overrightarrow{f}(x) \in P_k(T)$$

Ricaviamo quindi che $\forall x \in P(S)$ abbiamo che $|\overrightarrow{f}(x)| = |x|$ e quindi $|T| = |S| \Rightarrow |P_k(T)| = |P_k(S)|$

Domanda - Come si calcola la somma di tutti le $P_k(S)$?

Definito il coefficiente binomiale come la cardinalità dell'insieme con k parti di un'insieme S con cardinalità n, la cardinalità dell'insieme delle parti di S è pari a 2^n, ovvero l'unione di tutti gli insiemi di k parti di S:

$$|\bigcup_{k=0}^{n} P_k(S)| = |P(S)| = 2^n$$

Ma questo è vero solo se gli insiemi sono a due a due disgiunti tra loro: $\forall i, j \in \mathbb{N}(i, j \leq n \wedge i \neq j) \Rightarrow (P_i(S) \cap P_j(S) = \emptyset)$

Per definizione del coefficiente binomiale allora sappiamo che è vero che $\forall n \in \mathbb{N} \sum_{k=0}^{n} \binom{n}{k} = 2^n$

Teorema - Proprietà simmetrica del Coefficiente binomiale

Per dimostrarne la proprietà simmetrica dobbiamo provare che esiste un'applicazione biettiva da $P_k(S)$ al suo complemento $P_{n-k}(S)$, per fare ciò partiamo da un'applicazione iniettiva $f : a \to b$ dalla quale deduciamo che tutte le sue restrizioni e riduzioni sono iniettive.

In particolare però $\forall c \in P(a)$ se applichiamo una restrizione a c e una riduzione a $im\ f$ otteniamo un'applicazione

biettiva:

$$g : x \in c \longmapsto f(x) \in im\ f$$

Se prendiamo l'applicazione che ci da il complemento di $P(S)$:

$$c : x \in P(S) \longmapsto S \setminus x \in P(S) \text{ questa è biettiva } (c_o c = id_{P(S)})$$

Dato un'insieme finito $|S| = n$ sappiamo che:

$$\forall k \in \mathbb{N}(k \leq n)\ P_k(S) \subseteq P(S)$$

Allora l'immagine di $P_k(S)$ tramite l'applicazione c sarà costituita dal complemento di $P(S)$ con elementi che hanno cardinalità $n - k$, cioè $\overrightarrow{c}(P_k(S)) = P_{n-k}(S)$.

Applicando la restrizione la riduzione a c otteniamo un'applicazione biettiva:

$$c : x \in P_k(S) \longmapsto S \setminus x \in P_{n-k}(S) \text{ con inversa } c^{-1} : x \in P_{n-k}(S) \longmapsto S \setminus x \in P_k(S)$$

Quindi questa applicazione verifica la simmetria dei coefficienti binomiali: $\forall n \in \mathbb{N}\ \forall k \in \mathbb{N}\ (k \leq n) \Rightarrow (\binom{n}{k} = \binom{n}{n-k})$

Nota - L'uso delle applicazioni biettive nel Calcolo combinatorio

Le applicazioni biettive sono usate nel calcolo combinatorio perché permettono di contare il numero di elementi di un'insieme in maniera molto rapida.

Teorema - In $P(S)$ aggiungendo o sottraendo un elemento raddoppia o dimezza le cardinalità

Sia $S \neq \emptyset$ e $a \in S$ possiamo definire le seguenti applicazioni:

$$A = \{x \in P(S) \mid a \in x\} = P(S) \setminus B$$

$$B = \{x \in P(S) \mid a \notin x\} = P(S \setminus \{a\})$$

Sappiamo quindi che $A \cap B = \emptyset$ perché sono insiemi disgiunti quindi $A \cup B = P(S)$ e sono insiemi equipotenti perché:

$$\alpha : x \in A \longmapsto x \setminus \{a\} \in B$$

$$\beta : x \in B \longmapsto x \cup \{a\} \in A$$

Sono applicazioni biettive e inverse tra di loro.
Dimostrazione che $\beta_o\alpha = id_A$ e $\alpha_o\beta = id_B$:

$$\forall x \in A\ (\beta_o\alpha)(x) = \beta(\alpha(x)) = \beta(x \setminus \{a\}) = (x \setminus \{a\}) \cup \{a\} = x$$

$$\forall y \in B\ (\alpha_o\beta)(y) = \alpha(\beta(y)) = \alpha(y \cup \{a\}) = (y \cup \{a\}) \setminus \{a\} = y$$

Dimostrato che $|A| = |B|$, sono insiemi disgiunti e S è un'insieme finito, allora possiamo dire che $|P(S)| = |A| + |B| = 2|B| = 2|P(S \setminus \{a\})|$

Teorema - Formula ricorsiva del Coefficiente Binomiale

Sia $S \neq \emptyset$ perché $a \in S$, definiamo poi la cardinalità $|S| = n + 1$ e $|S \setminus \{a\}| = n$, sia $\forall k \in \mathbb{N}$.

Definiamo i seguenti insiemi:

$$A_k = A \cap P_k(S) = \{x \in P_k(S) \mid a \in x\} = P_k(S) \setminus B_k$$

$$B_k = B \cap P_k(S) = \{x \in P_k(S) \mid a \notin x\} = P_k(S \setminus \{a\})$$

$$A_{k+1} = A \cap P_{k+1}(S) = \{x \in P_{k+1}(S) \mid a \in x\}$$

Definite le applicazioni:

$$\alpha : x \in A_{k+1} \longmapsto x \setminus \{a\} \in B_k$$

$$\beta : x \in B_k \longmapsto x \cup \{a\} \in A_{k+1}$$

Se uso l'applicazione $\overrightarrow{\beta}(B_k) = A_{k+1}$ quindi posso dire che sono insiemi equipotenti $|B_k| = |A_{k+1}| = \binom{n}{k}$.
Perché esiste un'applicazione biettiva che $\beta_o\alpha = id_{A_{k+1}}$ e $\alpha_o\beta = id_{B_k}$:

$$(\beta_o\alpha)(A_{k+1}) = \beta(\alpha(A_{k+1})) = \beta(B_k) = A_{k+1}$$

$$(\alpha_o\beta)(B_k) = \alpha(\beta(B_k)) = \alpha(A_{k+1}) = B_k$$

Dimostrazione quindi essendo A_k e B_k insiemi disgiunti abbiamo che $P_k(S) = A_k \cup B_k$ e di conseguenza:

- La cardinalità di $P_k(S)$ viene calcolata come $|P_k(S)| = |A_k| + |B_k|$
- La cardinalità di $P_{k+1}(S)$ viene calcolata come $|P_{k+1}(S)| = |A_{k+1}| + |B_{k+1}|$

Ma sappiamo che $|P_{k+1}(S)| = |A_{k+1}| + |B_{k+1}|$ espresso come coefficiente binomiale $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$

Teorema - Calcolare gli elementi di $P(S)$

$\forall S\ \forall n \in \mathbb{N}$ sia $\varphi(n) : (|S| = n) \Rightarrow (|P(S)| = 2^n)$.

Applichiamo il principio di induzione:

- Base induttiva: $\varphi(0) : (|S| = 0) \Rightarrow (|P(S)| = 1)$
- Passo induttivo: $\forall n \in \mathbb{N}\ \varphi(n+1) : (|S| = n+1) \Rightarrow (|P(S)| = 2^{n+1})$

Dimostrazione riscriviamo quindi $\varphi(n+1)$ come $\varphi(n) + (n+1)$ e dimostriamo che questa sia vera.
(Sappiamo che $|P(S)| = 2|P(S \setminus \{a\}|$ e che $|S \setminus \{a\})| = n - 1$ essendo $S \neq \emptyset \wedge \exists a \in S$):

$$|P(S)| = 2^{n+1} \Rightarrow 2|P(S \setminus \{a\}| = 2 \cdot 2^n = 2^{n+1}$$

Teorema - Formula chiusa dei Coefficienti Binomiali

Sia $\varphi(n) : \forall k \in \mathbb{N}(k \leq n) \Rightarrow (\binom{n}{k} = \frac{n!}{k!(n-k)!})$ la formula per il calcolo del coefficiente binomiale e applichiamo il principio di induzione:

- Base induttiva: $\varphi(0) : \forall k \in \mathbb{N}(k \leq 0) \Rightarrow (\binom{0}{0} = \frac{0!}{0!(0-0)!} = \frac{0!}{0!} = \frac{1}{1} = 1)$
- Passo induttivo: $\varphi(n) : \forall k \in \mathbb{N}(k \leq n+1) \Rightarrow \left(\binom{n+1}{k} = \frac{(n+1)!}{k!((n+1)-k)!}\right)$

Dimostrazione riscriviamo quindi $\varphi(n+1)$ come $\varphi(n)+(n+1)$ e dimostriamo che questa sia vera (usando la formula ricorsiva):

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(k-1)!(n-(k-1))!} + \frac{n!}{k!(n-k)!} = \frac{n!}{(k-1)!(n-k)!}\left(\frac{1}{n-k+1} + \frac{1}{k}\right) = \frac{n!}{(k-1)!(n-k)!} \cdot \frac{n+1}{(n-k+1)k} = \frac{(n+1)!}{k!(n-k+1)!}$$

Da questa dimostrazione possiamo anche ricavare che $\binom{0}{0} = \binom{n}{n} = 1$.

Formula del binomio Newtown

Definizione - Formula del binomio di Newtown

Siano a e b due elementi di una struttura commutativa, allora:

$$\forall n \in \mathbb{N}\ (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Notiamo che $(a+b)^2 = a^2+ab+ba+b^2$ e per la commutatività possiamo unire $ab+ba$ in $2ab$ e ottenere $a^2+2ab+b^2$

Partizione e Classi di Equivalenza

Definizione - Partizione

Sia A un'insieme, definiamo $F \in Partz(A)$ se:

- $F \subseteq P(A) \setminus \emptyset$
- $\forall x \in A(\exists! b \in F(x \in B))$

Allo stesso modo è equivalente la seguente definizione:

- $A = \bigcup F$
- $\emptyset \notin F$
- $\forall b, c \in F((b \not\subseteq c) \Rightarrow (b \cap c = \emptyset))$

Quindi una partizione è "spezzettare un'insieme in tante parti non vuote, dette blocchi, disgiunte tra loro".

Partizioni banali: le partizioni banali di A sono: $A, P_1(A)$.

Proiezione di F su A (π_F): ovvero l'applicazione suriettiva $x \in A \longmapsto$ "l'unico $b \in F$ tale che $x \in b$" $\in F$

Esempio - Partizioni

Se $A = \emptyset$ allora le partizioni di A sono:

- $Partz(\emptyset) = \{\emptyset\}$

Se $|A| = 1$ allora le partizioni di A sono:

- $Partz(A) = \{\{A\}\} = P_1(A)$

Se $A = \{1, 2\}$ allora le partizioni di A sono:

- $Partz(A) = \{P_1(A), \{A\}\}$

Se $A = \{1, 2, 3\}$ allora le partizioni di A sono:

- $Partz(A) = \{P_1(A), \{A\}, \{\{\{1\}, \{2, 3\}\}, \{\{2\}, \{1, 3\}\}, \{\{3\}, \{1, 2\}\}\}$

Domanda - Se A è finito, posso ricavare la sua cardinalità da una partizione?

Sia $F \in Partz(A)$ con A finito, la somma delle cardinalità dei blocchi della partizione saranno uguali alla cardinalità di A, ovvero:

$$|A| = \sum_{b \in F} |b|$$

Classi di equivalenza

Definizione - Classi di equivalenza

Preso la relazione $\rho \in Eq(A)$ possiamo definire una classe di equivalenza come $\forall x \in A\ [x]_\rho = \{y \in A \mid y \rho x\} \subseteq A$, ovvero l'insieme di tutti gli elementi in relazione con x, sappiamo per certo che:

- $\forall x \in A (x \in [x]_\rho)$ quindi $[x]_\rho \neq \emptyset$
- $\forall x, y \in A (x \rho y \Leftrightarrow y \in [x]_\rho \Leftrightarrow y \rho x \Leftrightarrow x \in [y]_\rho \Leftrightarrow [x]_\rho = [y]_\rho)$

Domanda - In che altro modo posso rappresentare una classe di equivalenza?

Osservo la definizione di classe di equivalenza e tramite una serie di passaggi logici posso dedurre che la classe di equivalenza sia l'anti-immagine del singleton dell'immagine di x, ovvero:

$$\forall x \in A ([x]_\sim = \{y \in A \mid y \sim x\} = \{y \in A \mid f(y) = f(x)\} = \overleftarrow{f}(\{f(x)\})$$

Esempio - Classe di equivalenza

Data la funzione: $f : x \in \mathbb{Z} \longmapsto x^2 \in \mathbb{N}$

Nucleo $\sim$: $\forall x, y \in \mathbb{Z} (x \sim y \Leftrightarrow x^2 = y^2)$

Classe di equivalenza: $[3]_\sim = \overleftarrow{f}(\{9\}) = \{3, -3\}$

Teorema - Due elementi hanno la stessa classe di equivalenza se sono in relazione di equivalenza

Presa la relazione $\rho \in Eq(a)$ allora so per certo che $x \rho y \Leftrightarrow y \rho x \Leftrightarrow [x]_\rho = [y]_\rho$, questo perché:

1. Se $x \in [x]_\rho$ e $x \rho y$ allora $x \in [y]_\rho$
2. $\forall z \in [x]_\rho$ so che $z \rho x$ ma anche che $x \rho y$ quindi per la proprietà transitiva $(z \rho x \wedge x \rho y) \Rightarrow (z \rho y)$ e allora $[x]_\rho \subseteq [y]_\rho$
3. Inoltre so che per la proprietà simmetrica $y \rho x$ ma allora $[y]_\rho \subseteq [x]_\rho$

Concludo sapendo che $[x]_\rho = [y]_\rho$

Definizione - Insieme quoziente

Viene chiamato insieme quoziente di A rispetto a ρ l'insieme $\frac{A}{\rho} = \{[x]_\rho \mid x \in A\}$, ovvero l'insieme di tutte le classi di equivalenza, per le proprietà delle classi di equivalenza sappiamo che:

- $\forall x \in A\ [x]_\rho$ è l'unico elemento di $\frac{A}{\rho}$ a cui x appartiene
- $\frac{A}{\rho} \in Partz(A)$

Teorema - Fondamentale su partizioni e relazioni di equivalenza

Sia A un'insieme e $\rho \in Eq(A)$ allora posso formare l'applicazione biettiva:

$$\rho \in Eq(A) \longmapsto \frac{A}{\rho} \in Partz(A)$$

Dimostrazione: se f è biettiva allora:

- **Se f è iniettiva**: $\forall \rho, \sigma \in Eq(A)$ supponiamo che $f(\rho) = f(\sigma) \Rightarrow \frac{A}{\rho} = \frac{A}{\sigma}$

  So che $\forall x \in A\ [x]_\rho$ è l'unico elemento di $\frac{A}{\rho}$ a cui x può appartenere, quindi $\forall x, y \in A$ so che $x \rho y \Leftrightarrow y \in [x]_\rho \Leftrightarrow y \in [x]_\sigma \Leftrightarrow x \sigma y$ dal quale deduco che $\rho = \sigma$

- **Se f è suriettiva**: $\forall F \in Partz(A)$ abbiamo l'applicazione suriettiva $\pi_F : A \to F$.

  Prendiamo il nucleo di equivalenza di π_F, quindi $\sim \in Eq(A)$, sappiamo che $\forall x, y \in A (x \sim y \Leftrightarrow \pi_F(x) = \pi_F(y) \Leftrightarrow y \in \pi_F(x))$ dal quale deduciamo che $[x]_\sim = \pi_F(x)$.

  Concludiamo che $\frac{A}{\sim} = \{[x]_\rho \mid x \in A\} = \{\pi_F(x) \mid x \in A\} = im\ \pi_F = F$.

Nota - Prendere sempre il nucleo di equivalenza

Prendere il nucleo di equivalenza conviene perché non va dimostrato che esiste!

Domanda - Come si contano le relazioni di equivalenza?

Basta contare il numero di partizioni che ha un'insieme perché abbiamo dimostrato che esiste un'applicazione biettiva da $Eq(A)$ a $Partz(A)$, quindi i due insiemi sono equipotenti.

Esempio - Contiamo le relazioni di equivalenza di un insieme

Dato l'insieme $A = \{n \in \mathbb{N} \mid n < 8\}$, trovare tutte le relazioni di equivalenza tali che $1 \in [3]_\rho, 2 \notin [4]_\rho, \{1, 5, 6, 7\} \in [4]_\rho$.

Sappiamo che sono in relazione fra loro $\{1, 3, 4, 5, 6, 7\} \subseteq b_1$, quindi chiedo le partizioni tali che $2 \notin b_1$, ed ottengo le seguenti partizioni:

- $0, 2 | 1, 3, 4, 5, 6, 7$
- $0 | 2 | 1, 3, 4, 5, 6, 7$
- $2 | 0, 1, 3, 4, 5, 6, 7$

Quindi il numero di relazioni di equivalenza sono esattamente 3.

Definizione - Operazione quoziente

$\forall S$ definiamo la struttura $(S, *)$ e $\sim \in Eq(S)$ con la proprietà $\forall a, b\ \sim: a\ \sim\ b \Leftrightarrow (a = b = 0 \vee ab > 0)$, chiamiamo l'operazione quoziente l'operazione definita in questo modo:

$$\overline{*} : \frac{S}{\sim} \times \frac{S}{\sim} \to \frac{S}{\sim}$$

Questa operazione non è sempre ben definita, infatti per esserlo deve rispettare questa definizione: $\forall a, b, a', b'\ (a\ \sim\ a' \wedge b\ \sim\ b') \Rightarrow (a * b\ \sim\ a' * b')$, quando succede si dice:

- La relazione $\sim$ e l'operazione $*$ sono compatibili
- La relazione $\sim$ è una congurenza della struttura quando è compatibile con tutte le operazioni della struttura.

Definizione - Proiezione canonica

Sia A un'insieme e $\rho \in Eq(A)$, l'applicazione $\pi_\rho : x \in A \longmapsto [x]_\rho \in \frac{A}{\rho}$ è detta proiezione canonica perché coincide col suo nucleo di equivalenza:

$$\forall x, y \in A(x \rho y \Leftrightarrow [x]_\rho = [y]_\rho \Leftrightarrow \pi_\rho(x) = \pi_\rho(y))$$

Da questo ricaviamo che ogni relazione di equivalenza è il nucleo di equivalenza della sua proiezione canonica.

Nota - La proiezione canonica

La proiezione canonica $\pi_\sim : a \in S \longmapsto [a]_\sim \in \frac{S}{\sim}$ è un omomorfismo suriettivo da $(S, *)$ a $(\frac{S}{\sim}, \overline{*})$, quindi conserva il tipo di struttura algebrica.

Esempio - Operazioni quoziente

Sia la struttura $(S, *) = (\mathbb{Z}, \cdot)$ e sia $\frac{\mathbb{Z}}{\sim} = \{\mathbb{Z} \setminus \mathbb{N}, \{0\}, \mathbb{N}^*\}$, allora l'operazione è ben definita.

Sia la struttura $(S, *) = (\mathbb{Z}, +)$ e sia $\frac{\mathbb{Z}}{\sim} = \{\mathbb{Z} \setminus \mathbb{N}, \{0\}, \mathbb{N}^*\}$, allora l'operazione non è ben definita.

Teorema - Compatibilità

Sia $(S, *)$ e $\sim \in Eq(S)$ allora possiamo dire che:

- $*$ è compatibile a sinistra rispetto a $\sim \Leftrightarrow \forall a, b, b' \ (b \sim b') \Rightarrow (a * b \sim a * b')$
- $*$ è compatibile a destra rispetto a $\sim \Leftrightarrow \forall a, b, b' \ (b \sim b') \Rightarrow (b * a \sim b' * a)$
- $*$ è compatibile rispetto a $\sim \Leftrightarrow \forall a, b, a', b' \ (a \sim a' \ \wedge \ b \sim b') \Rightarrow (a * b \sim a' * b')$

Dimostrazione

$$(a \sim a' \ \wedge \ b \sim b') \Rightarrow ((a * b \ \sim \ a * b') \wedge (a * b' \ \sim \ a' * b')) \Rightarrow (a * b \ \sim \ a' * b')$$

Omomorfismo per insiemi

Teorema - Omomorfismo per insiemi

$\forall A, B$ e $\forall f \in Map(A, B)$, inoltre sia $\sim$ il nucleo di equivalenza di f allora:

$$\begin{array}{ccc} \frac{A}{\sim} & \xrightarrow{h'} & im\ f \\ {\scriptstyle \pi_A}\uparrow & & \downarrow{\scriptstyle \iota} \\ A & \xrightarrow{f} & B \end{array}$$

So che l'applicazione $h : y \in im\ f \longmapsto \overleftarrow{f}(\{y\}) \in \frac{A}{\sim}$ è ben definita perché:

- $\forall x \in A([x]_\sim = \overleftarrow{f}(\{f(x)\})$
- $\forall y \in im\ f(\exists x \in A(y = f(x))$

Allora so che $\overleftarrow{f}(\{y\}) = \overleftarrow{f}(\{f(x)\}) = [x]_\sim \in \frac{A}{\sim}$.

Dimostrazione della biettività di $h : im\ f \to \frac{A}{\sim}$ osservando che:

- **h è suriettiva** perché $\forall c \in \frac{A}{\sim}(\exists x \in A(c = [x]_\sim))$, allora posso dire che $c = \overleftarrow{f}(\{f(x)\})$ ma sappiamo che $f(x) \in im\ f$ e quindi $c = h(f(x))$
- **h è iniettiva** assumiamo che $\forall y, z \in im\ f (h(y) = h(z) \Leftrightarrow \overleftarrow{f}(\{z\}) = \overleftarrow{f}(\{y\})$, prendiamo $x \in \overleftarrow{f}(\{y\})$ vuol dire che $f(x) = y$ ma per l'assunzione di prima sappiamo anche che $x \in \overleftarrow{f}(\{z\})$ ma questo vuol dire che $f(x) = z$, ma quindi $y = f(x) = z$.

Quindi essendo h biettiva ha una singola inversa che è $h' : [x]_\sim \in \frac{A}{\sim} \longmapsto f(x) \in im\ f$

Nota - Ogni applicazione arbitraria può essere scomposta come iniettiva composta una suriettiva

Presa l'applicazione $f : A \to B$ e sia $\sim$ il nucleo di equivalenza, osservando il diagramma commutativo:

$$\begin{array}{ccc} \frac{A}{\sim} & \xrightarrow{h} & im\ f \\ {\scriptstyle \pi_A}\uparrow & & \downarrow{\scriptstyle \iota} \\ A & \xrightarrow{f} & B \end{array}$$

Possiamo ricavare che $f = \iota_o h_o \pi_\sim$ ovvero abbiamo composto $\iota_o h$ che è iniettiva (perché essendo h biettiva, la composta di una biettiva ed una iniettiva) e $\pi_\sim$ è suriettiva.

Aritmetica Modulare

Elementi associati

Definizione - Elementi associati

Due elementi sono detti associati in $(S, \cdot)$ se si dividono reciprocamente, ovvero:

$$\forall a, b \in S\ (a \underset{(S,\cdot)}{\sim} b) \Rightarrow (a \underset{(S,\cdot)}{|} b \ \wedge\ b \underset{(S,\cdot)}{|} a)$$

Sappiamo che $\underset{(S,\cdot)}{\sim} \in Eq(S)$ perché:

- **Riflessiva**: $(a \underset{(S,\cdot)}{\sim} a = a \underset{(S,\cdot)}{\sim} a)$
- **Simmetrica**: $(a \underset{(S,\cdot)}{\sim} b = b \underset{(S,\cdot)}{\sim} a)$
- **Transitiva**: $(a \underset{(S,\cdot)}{\sim} b \ \wedge\ b \underset{(S,\cdot)}{\sim} c) \Rightarrow (a \underset{(S,\cdot)}{\sim} c)$

Nota - Due elementi associati si comportano alla stessa maniera rispetto alla divisibilità

Ovvero $\forall a, b, a', b' \in S\ (a \underset{(S,\cdot)}{\sim} a' \ \wedge\ b \underset{(S,\cdot)}{\sim} b') \Rightarrow (a \underset{(S,\cdot)}{|} b \Leftrightarrow a' \underset{(S,\cdot)}{|} b')$, quindi sono equivalenti le tre condizioni:

1. $x \underset{(S,\cdot)}{\sim} y$
2. $Div(x) = Div(y)$
3. $xS = yS$

Dove $Div(x) = \{a \in S \mid a \underset{(S,\cdot)}{|} x\}$ è l'insieme dei divisori di x e $xS = \{a \in S \mid x \underset{(S,\cdot)}{|} a\}$ è l'insieme dei multipli di x.

Esempio - Elementi associati

$(1 \underset{(\mathbb{Z},\cdot)}{\sim} -1) \Rightarrow (1 \underset{(\mathbb{Z},\cdot)}{\mid} -1 \land -1 \underset{(\mathbb{Z},\cdot)}{\mid} 1)$

Divisibilità

Definizione - Divisiblità

Sia $(S,*)$ un semi-gruppo commutativo allora $|_{(S,*)} \in Rel(S)$ secondo la seguente definizione:

$$\forall a,b \in S \; a \underset{(S,*)}{\mid} b \Leftrightarrow \exists c \in S(b = ac)$$

!ATTENZIONE! divisibilità non vuol dire divisione!

Questa è la relazione di divisibilità in $(S,*)$ e viene letta come "a divide b" oppure "b è multiplo di a". inoltre ha le seguenti proprietà:

- **Transitiva**: $\forall x,y,z \in S((x \underset{(S,*)}{\mid} y \land y \underset{(S,*)}{\mid} z) \Rightarrow (\exists c,d \in S(y = xc \land z = yd)))$

  Posso quindi riscrivere z come multiplo di x più un elemento: $(z = (xc)d) \Rightarrow (z = x(cd))$

Sia $(S,*,t)$ un monoide allora valgono che queste ulteriori proprietà:

- **Riflessiva** quando è un monoide: $\forall a \in S(a \underset{(S,*,t)}{\mid} a) \Leftrightarrow a = a \cdot t$
- **Gli invertibili dividono sempre**: $\forall u \in U(S) \; \forall a \in S(u \underset{(S,*,t)}{\mid} a \Leftrightarrow \exists c \in S(a = u \cdot c))$

  Quindi sfruttando la definizione posso dire che $a = u(u^{-1} \cdot a) \Rightarrow a = (u \cdot u^{-1})a \Rightarrow a = t \cdot a \Rightarrow a = a$

Divisori banali: $\forall a \in (S,*,t)$ ha sempre come divisori i suoi associati e gli invertibili.

Sia $(S,*,t,')$ un gruppo abeliano allora otteniamo la seguente proprietà:

- **Relazione universale**: $\underset{(S,*,t,')}{\mid}$ è la relazione universale in S.

Sia $(R,+,\cdot)$ un anello commutativo sappiamo che:

- **Combinazione lineare**: $\forall a,b,c \in R$ e sappiamo che $a \underset{(R,\cdot)}{\mid} b \land a \underset{(R,\cdot)}{\mid} c$ allora possiamo dire $\exists s,d \in R(a \underset{(R,\cdot)}{\mid} bs + cd)$

  Usando la definizione abbiamo che $\exists \beta,\gamma \in R(b = a\beta \land c = a\gamma) \Rightarrow (bs + cd = a\beta s + a\gamma d = a(\beta s + \gamma d))$

Esempio - Divisibilità

$2 \underset{(\mathbb{Z},\cdot)}{\mid} 6$ attenzione però $6 \underset{(\mathbb{Z},\cdot)}{\nmid} 2$ ovvero per definizione $\exists c \in \mathbb{Z}(6 = 2 \cdot c)$

$\{1,2\} \underset{(P(\mathbb{N}),\cap)}{\mid} \emptyset$ ovvero per definizione $\exists c \in P(\mathbb{N})(\emptyset = \{1,2\} \cap c)$

Esempio - Divisori banali

In $(\mathbb{Z},\cdot)$ $\forall a \in \mathbb{Z}$ i divisori banali di a sono $a, a^{-1}, 1, -1$

In $(\mathbb{N},\cdot)$ $\forall a \in \mathbb{N}$ i divisori banali di a sono $a, 1$

Nota - 0 divide 0

Nel "concetto di divisione" non esiste la divisione $\frac{0}{0}$ ma invece nel "concetto di divisibilità" esiste $0 \underset{(\mathbb{Z},\cdot)}{\mid} 0$ perché per definizione $\exists c \in \mathbb{Z}(0 = 0 \cdot c)$.

Per provare ulteriormente questo concetto abbiamo che $\forall a \in \mathbb{Z}(a \underset{(\mathbb{Z},\cdot)}{\mid} 0)$ perché usando ancora una volta la definizione abbiamo che $\exists c \in \mathbb{Z}(0 = a \cdot c)$

Nota - La divisibilità negli anelli si applica solo alla moltiplicazione

In un anello la divisibilità rispetto l'operazione di addizione è la relazione universale perché trattiamo sempre un gruppo, quindi se ne discute soltanto per la moltiplicazione.

Teorema - Gli invertibili sono sempre associati

Sia $(M,\cdot,t)$ un monoide commutativo e $a \in M$ allora valgono le seguenti affermazioni:

1. $\forall u \in U(M)(a \sim au)$ sono associati, ovvero $a \underset{(M,\cdot,t)}{\mid} au$
2. Se a è cancellabile allora $\forall b \in M(a \sim b) \Leftrightarrow \exists u \in U(M)(b = au)$ (oppure possiamo dire che $[a]_{\sim} = aU(M)$)

Dimostrazione

- " $\Leftarrow$ " Sappiamo essere vera perché un multiplo di a è sempre associato ad a, ovvero $\exists v \in U(M)(a = (au)v) = (a = a(uv)) = (a = a)$
- " $\Rightarrow$ " Se $a \sim b$ allora $a \underset{(M,\cdot,t)}{\mid} b \ \wedge \ b \underset{(M,\cdot,t)}{\mid} a$, quindi abbiamo che:
  - $(a \underset{(M,\cdot,t)}{\mid} b) \Rightarrow (\exists u \in U(M)(b = au))$
  - $(b \underset{(M,\cdot,t)}{\mid} a) \Rightarrow (\exists v \in U(M)(a = bv))$

  Tramite una serie di uguaglianze ci riconduciamo a $(a = bv) = (a = (au)v) = (a = a(uv))$, ma noi sappiamo anche che $a = at$ quindi $a = at = a(uv)$, essendo però a cancellabile otteniamo che $t = uv$ e per la proprietà commutativa del monoide abbiamo che $v = u^{-1}$.

Esempio - Invertibili associati

In $(\mathbb{Z},\cdot)$ $\forall m \in \mathbb{Z} \setminus \{0\}$ gli associati sono 1 e -1

In $(\mathbb{N}^*,\cdot)$ $\forall n \in \mathbb{N}^*$ l'unico associato è 1

Teorema - Divisione con resto

$\forall a, b \in \mathbb{Z}(b \neq 0) \Rightarrow (\exists!(q,r) \in \mathbb{Z} \times \mathbb{N}(a = bq + r \ \wedge \ 0 \leq r < |b|))$

Dimostrazione

1. **Esistenza**: sia $r = a \mod b$, quindi $0 \leq r < |b|$ e inoltre $r \underset{b}{\equiv} a$, ma questo significa che $\exists k \in \mathbb{Z}(a = r + kb)$ ponendo $q = k$ (a si ottiene da r sommando k volte b)

2. **Unicità**: oltre alla coppia (q, r) poniamo l'esistenza della coppia $(q', r') \in \mathbb{Z} \times \mathbb{N}(a = bq' + r' \ \wedge \ 0 \leq r' < |b|)$ allora:
   - $r' \underset{b}{\equiv} a$ quindi $r' = a \mod b = r$ quindi $r' = r$
   - Deduciamo quindi anche che $qb + r = a = q'b + r$ ma segue che $q'b = qb$ ma essendo b cancellabile perché $b \neq 0$ allora $q' = q$

Divisori propri

Definizione - Divisori propri

Sono detti divisori propri i divisori non associati ad a, attenzione ai seguenti casi:

- $\forall a \in \mathbb{P}$ sappiamo che i divisori propri di a sono $\{1, -1\}$
- $\forall u \in U(M)$ sappiamo che i divisori propri di u non esistono

Esempio - Divisori propri

In $(\mathbb{Z}, \cdot)$ abbiamo che i divisori propri di 15 sono $\{1, -1, 3, -3, 5, -5\}$ (mancano 15 e -15 perché sono associati)

Elementi irriducibili

Definizione - Irriducibile

Sia $(M, \cdot, t)$ un monoide commutativo, allora a si dice irriducibile quando:

- $a \notin U(M)$
- a ha solo divisori banali

Domanda - Ma gli elementi irriducibili sono numeri primi?

Questa nozione coincide con quella di numero primo in $\mathbb{N}^*, \mathbb{N}, \mathbb{Z}$ quindi per questo corso li chiameremo numeri primi.

Divisori comuni

Definizione - Divisori comuni

Sia $(M, \cdot, t)$ un monoide commutativo con $S \subseteq M$ allora abbiamo che i divisori comuni sono:

$$Div(S) = \{y \in M \mid \forall x \in S(y \underset{(M,\cdot,t)}{|} x)\}$$

In modo equivalente, se $S \neq \emptyset$, abbiamo che $Div(S) = \bigcap_{x \in S} Div(x)$

Esempio - Divisori comuni

Sia $M = (\mathbb{Z}, \cdot, 1)$ e la sua parte $S = \{16, 20\}$ allora ricaviamo che $Div(S) = \{1, -1, 2, -2, 4, -4\}$

MCD e MCM

Definizione - Massimo Comune Divisore

Sia $(M, *, t)$ un monoide commutativa e $S \subseteq M$ allora se $\forall d \in M$ diciamo che d è un MCD di S in M quando:

- $d \in Div(S)$
- $\forall x \in Div(S)\ (x \underset{(\mathbb{Z},\cdot)}{\mid} d)$

Esempio - MCD

Sia $M = (\mathbb{Z}, \cdot, 1)$ e la sua parte $S = \{16, 20\}$ allora ricaviamo che $Div(S) = \{1, -1, 2, -2, 4, -4\}$ e abbiamo come MCD 4 oppure -4

Definizione - MCM

Sia $(M, *, t)$ un monoide commutativa e $S \subseteq M$ allora se $\forall d \in M$ diciamo che d è un MCM di S in M quando:

- $d \in SM$
- $\forall x \in SM\ (d \underset{(\mathbb{Z},\cdot)}{\mid} x)$

Esempio - MCM

Sia $M = (\mathbb{Z}, \cdot, 1)$ e la sua parte $S = \{16, 20\}$ allora ricaviamo che $SM = \{0, 16, -16, 20, -20, 32, -32, ...\}$ e abbiamo come MCM 80 oppure -80

Nota - Qualsiasi nozione definita con la divisione vale anche per gli associati

Sia d un $MCD(X)$, allora sappiamo per certo che gli $MCD(X)$ sono tutti e soli gli associati a d in M perché:

- Sia h un $MCD(X)$ allora sappiamo che h è un divisore comune a tutti gli elementi di X, però ogni divisore comune di X divide anche d, quindi sono associati
- Sia invece h associato a d, quindi con gli stessi multipli e divisori di d, allora anche h divide tutti gli elementi di X

Teorema - Algoritmo di Euclide

Sia $a, b \in \mathbb{Z}$ possiamo dire che:

1. Se $b \underset{\mathbb{Z}}{\mid} a$ allora sappiamo che $Div(\{a, b\}) = Div(b)$ perché tutti i numeri che dividono b dividono anche a, quindi b è un MCD
2. Siano $q, r \in \mathbb{Z}$ con la proprietà che $a = bq + r$ allora sappiamo che $Div(\{a, b\}) = Div(\{b, r\})$, questo perché:

$$\exists c \in \mathbb{Z}(c \underset{\mathbb{Z}}{\mid} b \ \wedge\ c \underset{\mathbb{Z}}{\mid} r) \Rightarrow (c \underset{\mathbb{Z}}{\mid} bq + r)$$

Questa combinazione lineare è uguale ad a, similmente ricaviamo quella per r

$$(c \underset{\mathbb{Z}}{\mid} b \ \wedge\ c \underset{\mathbb{Z}}{\mid} a) \Rightarrow (c \underset{\mathbb{Z}}{\mid} a - (bq))$$

Da questo ricaviamo che l'MCD non cambia e quindi nemmeno i $Div(\{a, b\})$ ovvero $\forall d \in \mathbb{Z}$ sappiamo che d è un $MCD(\{a, b\}) \Leftrightarrow d$ è un $MCD(\{b, r\})$

Per eseguire l'algoritmo vanno visti in maniera ricorsiva i seguenti passi:

- Se $a \mid b \ \wedge \ b = 0$ allora a è l'MCD
- Se $b \neq 0$ allora procedo con la divisione aritmetica e riscrivo $a = bq + r$ (con $0 \leq r < |b|$)
- Se $r \neq 0$ allora riscrivo la divisione aritmetica $b = rq + r_1$
- Se $r = 0$ allora b è l'MCD che cercavamo

Domanda - Troveremo mai un resto uguale a 0?

La risposta è sì, perché $|b| > r_1 > r_2 > .... > r_n \geq 0$ ed essendo la divisione aritmentica nei numeri naturali per il principio di buon ordinamento hanno un minimo (ovvero 0) che prima o poi raggiungeremo essendo la successione strettamente decrescente.

Esempio - Applicazione dell'Algoritmo di Euclide

Se stiamo effettuando la divisione aritmetica tra 35 e 9 allora applicando l'algoritmo otteniamo

- $35 = \underline{9} \cdot 3 + \underline{8}$ il resto non è uguale a 0, procediamo con la prima iterazione
- $\underline{9} = \underline{8} \cdot 1 + \underline{1}$ il resto non è uguale a 0, effettuiamo un'altra iterazione
- $\underline{8} = \underline{1} \cdot 8 + 0$ ci fermiamo avendo ottenuto il resto pari a 0 e posso direttamente dire che 1 è l'MCD che cercavo

Notare che ci si può fermare anche al primo resto non nullo, ovvero l'MCD

Teorema - Bézout

Si tratta di un'estensione dell'algoritmo di Euclide, infatti dato d come $MCD(\{a, b\})$ (cioè l'ultimo resto non nullo che indichiamo con r_t) questo teorema ci dice che possiamo riscrivere d come combinazione lineare dei resti delle divisioni precedenti:

$$d = r_t = (1)r_{t-2} + (-q_t)r_{t-1}$$

Possiamo poi sostituire r_{t-1} con la combinazione lineare dei resti precedenti fino a risalire alla combinazione lineare di $d = bq + r$ e sostituendo infine r otteniamo $d = ua + vb$.

Quindi concludiamo che $\forall a, b \in \mathbb{Z}$ se d è un $MCD(\{a, b\})$ allora abbiamo che $\exists u, b \in \mathbb{Z}(d = ua + vb)$

Esempio - Bézout

L'$MCD(\{35, 9\}) = 1$ perché per l'algoritmo di euclide abbiamo:

- $35 = \underline{9} \cdot 3 + \underline{8}$
- $\underline{9} = \underline{8} \cdot 1 + 1$

Bèzout ci dice che possiamo riscrivere 1 come:

- $1 = (1)9 + (-1)8$
- $1 = (1)9 + (-1)(35 + (-3)9)$
- $1 = (-1)35 + (4)9$

L'$MCD(\{34, 26\}) = 2$ perché per l'algoritmo di euclide abbiamo:

- $34 = \underline{26} + \underline{8}$
- $\underline{26} = \underline{8} \cdot 3 + 2$

Bèzout ci dice che possiamo riscrivere 2 come:

- $2 = 26 + (-3)8$
- $2 = 26 + (-3)(34 + (-1)26)$
- $2 = (-3)34 + (4)26$

Teorema - Lemma di Euclide

Abbiamo che $\forall a, b, c \in \mathbb{Z}$ se $a \underset{(Z,\cdot)}{|} bc$ con a e b sono co-primi allora $a|c$

Dimostrazione secondo il teorema di Bézout abbiamo che $\exists u, v \in \mathbb{Z}(1 = ua + vb)$ ma moltiplicando tutto per c abbiamo che $c = acu + bcv$ quindi:

- ac è un multiplo di a
- bc è un multiplo di a (per ipotesi)
- c è una combinazione lineare di multipli di a quindi anche esso un multiplo di a

Nota - Numeri co-primi

Due numeri a e b sono detti co-primi se il loro $MCD(\{a, b\}) = 1$

Teorema - Fondamentale dell'Aritmetica

Sappiamo che nel monoide $(\mathbb{N}^*, \cdot)$ abbiamo che $\forall n \in \mathbb{N}^*$ se $n > 1$ allora $\exists k \in \mathbb{N}^*(\exists p_1, p_2, ..., p_k \in \mathbb{P}(n = p_1 \cdot p_2 \cdot .... \cdot p_k))$ e questa composizione è unica a meno dell'ordinamento.

Dimostrazione

- **Esistenza fattorizzazione** Se chiamiamo C l'insieme degli elementi in $\mathbb{N}^*$ non prodotti di primi, esso avrà un minimo che indichiamo con m, questo elemento essendo non primo ha sicuramente un divisore non banale che chiamiamo a per il quale $a \underset{(\mathbb{N}^*,\cdot)}{|} m$ e usando la definizione di divisibilità abbiamo che $\exists b \in \mathbb{N}^*(m = ab)$, però per la minimalità di m sappiamo che $1 < a < m \ \wedge \ 1 < b < m$ ma questo ci dice che a e b sono primi e quindi m è un prodotto di primi.
- **Unicità** Sia sempre C l'insieme degli elementi in $\mathbb{N}^*$ che abbiano prodotti di primi diversi, esso avrà un minimo che chiamiamo $n = p_1 \cdot p_2 \cdot ... \cdot p_k = q_1 \cdot q_2 \cdot ... \cdot q_l$ dove $\forall p, q \in \mathbb{P}$ con $p \neq q$, sappiamo quindi che $p_k \neq q_l$ quindi sono co-primi e per il lemma di euclide $p_k \underset{(\mathbb{N}^*,\cdot)}{|} (q_1 \cdot q_2 \cdot ... \cdot q_{l-1})$ ma iterando questo processo otteniamo che $p_k \underset{(\mathbb{N}^*,\cdot)}{|} 1$ ma questo è impossibile (per la definizione di divisibilità), allora possiamo dire che $\exists i \in \{1, 2, .., l\}(p_k = q_l)$ e assumiamo $i = l$ allora preso $\frac{n}{p_k} = p_1 \cdot p_2 \cdot ... \cdot p_{k-1} = q_1 \cdot q_2 \cdot ... \cdot q_{l-1}$ e otteniamo due possibili casi:
  - $\frac{n}{p_k} = 1 = p_k = q_l$
  - $\frac{n}{p_k} > 1$ allora basta ripetere il processo di prima

Se ci spostiamo nel monoide $(\mathbb{Z}, \cdot)$ sappiamo che $\forall n \in \mathbb{Z} \setminus \{0, 1, -1\}$ (ovvero $n \in \mathbb{Z}$ e $|n| > 1$) abbiamo due casi:

1. Se $n > 1$ abbiamo che sicuramente sarà prodotto di primi perché in $\mathbb{N}^*$

2. Se $n < 1$ invece sappiamo che l'esistenza è verificata perché p_k e $-p_k$ sono associati e l'unicità vale a meno della posizione e del segno di ogni fattore

Domanda - Come faccio a dire che vale l'unicità a meno della loro posizione?

Semplicemente basta usare le permutazioni, dicendo che se abbiamo $p_1 \cdot p_2 \cdot ... \cdot pk = q_1 \cdot q2 \cdot ... \cdot q_l$ e questi fattori sono irriducibili allora sappiamo che $k = l \ \wedge \ \exists \sigma \in Sym(\{1,2,...,k\})(\forall i \in \{1,2,...,k\}(p_i \sim q_{\sigma(i)}))$

Congurenza Modulo

Definizione - Congurenza Modulo

$\forall m \in \mathbb{Z}$ abbiamo l'operazione $\underset{m}{\equiv} \in Eq(\mathbb{Z})$ e viene letta come a e congruo b modulo m, definita come:

$$\forall a, b \in \mathbb{Z} \ a \underset{m}{\equiv} b \Leftrightarrow m \mid b - a \Leftrightarrow m \mid a - b$$

Viene letto come a e b sono congrui modulo m, inoltre l'operazione ha le seguenti proprietà:

- **Riflessiva**: $a \underset{m}{\equiv} a \Leftrightarrow m \mid a - a \Leftrightarrow m \mid 0$
- **Simmetrica**: $a \underset{m}{\equiv} b \Leftrightarrow b \underset{m}{\equiv} a$
- **Transitiva**: $(a \underset{m}{\equiv} b \ \wedge \ b \underset{m}{\equiv} c) \Rightarrow (c \underset{m}{\equiv} a) \Leftrightarrow (m \mid b - a \ \wedge \ m \mid c - b) \Rightarrow (m \mid (b-a) + (c-a) = m \mid c - a)$

Tieni a mente! le congruenze per modulo m sono le stesse per modulo $-m$, ovvero $\underset{m}{\equiv} = \underset{-m}{\equiv}$.

Nota - Notazione per la congruenza modulo

- Quoziente della congruenza modulo sarà indicato con $\mathbb{Z}_m = \frac{\mathbb{Z}}{\underset{m}{\equiv}}$
- Classe di equivalenza della congruenza modulo sarà indicata con $[a]_m = [a]_{\underset{m}{\equiv}}$

Teorema - Si tratta dell'unica congruenza nell'anello degli interi

La congurenza modulo m è l'unica compatibile con l'addizione nell'anello $(\mathbb{Z}, +, \cdot)$.

Dimostrazione (essendo questo anello commutativo possiamo verificarla soltanto a destra e sapere che vale anche a sinistra)

- $\underset{m}{\equiv}$ è compatibile con $+$ perché $\forall a, b, c \in \mathbb{Z}(a \underset{m}{\equiv} b) \Rightarrow (a + c \underset{m}{\equiv} b + c) \Leftrightarrow (m \underset{(\mathbb{Z},+)}{\mid} a - b) \Rightarrow (m \underset{(\mathbb{Z},+)}{\mid} (a+c) - (b + c)) = (m \underset{(\mathbb{Z},+)}{\mid} a - b)$
- $\underset{m}{\equiv}$ è compatibile con $\cdot$ perché $\forall a, b, c \in \mathbb{Z}(a \underset{m}{\equiv} b) \Rightarrow (ac \underset{m}{\equiv} bc) \Leftrightarrow (m \underset{(\mathbb{Z},\cdot)}{\mid} ab) \Rightarrow (m \underset{(\mathbb{Z},\cdot)}{\mid} ac - bc) = (m \underset{(\mathbb{Z},\cdot)}{\mid} (a - b)c)$

Allora $\mathbb{Z}_m$ è un anello unitario commutativo, inoltre $\pi_m : a \in \mathbb{Z} \longmapsto [a]_m \in \mathbb{Z}_m$ è un omomorfismo suriettivo di anelli unitari.

Esempio - Congruenza Modulo

$\forall a, b \in \mathbb{Z}$ osserviamo le congruenze modulo:

- $\underset{0}{\equiv} = id_{\mathbb{Z}}$ applicando la definizione $a \underset{0}{\equiv} b \Leftrightarrow 0 \underset{(Z,+)}{|} a - b \Leftrightarrow a = b$ perché 0 è multiplo solo di se stesso
- $\underset{1}{\equiv}$ = relazione universale, applicando la definizione $a \underset{1}{\equiv} b \Leftrightarrow 1 \underset{(Z,+)}{|} a - b$ è sempre vera perché 1 è multiplo di ogni numero
- $\underset{2}{\equiv}$ applicando la definizione $a \underset{2}{\equiv} b \Leftrightarrow 2 \underset{(Z,+)}{|} a - b \Leftrightarrow$ ovvero se a e b hanno la stessa parità

Con la congruenza modulo possiamo semplificare pure le operazioni ad esempio:

1. Prendiamo in esempio che l'orologio segni le ore 13:00 e vogliamo sapere che ora saranno tra $32+54$ ore, posso riscrivere la somma in modo equivalente con due numeri congrui modulo 24 a 32 e 54, quindi:
   (a) $32 \underset{24}{\equiv} 8$
   (b) $54 \underset{24}{\equiv} 6$

   Da qui ricavo la somma 8+6 che è del tutto equivalente alla somma 32+54, quindi saranno le ore 13+(8+6) = 27 (posso ancora reiterare lo stesso processo) $27 \underset{24}{\equiv} 3$ e quindi saranno le 03:00.
2. Prendiamo in esempio di svolgere un'operazione che richieda 32 ore e vada svolta 54 volte, per sapere l'orario nel quale terminerò posso sempre applicare il ragionamento fatto sopra, quindi $32 \cdot 54$ sarà congruo a $8 \cdot 4 = 48$ (reitero lo stesso processo) quindi ancora $48 \underset{24}{\equiv} 0$, concludo che terminerò alla stessa ora in qui ho cominciato.
3. Altro esempio, poniamo in esempio che oggi sia lunedì e vogliamo sapere tra 2^{37} giorni che giorno sarà, questo calcolo lo possiamo svolgere a mente perché lavorando con i giorni della settimana sto lavorando modulo 7, quindi osserviamo che:
   - $2^{37} = 2 \cdot 2^{36}$ ma sappiamo ache che $2^{36} = 2^3 \cdot 2^3 \cdot 2^3 \ldots$ per 12 volte
   - $2^3 = 8$ e lavorando modulo 7 sappiamo che $8 \underset{7}{\equiv} 1$ e quindi $2^{36} \underset{7}{\equiv} 1$

   Se abbiamo iniziato lunedì finiremo esattamente tra 2 giorni della settimana, ovvero mercoledì.

Nota - La congruenza modulo si usa per stabilire i criteri di disibilità

Definiamo un numero $n = "c_k + c_{k-1} + \ldots + c_1 + c_0" = \sum_{i=0}^{k} c_i \cdot 10^i$

Quindi il numero $537 = 100 \cdot 5 + 10 \cdot 3 + 7 \cdot 1$ secondo il sistema posizionale decimale, questa informazione ci aiuta a capire i criteri di divisibilità per un numero:

- **Criterio di divisibilità per 9**: sappiamo che $\forall i \in \mathbb{N}(10^i \underset{9}{\equiv} 1)$ e quindi la somma di un numero viene riscritta come $\sum_{i=0}^{k} c_i \cdot 1$ da dove ricaviamo che la somma delle cifre ci permettere di dire che $537 \underset{9}{\equiv} = 5+3+7 \underset{9}{\equiv} = 15 \underset{9}{\equiv} 6$
- **Criterio di divisibilità per 4**: sappiamo che $\forall i \in N^* \setminus \{1\}(10^i \underset{100}{\equiv} 0)$ (questo perché 4 divide 100 ed hanno lo stesso criterio di divisibilità) e quindi la somma di un numero viene riscritta come $(\sum_{i=2}^{k} c_i \cdot 0) + c_1 \cdot 10 + c_0 = c_1 \cdot 10 + c_0$ da dove ricaviamo che la somma delle ultime due cifre ci permettere di dire che $537 \underset{4}{\equiv} = 37 \underset{4}{\equiv} 1$
- **Criterio di divisibilità per 3**: essendo che 3 divide 9 hanno lo stesso criterio di divisibilità

- **Criterio di divisibilità per 2**: sappiamo che $\forall i \in \mathbb{N}^*(10^i \underset{2}{\equiv} 0)$ e quindi la somma di un numero viene riscritta come $(\sum_{i=1}^{k} c_i \cdot 0) + c_0 = c_0$ da dove ricaviamo che l'ultima cifra ci permettere di dire che $537 \underset{2}{\equiv} 1$

Definizione - Classe di equivalenza congruenza modulo

Siano $\forall m, a \in \mathbb{Z}$ allora possiamo descrivere la classe di equivalenza di a come:

$$[a]_{-m} = [a]_m = \{b \in \mathbb{Z} \mid a \underset{m}{\equiv} b\} = \{b \in Z \mid m \underset{(\mathbb{Z},+)}{|} a - b\} = \{b \in \mathbb{Z} \mid \exists k \in \mathbb{Z}(mk = a - b)\} = \{b \in \mathbb{Z} \mid b = a + mk\} = \{a + mk \mid k \in \mathbb{Z}\} = a + m\mathbb{Z}$$

L'insieme delle classi di equivalenza congruenza modulo ha cardinalità $\mathbb{Z}_m = |m|$, inoltre gli elementi sono $\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, ..., [m-1]_m\}$

Esempio - Classi di equivalenza congruenza modulo

$[3]_5 = 3 + 5\mathbb{Z} = \{3 + 5k \mid k \in \mathbb{Z}\} = \{...., -12, -7, -2, 3, 8, 13, 18, ...\}$

Teorema - L'insieme delle classi di equivalenza congruenza modulo non è vuoto

Sono sicuro che l'insieme delle classi di equivalenza congruenza modulo m non è vuoto perché $\forall a, m \in \mathbb{Z}(m \neq 0) \Rightarrow ([a]_m \cap \mathbb{N} \neq \emptyset)$ quindi posso dire che sicuramente trovo a stesso al suo interno.

Posso anche accertarmi che $\forall k \in \mathbb{Z}(a + mk \geq 0) \Leftrightarrow (mk \geq -a)$ ci sara un insieme di numeri naturali che per il principio di buon ordinamento dei naturali avrà un minimo che definiamo $\exists r = \min([a]_m \cap \mathbb{N}) := a \mod m$, che ha la proprietà di $0 \leq r < |m|$.

Dimostrazione sicuramente su r ho le seguenti informazioni:

- $r \underset{m}{\equiv} r - |m|$
- $r - |m| < r$
- $r - |m| \in [a]_m$

Quindi concludo che per la minimalità di r abbiamo che $r - |m| < 0 = r < |m|$ e quindi in $\mathbb{Z}_m = \{[0]_m, ..., [m-1]_m\}$.

Da questo posso anche dedurre che la cardinalità di $\mathbb{Z}_m = |m|$.

Dimostrazione $\forall i, j \in \mathbb{N}(i < j < |m|) \Rightarrow i \underset{m}{\not\equiv} j$ ma questo perché $0 < j - i \leq j < |m|$ e quindi $j - i$ non può essere un multiplo di m perché più piccolo.

Equazione diofantea

Definizione - Equazione diofantea

Un equazione diofantea è un'equazione di primo grado definita nell'anello degli interi, quindi non cerchiamo soluzioni in $\mathbb{R}$ ma ci concentriamo sulle soluzioni in $\mathbb{Z}$, ovvero

$$\forall c \in \mathbb{Z}(ax + by = c)$$

Quindi diciamo che c è una combinazione lineare di a e b ed ha soluzioni soltanto quando $d := MCD(a, b) \ \wedge \ d \mid c$

!ATTENZIONE! un'equazione diofantea può non avere soluzioni ma se ne ha ne ha infinite, questo perché se $\exists u, v \in \mathbb{Z}$ e la coppia (u, v) è soluzione, quindi $au + bv = c$ otteniamo che $\forall k \in \mathbb{Z}(a(u + bk) + b(v - ak) = c)$

Domanda - Come trovo tutte le soluzioni dell'equazione diofantea?

Se abbiamo trovato una soluzione con la coppia (α, β) possiamo trovare il resto delle soluzioni perché

$$(c = dk \ \wedge \ a\alpha + b\beta = d) \Rightarrow (a(\alpha k) + b(\beta k) = dk = c)$$

Esempio - Equazione diofantea

- $2x = 1$ non ha soluzioni perché $a = 2 \ \wedge \ b = 0$ e il loro $MDC(a, b) = 2$ ma sappiamo che $2 \nmid 1$
- $6x + 15y = 9$ ha soluzioni perché $a = 6 \ \wedge \ b = 15$ e il loro $MCD(a, b) = 3$ ma sappiamo che $3 \mid 9$

Equazione congruenziale

Definizione - Equazione congruenziale

Sia $0 \neq m \in \mathbb{Z}$ e $A, C, X \in \mathbb{Z}$ e rispettivamente $A = [a]_m$, $C = [c]_m$ e $X = [x]_m$, in modo da ottenere l'equazione $AX = C$ in $\mathbb{Z}_m$ che riscriviamo sotto forma di equazione congruenziale che si trova nell'anello $\mathbb{Z}_m$ in questo modo

$$ax \underset{m}{\equiv} c$$

Sappiamo che u è soluzione di $ax \underset{m}{\equiv} c \Leftrightarrow \forall v \in \mathbb{Z}$ la coppia (u, v) è soluzione di $ax + my = c$ perché risolvere un'equazione congruenziale e la stessa identica cosa di risolvere un'equazione diofantea

- " $\Rightarrow$ " Se u è soluzione dell'equazione congruenziale $au \underset{m}{\equiv} c$ abbiamo che $m \mid c - au$ quindi per definizione $\exists v \in \mathbb{Z}(c - au = mv)$ riscriviamo l'eguaglianza $au + mv = c$ e abbiamo che la coppia (u, v) è soluzione dell'equazione diofantea
- " $\Leftarrow$ " Se la coppia (u, v) è soluzione dell'equazione diofantea $au + mv = c$ allora so per certo che $m \mid c - au$ perché $c - au = mv$ e quindi $au \underset{m}{\equiv} c$ quindi u è soluzione dell'equazione congruenziale

Equazione ridotta Se a ed m sono co-primi allora l'insieme delle soluzioni è $[a]_m \cdot [a^{-1}]_m$

Domanda - Quando un'equazione congruenziale ha soluzioni?

Sappiamo che se a e m sono co-primi l'equazione congruenziale ha una soluzione perché $\forall a, u, m \in \mathbb{Z}$ abbiamo che

$$[a]_m \in U(\mathbb{Z}_m) \Leftrightarrow [u]_m \text{ e l'inverso di } [a]_m \text{ in } \mathbb{Z}_m \Leftrightarrow [a \cdot u]_m = [1]_m \Leftrightarrow au \underset{m}{\equiv} 1$$

Abbiamo che a e m devono essere co-primi perché l'$MCD(a, m) = 1$ e deve dividere 1

!ATTENZIONE! se $m = 0$ allora a è invertibile $\Leftrightarrow a = 1 \ \vee \ a = -1$

Esempio - Elementi invertibili in $\mathbb{Z}_m$

Prendiamo in esempio $\mathbb{Z}_{30}$ dove la classe di $[15]_{30}$ non è invertibile ma in $\mathbb{Z}_{31}$ la classe di $[15]_{31}$ è invertibile

Teorema - $\mathbb{Z}_m$ è un dominio di integrità quando m è primo

Se $m \neq 0$ allora $\mathbb{Z}_m$ è finito e sappiamo che:

- Gli elementi co-primi con m sono invertibili
- Essendo in un monoide finito, gli elementi invertibili sono anche cancellabili
- Gli elementi non cancellabili (ovvero non co-primi con m) sono divisori-dello-zero

Dimostrazione Sia $m \neq 0$ e $a \in \mathbb{Z}_m$ con a non co-primo con m, inoltre abbiamo $d = MCD(a, m)$ allora sappiamo che

- $d \mid m$ perciò $\exists n \in \mathbb{Z}(m = dn)$ dove, non essendo a ed m co-primi, abbiamo $(|d| > 1) \Rightarrow (|n| < |m|)$
- $(d \mid a) \Rightarrow (dn \mid an)$ ma sappiano che $m = dn$ perciò $m \mid an$

Questo ci porta alla conclusione che $[a \cdot n]_m = [0]_m$ (quindi divisore dello zero) e siccome $|n| < |m|$ con $m \neq 0$ sappiamo che n non è multiplo di m e quindi $[n]_m \neq [0]_m$

Dalla conclusione sappiamo che $\mathbb{Z}_m$ è un campo perché quando $m \neq 0$ ed è primo tutte le classi di $\mathbb{Z}_m$, tranne lo 0_{Z_m}, sono invertibili

Ma $\mathbb{Z}_m$ è un dominio di integrità perché è un anello commutativo e monoide finito, quindi gli elementi invertibili sono cancellabili e non divisori-dello-zero

Esempio - Domini di integrità quando $m \neq 0$ ed è primo

Sono domini di integrità $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5 \ldots$

Non è un dominio di integrità invece $\mathbb{Z}_6$ perché $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$ in questo caso sappiamo che

- $[0]_6 = 0_{\mathbb{Z}_6}$ ovvero lo zero dell'anello
- $[1]_6, [5]_6$ sono gli elementi invertibili
- $[2]_6, [3]_6, [4]_6$ sono gli elementi non cancellabili (quindi divisori-dello-zero)

Nota - Se m è primo non ci sono divisori-dello-zero

Prendiamo il caso in cui $m > 1$ e non sia primo, allora sappiamo che esso è sicuramente prodotto di primi che definiamo così $m = h \cdot k$, quindi giungiamo alla conclusione che $[h \cdot k]_m = [m]_m = [0]_m$

Domanda - Quante soluzioni ha un'equazione congruenziale e come le trovo?

Se sappiamo che u è soluzione dell'equazione congruenziale $ax \underset{m}{\equiv} c$ e abbiamo $u \underset{m}{\equiv} u'$ tramite la compatibilità abbiamo

$$(au \underset{m}{\equiv} c) \Rightarrow (au' \underset{m}{\equiv} c)$$

Quindi l'insieme delle soluzioni è $[u]_m$ e tutti gli elementi congrui modulo m appartenenti a quella classe.

Per trovare le soluzioni bisogna fare delle osservazioni, sia R un anello commutativo unitario e $A, C, X \in R$ e vogliamo risolvere $AX = C$

1. $A \in U(R) \Rightarrow CA^{-1}$ è l'unica soluzione
2. A cancellabile $\Rightarrow$ ha al massimo una soluzione
3. A divisore-dello-zero $\Rightarrow$ non ha soluzione oppure ne ha più di una

Vediamo cosa succede quando una di queste condizioni si verificano

1. Moltiplicando l'equazione per A^{-1} troviamo che $X = CA^{-1}$
2. Se prendiamo H e K soluzioni dell'equazione abbiamo che $(AH = C = AK) \Rightarrow (H = K)$
3. Sia H soluzione, $0_R \neq B$ e $AB = 0$ otteniamo che $A(H + B) = AH + AB = AH = C$

Esempio - Soluzioni con divisiore-dello-zero

In $\mathbb{Z}_6$ abbiamo che l'equazione $[2]_6[x]_6 = [0]_6$ dove $[2]_6$ è divisore-dello-zero e abbiamo come soluzioni $[0]_6$ e $[3]_6$

Nota - Semplificare le equazioni congruenziali

Ci sono da effettuare diversi passaggi per semplificare un'equazione congruenziale

1. Chiedersi se ha soluzioni, quindi l'$MCD(a, m)$ divide c? (In alcuni casi è più semplice controllare se un multiplo in comune tra a e m divide c)
2. Siano $a', c' \in \mathbb{N}$ con la proprietà che $a' \underset{m}{\equiv} a$ e $c' \underset{m}{\equiv} c$ allora $(ax \underset{m}{\equiv} c) = (a'x \underset{m}{\equiv} c')$
3. Siano $m, a, c, n \in \mathbb{Z}$ con $n \neq 0$ allora $an \underset{mn}{\equiv} cn \Leftrightarrow mn \mid (a - c)n \Leftrightarrow m \mid a - c \Leftrightarrow a \underset{m}{\equiv} c$
4. $\forall n \in \mathbb{Z} \setminus \{0\}$ se n è co-primo con m allora $(axn \underset{m}{\equiv} cn) \Rightarrow (ax \underset{m}{\equiv} c)$

Esempio - Semplificazioni

1. $10567890x \underset{324235235}{\equiv} 31$ non ha soluzioni perché l'$MCD(a, m)$ è multiplo di 5 ma $5 \nmid 31$
2. $(87x \underset{89}{\equiv} 16) = (-2x \underset{89}{\equiv} 16)$ perché sappiamo che $87 \underset{89}{\equiv} -2$
3. $(2x \underset{6}{\equiv} 0) = (x \underset{3}{\equiv} 0)$ perché sappiamo che possiamo dividere tutto per 2
4. $(21x \underset{100}{\equiv} 15) = (7x \underset{100}{\equiv} 5)$ perché sappiamo che 3 è co-primo con 100

Funzione di Eulero

Definizione - Funzione di Eulero

La Funzione di Eulero rappresenta in questo contesto il numero degli invertibili di $\mathbb{Z}_m$ ed è strutturata così

$$\forall m \in \mathbb{N}^* \quad \varphi(m) = |U(\mathbb{Z}_m)| = |\{i \in \mathbb{N}^* \mid i \leq m \ \wedge \ i \text{ è comprimo con } m\}|$$

Il calcolo risulta molto facile se conosciamo la fattorizzazione del numero perché sia $a = \prod_{i=1}^{k} p_i^{\alpha_i}$ quindi

$$\varphi(a) = \prod_{i=1}^{k} (p_i - 1)p_i^{\alpha_i - 1}$$

Allora ad ogni numero primo p^n togliamo i suoi multipli $\frac{p^n}{p} = p^{n-1}$ che ci porta alla formula $p^n - p^{n-1} = (p - 1)p^{n-1}$

Esempio - Funzione di Eulero

$\varphi(25) = 25 - 5 = (5-1)5 = 20$

$\varphi(6) = (2-1)\cdot(3-1) = 2$

$\varphi(5) = 5 - 1 = (5-1)1 = 4$

Elemento periodico

Definizione - Elemento periodico

Sia $(G, \cdot, 1_G, ^{-1})$ un gruppo e $x \in G$ viene definito periodico $x \Leftrightarrow \exists n \in \mathbb{N}^*(x^n = 1_G)$ (notazione additiva $n \cdot x = 1_G$)

Se x è periodico abbiamo che il suo periodo è $o(x) = min\{n \in \mathbb{N}^* \mid x^n = 1_G\}$

Domanda - Cosa succede se G è finito?

Se G è finito e $|G| = n$ allora $\forall x \in G(x^n = 1_G)$ perché in un gruppo finito tutti gli elementi sono periodici ed il loro periodo è al massimo n

Da questo ricaviamo che il periodo deve dividere la cardinalità di G

Nota - Periodici nei Monoidi

Se siamo all'interno di un monoide ha senso parlare di periodo se $x \in U(M)$

Esempio - Elemento periodico

L'unità è sempre periodica perché $(1_G)^1 = 1_G$

All'interno di $(\mathbb{Q} \setminus \{0\}, \cdot, 1, ^{-1})$ (il gruppo moltiplicativo del campo dei razionali) abbiamo:

- $(1)^1 = 1_G$ è periodico
- $(-1)^2 = 1_G$ è periodico
- 3 non è periodico perché $\nexists n \in \mathbb{N}^*(3^n = 1)$

Periodi nelle varie strutture:

- $(\mathbb{Q} \setminus \{0\}, \cdot, 1, ^{-1})$ per l'elemento -1 abbiamo $o(-1) = 2$
- $(U(\mathbb{Z}_7), \cdot, [1]_7, ^{-1})$ per l'elemento $[2]_7$ abbiamo $o([2]_7) = 3$
- $(\mathbb{Z}_7, +, [0]_7, ^{-1})$ per l'elemento $[2]_7$ abbiamo $o([2]_7) = 7$

Teorema - Il periodo di un elemento periodico è sempre multiplo del suo periodo minimo

Supponiamo x sia periodico con $o(x) = m$ allora $\forall n \in \mathbb{Z}$ abbiamo che

1. Se $n \mod m = r \neq 0$ sappiamo che $\exists q \in \mathbb{Z}(n = mq + r)$
2. $x^n = 1_G \Leftrightarrow m \mid n$

Dimostrazione

1. Quindi abbiamo $x^n = x^{mq+r} = x^{mq} \cdot x^r = (x^m)^q \cdot x^r = (1_G)^q \cdot x^r = x^r$
2. $(m \mid n) \Rightarrow (r = 0) \Rightarrow (x^n = x^0 = 1_G)$

NOTA Se $(m \nmid n) \Rightarrow (0 < r < m)$ ma essendo m il periodo minimo di x abbiamo che $x^n = x^r \neq 1_G$

Domanda - Quando due potenze sono uguali?

Quando abbiamo che $\forall a, b \in \mathbb{Z}((x^a = x^b) \Leftrightarrow (x^{a-b} = x^a \cdot (x^b)^{-1} = 1_G) \Leftrightarrow (m \mid a - b) \Leftrightarrow (a \underset{m}{\equiv} b))$

Nota - Esistono elementi di qualsiasi periodo finito

Una permutazione ciclica ha periodo k (dove k è la sua lunghezza) perché dopo k volte si è tornati al punto di partenza, questo ci permette di effettuare calcoli in artimentica modulare come ad esempio rispondere alla domanda *"Supponendo oggi sia lunedì, tra 2^{500} giorni che giorno della settimana sarà?"*

Abbiamo le seguenti informazioni:

- $k = 7$ (la lunghezza della nostra permutazione ciclica che rappresentano i giorni della settimana)
- $o([2]_7) = 3$ (il periodo della classe di resto rispetto alla moltiplicazione)
- $500 \mod 3 = 2$ (essendo il resto diverso da zero abbiamo che $x^n = x^r \neq 1G$)
- $(2^{500} \underset{7}{\equiv} 2^2) \Rightarrow (2^{500} = 2^2 = 4)$

Questo ci da la nostra risposta: *"Sarà venerdì"*

Principio di Induzione

Definizione - Principio di Induzione (1° Forma)

Se un principio vale per n allora esso vale anche per $n+1$, quindi supponendo che esso valga per 0 allora possiamo dire che vale per tutto $\mathbb{N}$, ovvero fissato un numero naturale b il principio varrà per ogni numero naturale maggiore di b.

$$\forall b \in \mathbb{N} \text{ abbiamo che } N_b := \{n \in \mathbb{N} \mid n \geq b\}$$

Sia $\varphi(n)$ un predicato unario nella variabile n definiamo così il principio di induzione:

$$(\varphi(b) \wedge \forall n \in N_b(\varphi(n) \Rightarrow \varphi(n+1)) \Rightarrow (\forall n \in N_b(\varphi(n)))$$

Dimostrazione Assumiamo sia vero $\varphi(b) \wedge \forall n \in N_b(\varphi(n) \Rightarrow \varphi(n+1)$ e che esiste l'insieme dei contro-esempi $C = \{n \in N_b \mid \neg\varphi(n)\}$, se $C \neq \emptyset$ allora esiste il minimo di questo insieme che chiamiamo m con la proprietà di $\forall a \in C(m \leq a \wedge m \in C)$.

Siccome $\varphi(b)$ è vera sappiamo che $b \notin C$ e quindi $m \neq b$ ma sicuramente $m > b$, ma essendo il minimo di C possiamo anche dire che $m - 1 \in N_b$ e che $\varphi(m-1)$ è vera.

Ma qui scatta la contraddizione perché se $m - 1 \in N_b$ vuol dire che $\varphi(m-1) \Rightarrow \varphi(m)$ è vera ma noi sappiamo che $m \in C$, quindi possiamo concludere che $C = \emptyset$ e quindi $\forall n \in N_b(\varphi(n))$.

Definizione - Principio di Induzione (2° Forma)

Se un principio vale per un $i < n$ allora esso vale anche per n, ovvero fissato un numero naturale n il principio varrà per ogni numero naturale minore di n e per n stesso.

$$\forall b \in \mathbb{N} \text{ abbiamo che } N_b := \{n \in \mathbb{N} \mid n \geq b\}$$

Sia $\varphi(n)$ un predicato unario nella variabile n definiamo così il principio di induzione:

$$(\forall n \in N_b((\forall i \in N_b((i < n) \Rightarrow (\varphi(i)))) \Rightarrow (\varphi(n))) \Rightarrow (\forall n \in N_b(\varphi(n)))$$

Dimostrazione Assumiamo sia vero $\forall n \in N_b((\forall i \in N_b((i < n) \Rightarrow (\varphi(i)))$ e che esiste l'insieme dei contro-esempi $C = \{n \in N_b \mid \neg\varphi(n)\}$, se $C \neq \emptyset$ allora esiste il minimo di questo insieme che chiamiamo m con la proprietà di $\forall a \in C(m \leq a \wedge m \in C)$.

Siccome $\varphi(b)$ è vera sappiamo che $b \notin C$ e quindi $m \neq b$ ma sicuramente $m > b$, ma essendo il minimo di C possiamo anche dire che $\forall k \in N_b(k < m)$ sicuramente $k \notin C$ e quindi $\varphi(k)$ è vera.

Ma qui scatta la contraddizione perché se $k \in N_b$ vuol dire che $\varphi(k) \Rightarrow \varphi(m)$ è vera ma noi sappiamo che $m \in C$, quindi possiamo concludere che $C = \emptyset$ e quindi $\forall n \in N_b(\varphi(n))$.

Esempio - Principio di Induzione applicato alla somma degli n numeri naturali

Sia $\varphi(n) : \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ la somma dei primi n numeri positivi e applichiamo il principio di induzione.

- Base induttiva: $\varphi(1) : \frac{1(1+1)}{2} = \frac{2}{2} = 1$ (vera)
- Passo induttivo: $\forall n \in \mathbb{N}^*(\varphi(n) \Rightarrow \varphi(n+1))$ dove $\varphi(n+1) : \sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$.

Riscriviamo quindi $\varphi(n+1)$ come $\varphi(n) + (n+1)$ e dimostriamo che questa sia vera:

$$\sum_{i=1}^{n+1} i = (\sum_{i=1}^{n} i) + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

Esempio - Principio di Induzione su un'applicazione binaria

Sia $(S, *)$ un semi-gruppo e $x \in S$ sappiamo che $\forall n, m \in \mathbb{N}^*(x^{n+m} = x^n * x^m)$.

Definiamo anche la ricorsività che dice $x^1 = x$ e che $\forall n \in \mathbb{N}^*(x^{n+1} = x^n * x)$.

Quindi sia $\forall m \in \mathbb{N}^*$ $\varphi(m) : x^{n+m} = x^n * x^m$ e applichiamo il principio di induzione.

- Base induttiva: $\varphi(1) : x^{n+1} = x^n * x$ (vera)
- Passo induttivo: $\forall m \in \mathbb{N}^*(\varphi(m) \Rightarrow \varphi(m+1))$ dove $\varphi(m+1) : x^{n+(m+1)}$

Riscriviamo quindi $\varphi(m+1)$ come $\varphi(m) + (m+1)$ e dimostriamo che questa sia vera (sfruttiamo la proprietà associativa):

$$x^{n+(m+1)} = x^{(n+m)+1} = x^{n+m} * x = (x^n * x^m) * x = x^n * (x^m * x) = x^n * x^{m+1} = x^{n+(m+1)}$$

Omomorfismo e Isomorfismo

Omomorfismo

Definizione - Omomorfismo

Supponiamo di avere due strutture algebriche $(S, *)$ e $(T, \cdot)$ inoltre un'applicazione $f : S \to T$, questa applicazione è un omomorfismo da $(S, *)$ a $(T, \cdot)$ se e solo se:

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

Esempio - Omomorfismi

$g : x \in \mathbb{Z} \longmapsto 2x \in \mathbb{Z}$ è un omomorfismo da $(Z, +)$ a $(Z, +)$ perché:

$$\forall x, y \in \mathbb{Z}\ g(x + y) = 2(x + y) = 2x + 2y = g(x) + g(y)$$

$g : x \in \mathbb{Z} \longmapsto 2x \in \mathbb{Z}$ non è un omomorfismo da $(Z, \cdot)$ a $(Z, \cdot)$ perché:

$$\forall x, y \in \mathbb{Z}\ g(xy) = 2(xy)\ \neq\ g(x) \cdot g(y) = 4xy$$

$h : x \in P(\mathbb{Z}) \longmapsto x \cap \mathbb{N} \in P(\mathbb{N})$ è un omomorfismo da $(P(\mathbb{Z}), \cap)$ a $(P(\mathbb{N}), \cap)$ perché:

$$\forall x, y \in P(\mathbb{Z})\ h(x \cap y) = x \cap y \cap \mathbb{N} = (x \cap \mathbb{N}) \cap (y \cap \mathbb{N}) = h(x) \cap t(h)$$

$h : x \in P(\mathbb{Z}) \longmapsto x \cap \mathbb{N} \in P(\mathbb{N})$ è un omomorfismo da $(P(\mathbb{Z}), \cup)$ a $(P(\mathbb{N}), \cup)$ perché:

$$\forall x, y \in P(\mathbb{Z})\ h(x \cup y) = x \cup y \cup \mathbb{N} = (x \cup \mathbb{N}) \cup (y \cup \mathbb{N}) = h(x) \cup t(h)$$

Isomorfismo

Definizione - Isomorfismo

L'isomorfismo è un omomorfismo biettivo, ovvero se $f : (S, *) \longmapsto (T, \cdot)$ è un omomorfismo allora la sua inversa $f^{-1} : (T, \cdot) \longmapsto (S, *)$ è un omomorfismo, ovvero:

$$\forall x, y \in T(f^{-1}(a \cdot b) = f^{-1}(a) * f^{-1}(b))$$

Questa uguaglianza è vera perché:

$$\forall x, y \in T \begin{cases} f(f^{-1}(x \cdot y)) = x \cdot y \\ f(f^{-1}(x) * f^{-1}(y)) = f(f^{-1}(x)) \cdot f(f^{-1}(y)) = x \cdot y \end{cases} \tag{1}$$

Esempio - Isomorfismo

$g : x \in (\mathbb{R}^+, +) \longmapsto e^x \in (\mathbb{R}^+, \cdot)$ è un omomorfismo perché:

$$\forall x, y \in \mathbb{R}\ e^{x+y} = e^x \cdot e^y$$

$g^{-1} : x \in (\mathbb{R}^+, \cdot) \longmapsto \ln(x) \in (\mathbb{R}^+, +)$ è un omomorfismo perché:

$$\forall x, y \in \mathbb{R}\ \ln(e^x * e^y) = \ln(e^x) + \ln(e^y)$$

Quindi essendo g biettiva, esso è un isomorfismo.

Proprietà di omomorfismi suriettivi

Teorema - Commutatività negli omomorfismi suriettivi

Se $f : (S, *) \longmapsto (T, \cdot)$ un omomorfismo suriettivo allora se $*$ è commutativa $\Rightarrow \cdot$ è commutativa.

Dimostrazione $\forall x, y \in T \ \exists a, b \in S (x = f(a) \land y = f(b))$

$$x \cdot y = f(a) \cdot f(b) = f(a * b) = f(b * a) = f(b) \cdot f(a) = y \cdot x$$

Teorema - Associatività negli omomorfismi suriettivi

Se $f : (S, *) \longmapsto (T, \cdot)$ un omomorfismo suriettivo allora se $*$ è associativa $\Rightarrow \cdot$ è associativa.

Dimostrazione $\forall x, y, z \in T \ \exists a, b, c \in S (x = f(a) \land y = f(b) \land z = f(c))$

$$x \cdot (y \cdot z) = f(a) \cdot (f(b) \cdot f(c)) = f(a * (b * c)) = f((a * b) * c) = (f(a) \cdot f(b)) \cdot f(c) = (x \cdot y) \cdot z$$

Teorema - Elemento neutro negli omomorfismi suriettivi

Se $(S, *)$ ha neutro allora $f(t)$ sarà neutro in $(T, \cdot)$, definiamo $\forall x \in T \ \exists a \in S \ (f(x) = a)$, allora:

- t è un elemento neutro-a-sinistra in $(S, *) \Leftrightarrow x \cdot f(t) = f(a) \cdot f(t) = f(a * t) = f(a) = x$
- t è un elemento neutro-a-destra in $(S, *) \Leftrightarrow f(t) \cdot x = f(t) \cdot f(a) = f(t * a) = f(a) = x$
- t è un elemento neutro in $(S, *) \Leftrightarrow$ neutro sia a destra che a sinistra

Teorema - Elementi simmetrici negli omomorfismi suriettivi

Sia $(S, *, t)$ e $x \in S$ ha simmetrico $y \in S$ allora $f(x)$ avrà simmetrico $f(y)$ in $(T, \cdot, l)$, definiamo $\forall x, y \in T \ \exists a, b \in S$ $(f(x) = a \land f(y) = b)$, allora:

- x ha simmetrico-a-sinistra in $(S, *, t) \Leftrightarrow y \cdot x = t \Rightarrow f(y) \cdot f(x) = f(t) \Rightarrow f(y * x) = f(t) \Rightarrow b * a = l$
- x ha simmetrico-a-destra in $(S, *, t) \Leftrightarrow x \cdot y = t \Rightarrow f(x) \cdot f(y) = f(t) \Rightarrow f(x * y) = f(t) \Rightarrow a * b = l$
- x ha simmetrico $(S, *, t) \Leftrightarrow$ ha simmetrico sia a destra che a sinistra

Nota - Elementi cancellabili negli omomorfismi suriettivi

La cancellabilità **non sempre si conserva** negli omomorfismi suriettivi

Proprietà degli isomorfismi

Teorema - Elementi cancellabili negli isomorfismi

Sia $f : (S, *) \longmapsto (T, \cdot)$ un isomorfismo, se sappiamo che $x \in S$ è cancellabile in $(S, *)$ allora anche $f(x)$ sarà cancellabile in $(T, \cdot)$.

Dimostrazione

$$\forall a, b \in S \ (a * x = b * x) \Rightarrow (a = b)$$

$$\forall u, v \in T \ ((u \cdot f(x) = v \cdot f(x)) = (f(f^{-1}(u)) \cdot f(x) = f(f^{-1}(v)) \cdot f(x)) = (f(f^{-1}(u) * x) = f(f^{-1}(v) * x)))$$

Quindi sappiamo che $f^{-1}(u) * x = f^{-1}(v) * x \Rightarrow (f^{-1}(u) = f^{-1}(v)) = (u = v)$

Relazioni

Definizione - Relazione di equivalenza

Sia $\rho \in Rel(A)$, questo significa che $\rho = (A, A, \rho\#)$ (dove $\rho\# \subseteq A \times A$), ha le seguenti proprietà:

- ρ è riflessiva $\Leftrightarrow \forall x \in A(x \rho x)$
- ρ è simmetrica $\Leftrightarrow \forall x, y \in A(x \rho y \Leftrightarrow y \rho x)$
- ρ è transitiva $\Leftrightarrow \forall x, y, z \in A((x \rho y \wedge y \rho z) \Rightarrow (x \rho z))$

Inoltre basate sulle proprietà precedenti abbiamo:

- ρ è una relazione di equivalenza $\Leftrightarrow$ è riflessiva, simmetrica e transitiva

Relazioni banali: le relazioni banali sono quella di eguaglianza e universale.

Relazione capovolta: $\forall x, y \in A(x \overset{\curvearrowleft}{\rho} y \Leftrightarrow y \rho x)$

Definizione - Nucleo di equivalenza

Si definisce nucleo di equivalenza di un'applicazione la relazione binaria $\sim$ ponendo $(x \sim y \Leftrightarrow f(x) = f(y))$.

Data l'applicazione $f : A \to B$, prendiamo il suo nucleo di equivalenza $\sim \in Eq(A)$ e sappiamo che:

- $\sim$ è riflessiva perché $\forall x \in A(x \sim x)$ è vera $f(x) = f(x)$
- $\sim$ è simmetrica perché $\forall x, y \in A(x \sim y \Leftrightarrow y \sim x)$ è vera $f(x) = f(y) \Leftrightarrow f(y) = f(x)$
- $\sim$ è transitiva perché $\forall x, y, z \in A((x \sim y \wedge y \sim z) \Rightarrow (x \sim z))$ è vera $f(x) = f(y) = f(z)$

Definizione - Relazione d'ordine

Sia $\rho \in Rel(A)$ qesto significa che $\rho = (A, A, \rho\#)$ (dove $\rho\# \subseteq A \times A$), ha le seguenti proprietà:

- ρ è anti-simmetrica $\Leftrightarrow \forall x, y \in A((x \rho y \wedge y \rho x) \Rightarrow (x = y))$
- ρ è anti-riflessiva $\Leftrightarrow \forall x, y \in A(x \not\rho x)$

Possiamo quindi definire due tipi di relazioni d'ordine basate sulle precedenti proprietà:

- $\rho \in OL(A)$ (ovvero "Ordine Largo") $\Leftrightarrow$ è anti-simmetrica, riflessiva e transitiva
- $\rho \in OS(A)$ (ovvero "Ordine Stretto") $\Leftrightarrow$ è anti-riflessiva e transitiva

Insieme delle relazioni d'ordine lo indichiamo con $OL(A)$

Relazione duale $\forall x, y \in A(x \overset{\curvearrowleft}{\rho} y \Leftrightarrow y \rho x)$ ovvero passando alla capovolta otteniamo sempre una relazione d'ordine

Relazione d'ordine indotta Sia $B \subseteq A$ allora ρ induce su B, ovvero due elementi sono in relazione $\Leftrightarrow$ lo era già prima

Relazione totale ρ è una relazione totale $\forall x, y \in A \Leftrightarrow x$ e y sono confrontabili

Esempio - Relazione d'ordine

Sono relazioni di ordine largo:

- $(\mathbb{R}, \leq)$ $(\mathbb{N}, \underset{\mathbb{N},\cdot}{|})$
- $\forall A$ abbiamo $(A, \subseteq)$ $(A, =)$ $(P(A), \subseteq)$

Non è invece una relazione di ordine largo $(\mathbb{Z}, \underset{(\mathbb{Z},\cdot)}{|})$ perché non è anti-simmetrica

Sono relazione di ordine stretto:

- $(\mathbb{R}, <)$
- $\forall A$ abbiamo $(A, \subset)$ $(P(A), \subset)$

$(\mathbb{R}, \leq)$ è un'insieme totalmente ordinato quindi $\leq$ è totale

$(\mathbb{N}, |)$ non è un'insieme totalmente ordinato perché $2 \nmid 3 \ \wedge \ 3 \nmid 2$

$(P(\mathbb{N}), \subseteq)$ non è un'insieme totalmente ordinato perché $\{1\} \not\subseteq \{2\} \wedge \{2\} \not\subseteq \{1\}$

$\forall A$ $(A, =)$ non è totalmente ordinato se $|A| > 1$

Teorema - Esiste un'applicazione biettiva da $OL(A)$ a $OS(A)$

Sia $\rho \in OL(A)$ e definiamo ("rho diverso") $\rho_{\neq} \in Rel(A)$ in questo modo $\forall x, y \in A(x\rho_{\neq}y \Leftrightarrow (x\rho y \wedge x \neq y))$

Otteniamo che $\rho_{\neq} \in OS(A)$

Dimostrazione

- $\rho_{\neq}$ è anti-riflessiva per definizione perché nessun elemento può essere in relazione con se stesso
- $\rho_{\neq}$ è transitivo perché $\forall x, y, z \in A((x\rho_{\neq}y \wedge y\rho_{\neq}z) \Rightarrow ((x\rho y \wedge x \neq y) \wedge (y\rho z \wedge y \neq z)) \Rightarrow (x\rho z \wedge x \neq z) \Leftrightarrow x\rho_{\neq}z)$

Nota $x \neq y$ perché se $x = y$ avremmo $(x\rho y \wedge y\rho x) \Rightarrow (x = y)$ ma ρ è anti-simmetrica e questo genera un assurdo

Conclusione ottenendo un'applicazione biettiva da $\rho \in OL(A) \longmapsto \rho_{\neq} \in OS(A)$ perché ha un'inversa

Prendiamo $\sigma \in OS(A)$ e definiamo ("sigma uguale") $\sigma_{=} \in Rel(A)$ in questo modo $\forall x, y \in A(x\sigma_{=}y \Leftrightarrow (x\sigma y \vee x = y))$

Otteniamo che $\sigma_{=} \in OL(A)$

Dimostrazione

- $\sigma_{=}$ è riflessiva per definizione perché due elementi uguali sono in relazione tra loro
- $\sigma_{=}$ è anti-simmetrica perché $\forall x, y \in A((x\sigma_{=}y \wedge y\sigma_{=}x) \Rightarrow ((x\sigma y \vee x = y) \wedge (y\sigma x \vee y = x)) \Rightarrow (x = y))$
- $\sigma_{=}$ è transitiva perché $\forall x, y, z \in A((x\sigma_{=}y \wedge y\sigma_{=}z) \Rightarrow ((x\sigma y \vee x = y) \wedge (y\sigma z \vee y = z)) \Rightarrow (x\sigma_{=}z))$

NOTA

- Siamo sicuri che $\sigma_{=}$ è anti-simmetrica perché $((x\sigma y \vee x = y) \wedge (y\sigma x \vee y = x))$ genera quattro casi possibili
  1. $x\sigma y \wedge y\sigma x$

2. $x\sigma y \wedge y = x$
3. $x = y \wedge y\sigma x$
4. $x = y \wedge y = x$

Osserviamo il primo caso perché σ è transitiva quindi $x\sigma x$ ma essendo anche anti-simmetrica questo è un assurdo

- Siamo sicuri che $\sigma_=$ è transitiva perché $((x\sigma \vee x = y) \wedge (y\sigma z \vee y = z))$ genera quattro casi possibili

1. $x\sigma y \wedge y\sigma z$
2. $x = y \wedge y\sigma z$
3. $x\sigma y \wedge y = z$
4. $x = y \wedge y\sigma z$

Osserviamo solo il primo caso perché σ è transitiva quindi $x\sigma_= z$

Nota - Conviene studiare la relazione e la sua duale?

La risposta è no, perché studiata una relazione avrà le stesse proprietà della sua duale, ovvero se dimostriamo qualcosa per i minimi sarà automaticamente dimostrato anche per i massimi

Definizione - Elementi confrontabili

Sia $\rho \in OL(A)$ definiamo due elementi confrontabili in $(A, \rho) \Leftrightarrow \forall x, y \in A(x\rho y \vee y\rho x)$

Prese le relazioni d'ordine $\leq \in OL(A)$ e $< = \leq_{\neq} \in OS(A)$ otteniamo che $\forall x, y \in A$ abbiamo quattro casi possibili

1. $x < y$
2. $x = y$
3. $x > y$

} 1. $x \leq y$
2. $x \geq y$

} x e y sono confrontabili rispetto a $\leq$

4. Non sono confrontabili

Domanda - Posso "trasferire" una relazione d'ordine da un'insieme ad un altro?

Bhe si che si può, data l'applicazione $f : A \to B$ osserviamo i due casi, ovvero quello dell'ordine stretto e largo (perché hanno proprietà diverse e vengono definite in modo diverso):

- Partendo da $< \in OS(B)$ definiamo $\alpha_{\neq} \in Rel(A)$ in questo modo: $\forall x, y \in A(x\alpha_{\neq} y \Leftrightarrow f(x) < f(y))$ osserviamo che ha le seguenti proprietà
  - Anti-riflessiva per definizione perché $\forall x \in A(x \not\alpha_{\neq} x)$
  - Transitiva perché $\forall x, y, z \in A((x\alpha_{\neq} y \wedge y\alpha_{\neq} z) \Rightarrow (x\alpha_{\neq} z))$

  Quindi otteniamo che $\alpha_{\neq} \in OS(A)$
- Partendo da $\leq \in OL(B)$ definiamo $\alpha_= \in Rel(A)$ in questo modo: $\forall x, y \in A(x\alpha_= y \Leftrightarrow (x = y \vee f(x) < f(y)))$ osserviamo che ha le seguenti proprietà
  - Riflessiva per definizione perché $\forall x, y \in A(x\alpha_= x)$
  - Transitivita perché $\forall x, y, z \in A((x\alpha_= y \wedge y\alpha_= z) \Rightarrow (x\alpha_= z))$
  - Anti-simmetrica perché $\forall x, y \in A((x\alpha_= y \vee y\alpha_= x) \Rightarrow (x = y))$

  Quindi otteniamo che $\alpha_= \in OL(A)$

Nota - Perché non abbiamo definito $\alpha_=$ allo stesso modo di $\alpha_\neq$?

Per rendere più chiara l'idea poniamo in esempio che il nostro insieme A sia l'insieme di articoli venduti in un negozio, $B = (\mathbb{Q}, \leq)$ e f la funzione che ad ogni articolo associa un prezzo, adesso valutiamo i casi possibili:

- $\alpha_\neq$ in questo caso sarebbe la relazione "costare di meno", ovvero due articoli sono in relazione se uno costa di meno dell'altro
- $\alpha_=$ per come l'abbiamo definita prima sarebbe la relazione "essere lo stesso articolo oppure costare di meno", ovvero due articoli sono in relazione se sono lo stesso articolo o uno costa di meno dell'altro

Ma cosa sarebbe successo se avessimo definito $\alpha_=$ in questo modo $\forall x, y \in A(x\alpha_= y \Leftrightarrow f(x) \leq f(y))$? Seguendo l'esempio precedente per come l'abbiamo definita qui la relazione sarebbe "costare lo stesso prezzo o costare di meno", ovvero due articoli sono in relazione se hanno lo stesso prezzo o uno costa meno dell'altro

Ovviamente definire in questo modo $\alpha_=$ va contro la proprietà anti-simmetrica per essere una relazione d'ordine largo

Domanda - Ma quindi se B non ha massimali e non ha minimali nemmeno A?

Abbiamo definito $B = (\mathbb{Q}, \leq)$ che non ha minimali e massimali, abbiamo definito poi A come l'insieme di articoli venduti in un negozio nel quale troviamo sempre un prezzo minimale e un prezzo massimale, allora come si risolve il problema?

Basta considerare gli elementi minimali e massimali su $C := im\, f$, ovvero tra tutti gli articoli che hanno immagine, ed essendo un insieme ordinato finito abbiamo sempre minimale e massimale, ottenendo quindi

- x è minimale in $(A, \rho) \Leftrightarrow x$ è minimale in $(C, \leq)$
- x è massimale in $(A, \rho) \Leftrightarrow x$ è massimale in $(C, \leq)$

Insieme ordinato

Definizione - Insieme ordinato

Si chiama insieme ordinato (oppure catena) la coppia ordinata (A, ρ) dove $\rho \in OL(A)$

Sottoinsieme Ordinato ovvero una parte chiusa rispetto all'insieme ordinato

Nota - Il sottoinsieme di un insieme non totalmente ordinato può essere ancora ordinato

È sempre vero che un sottoinsieme di un insieme ordinato è totalmente ordinato ma non sempre è vero che un sottoinsieme di un insieme non totalmente ordinato sia non totalmente ordinato

Prendiamo in esempio $(\mathbb{N}, |\,)$ non è un insieme totalmente ordinato ma il suo sottoinsieme (tutte le potenze di due, $|\,$) è un sottoinsieme totalmente ordinato

Minimo e minimale, Massimo e massimale

Definizione - Minimo e minimale

Sia $\rho \in OL(A)$ e $x \in A$ definiamo:

- x è minimo in $(A, \rho) \Leftrightarrow \forall y \in A(x \rho y)$
- x è minimale in $(A, \rho) \Leftrightarrow \forall y \in A(y \rho x \Rightarrow x = y)$

In maniera duale otteniamo che:

- x è massimo in $(A, \rho) \Leftrightarrow \forall y \in A(y \rho x)$
- x è massimale in $(A, \rho) \Leftrightarrow \forall y \in A(x \rho y \Rightarrow x = y)$

Insiemi totalmente ordinati il minimo e il minimale, così come il massimo e il massimale, coincidono sempre

Nota indichiamo il minimo con $min(A, \rho)$ e $max(A, \rho)$

Esempio - Minimo e minimale

$(P(\mathbb{N}), \subseteq)$ ha i seguenti minimi e massimi

- minimo $\emptyset$ e quindi solo minimale perché $\forall y \in P(\mathbb{N})(\emptyset \subseteq y)$
- massimo $\mathbb{N}$ e quindi solo massimale perché $\forall y \in P(\mathbb{N})(y \subseteq \mathbb{N})$

$(\mathbb{N}, \mid)$ ha i seguenti minimi e massimi

- minimo 1 perché $\forall y \in \mathbb{N}(1 \mid y)$
- massimo 0 perché $\forall y \in \mathbb{N}(y \mid 0)$

$(P(\mathbb{N}) \setminus \{\emptyset\})$ non c'è minimo ma ha infiniti minimali (ovvero i singleton degli elementi)

Teorema - Se c'è un minimo allora è anche l'unico minimale

$\forall x \in A(x$ minimo in $(A, \rho) \Rightarrow x$ è l'unico minimale in $(A, \rho))$

Dimostrazione seguendo la premessa abbiamo due condizioni che vanno rispettate

$$\left.\begin{array}{l} x \text{ minimo in } (A, \rho) \Rightarrow \forall y \in A(x \rho y) \\ x \text{ minimale in } (A, \rho) \Rightarrow \forall y \in A(x \rho y \Rightarrow x = y) \end{array}\right\} x = y$$

Conclusione se esiste un minimo allora è unico

Nota per dualità abbiamo dimostrato che $x = min(A, \rho) = max(A, \overset{\frown}{\rho})$ e x minimale in (A, ρ) = massimale in $(A, \overset{\frown}{\rho})$

Teorema - A insieme finito e non vuoto ha sia minimali che massimali

Sia (A, ρ) un insieme ordinato, finito e non vuoto allora ha elementi minimali (e massimali per dualità)

Dimostrazione per controesempio minimo su $|A|$

1. Sia $C = \{n \in \mathbb{N} \mid \exists \rho \in OL(A)(|A| = n \wedge A \neq \emptyset \wedge (A, \rho)$ non ha minimali$)\}$ con $n = min(C)$ e (A, ρ) un controesempio tale che $|A| = n$
2. Sappiamo che $n > 0$ (perché $A \neq \emptyset$) quindi $\exists x \in A(x$ non è minimale) quindi sappiamo che esiste qualche elemento più piccolo di x
3. Definiamo l'insieme di elementi più piccoli di x, ovvero $B = \{y \in A \mid y \rho_{\neq} x\} \neq \emptyset$ e questo ci dice che $|B| < n$ perché $x \notin B$
4. $|B| \notin C$ allora esiste y minimale in (B, ρ) ma y è minimale anche in (A, ρ)

5. Se $\exists z \in A$ con la proprietà che $z \rho_{\neq} y \rho_{\neq} x$ per transitività $z \rho_{\neq} x$ quindi abbiamo che $z \in B$

Conclusione abbiamo generato un assurdo perché non esistono elementi di (A, ρ) più piccoli di y che è minimale in (A, ρ) per cui non è un controesempio minimo

Nota lo stesso vale per dualità riguardo i massimali

Teorema - Può esistere un minimale o un massimale che non sia ne minimo ne massimo

Sia $m \notin \mathbb{Z}$ e $A := \mathbb{Z} \cup \{m\}$ e definiamo $\rho \in Rel(A)$ in questo modo $\forall x, y \in A(x \rho y \Leftrightarrow ((x, y \in \mathbb{Z} \wedge x \leq y) \vee x = y = m))$

Verifichiamo che ρ sia una relazione d'ordine, ovvero

- ρ è riflessiva $\Leftrightarrow \forall a \in A(a \rho a)$
- ρ è anti-simmetrica $\Leftrightarrow \forall a, b \in A((a \rho b \wedge b \rho a) \Rightarrow (a = b))$
- ρ è transitiva $\Leftrightarrow \forall a, b, c \in A((a \rho b \wedge b \rho c) \Rightarrow (a \rho c))$

Dimostrazione

- Ogni numero è minore o uguale di se stesso e m è in relazione con se stesso
- Se $a \neq b$ allora $a, b \in \mathbb{Z} \wedge a \leq b \leq a$ ma se sono diversi è un assurdo
- Abbiamo che $b \in \{a, c\}$ oppure $a \neq b \wedge b \neq c$ quindi $a, b, c \in \mathbb{Z}$ per cui $a \leq b \wedge b \leq c$ quindi $a \leq c$

Concludo che in (A, ρ) m è un minimale e massimale mentre $\forall n \in \mathbb{Z}((n-1) \rho n \wedge n \rho (n+1))$ quindi n non è un massimale o un minimale

Maggiorante e Minoranti, Estremo Superiore e Estremo Inferiore

Definizione - Minorante e Maggiorante

Sia A un'insieme ordinato e $\alpha \in OL(A)$ con $X \subseteq A$ allora definiamo

- a è un minorante di X in $(A, \alpha) \Leftrightarrow \forall x \in X(a \alpha x)$
- a è un maggiorante di X in $(A, \alpha) \Leftrightarrow \forall x \in X(x \alpha a)$

Se a appartiene all'insieme X allora abbiamo

- a è un minorante di X in $(A, \alpha) \Leftrightarrow a = min(X, \alpha) \Leftrightarrow a \in X \cap X^{\downarrow(A,\alpha)}$
- a è un maggiorante di X in $(A, \alpha) \Leftrightarrow a = max(X, \alpha) \Leftrightarrow a \in X \cap X^{\uparrow(A,\alpha)}$

NOTA con $X^{\uparrow(X,\alpha)}$ indichiamo i maggioranti invece con $X^{\downarrow(X,\alpha)}$ indichiamo i minoranti

Esempio - Minoranti e Maggioranti

$(\mathbb{N}, \mid)$ i minoranti di $X \subseteq \mathbb{N}$ sono i divisori comuni e i maggioranti invece i multipli comuni

$\mathbb{N}^{\downarrow(\mathbb{Z},\leq)} = \{n \in \mathbb{Z} \mid n \leq 0\} = \{0\}^{\downarrow(\mathbb{Z},\leq)}$

$(P(S), \subseteq)$ abbiamo che $\forall X \subseteq P(S)$ se $X \neq \emptyset \Rightarrow (X^{\downarrow(P(S),\subseteq)} = \bigcap X \wedge X^{\uparrow(P(S),\subseteq)} = \bigcup X$

Nota - Maggioranti e Minoranti dell'insieme vuoto

Essendo la forma proposizionale sempre vera per ogni elemento dell'insieme otteniamo $\emptyset^{\uparrow(A,\alpha)} = A = \emptyset^{\downarrow(A,\alpha)}$

Nota - Un "De Morgan" dei Minoranti e Maggioranti

Quella che potremmo definire come una "legge di De Morgan" perché ha un concetto molto simile, ovvero

- $(X \cup Y)^{\downarrow} = X^{\downarrow} \cap Y^{\downarrow}$
- $(X \cup Y)^{\uparrow} = X^{\uparrow} \cap Y^{\uparrow}$

Definizione - Estremo Superiore e Inferiore

Sia A un'insieme e $\alpha \in OL(A)$ con (A, α) e $\alpha : x\alpha y \Leftrightarrow x = y \vee |x| = |y|$ abbiamo che

- Estremo superiore di $X = sup(X) = min(X^{\uparrow(A,\alpha)})$
- Estremo inferiore di $X = inf(X) = max(X^{\downarrow(A,\alpha)})$

Nota - Esistenza di Minoranti e Maggioranti con relativi Estremi

Se A ha non ha minoranti o maggioranti allora sicuramente non avrà estremi, ma può avere maggioranti e minoranti senza avere estremi, prendiamo in esempio il caso di $(P(A), \alpha)$ dove tutti gli insiemi di cardinalità 2 hanno come minoranti i singleton e l'insieme vuoto, ma non essendoci un massimo tra i singleton perché sono tutti massimali non esiste un estremo inferiore

Questo ci dice anche che è sempre garantita la presenza di un maggiorante e minorante quando A ha rispettivamente massimo e minimo, ovvero

- Se X ha massimo a allora $sup(X) = a$
- Se X ha minimo a allora $inf(X) = a$

Omomorfismo e Isomorfismo tra insiemi ordinati

Definizione - Omomorfismo tra insiemi ordinati

Siano A e B due insiemi ed $f : A \to B$ con $\alpha \in OL(A)$ e $\beta \in OL(B)$, quindi definiti gli insiemi ordinati (A, α) e (B, β) si tratta di un'omomorfismo se viene conservato l'ordinamento quando

- f è crescente da (A, α) a $(B, \beta) \Leftrightarrow \forall x, y \in A(x\alpha y \Rightarrow f(x)\ \beta\ f(y))$
- f è decrescente da (A, α) a $(B, \beta) \Leftrightarrow \forall x, y \in A(x\alpha y \Rightarrow f(x)\ \overset{\curvearrowleft}{\beta}\ f(y))$

Definizione - Isomorfismo tra insiemi ordinati

Siano A e B due insiemi ed $f : A \to B$ con $\alpha \in OL(A)$ e $\beta \in OL(B)$, quindi definiti gli insiemi ordinati (A, α) e (B, β) si tratta di un'isomorfismo se viene conservato l'ordinamento quando

- f è crescente da (A, α) a $(B, \beta) \Leftrightarrow \forall x, y \in A(x\alpha y \Rightarrow f(x)\ \beta\ f(y))$
- f^{-1} è crescente da (B, β) a $(A, \alpha) \Leftrightarrow \forall x, y \in B(x\beta y \Rightarrow f(x)\ \alpha\ f(y))$

Quindi otteniamo che per essere un'isomorfismo $\forall x, y \in A(x\alpha y \Leftrightarrow f(x)\ \beta\ f(y))$

Nota un'applicazione biettiva non implica un isomorfismo tra insiemi ordinati!

Nota - Gli isomorfismi conservano le proprietà degli insiemi ordinati

Gli isomorfismi tra insiemi ordinati conservano le proprietà, ovvero dati gli insiemi A e B e le relazioni d'ordine $\alpha \in OL(A)$ e $\beta \in OL(B)$ sappiamo che:

- Se x è minimo in (A, α) allora $f(x)$ è minimo in (B, β)
- Se x è massimo in (A, α) allora $f(x)$ è massimo in (B, β)
- Se (A, α) è totalmente ordinato allora (B, β) è totalmente ordinato

Esempio - Omomorfismo e isomorfismo

Data la funzione biettiva $id_{\mathbb{N}^*} : x \in \mathbb{N}^* \longmapsto x \in \mathbb{N}^*$ e gli insiemi ordinati $(\mathbb{N}^*, \mid)$ e $(\mathbb{N}^*, \leq)$ possiamo osservare che

- Otteniamo un omomorfismo da $(\mathbb{N}^*, \mid)$ a $(\mathbb{N}^*, \leq)$ perché $\forall x, y \in \mathbb{N}^* (x \mid y \Rightarrow x \leq y)$
- Non abbiamo un omomorfismo da $(\mathbb{N}^*, \leq)$ a $(\mathbb{N}^*, \mid)$ perché abbiamo come controesempio $2 \leq 3$ ma $2 \nmid 3$

Quindi non è un isomorfismo, infatti $(\mathbb{N}^*, \leq)$ è totalmente ordinato mentre $(\mathbb{N}^*, \mid)$ non lo è, anche se l'applicazione è biettiva!

Intervallo

Definizione - Intervallo

Sia A un'insieme e $\alpha \in OL(S)$ e dato l'insieme ordinato (A, α) abbiamo due tipi di intervallo

- **Intervallo chiuso** $\forall x, y \in A \; [x, y]_{(A,\alpha)} = \{a \in A \mid x \alpha a \wedge a \alpha y\}$
- **Intervallo aperto** $\forall x, y \in A \;]x, y[_{(A,\alpha_{\neq})} = \{a \in A \mid x \alpha_{\neq} a \wedge a \alpha_{\neq} y\}$

Nota si possono usare le combinazioni di intervallo aperto e chiuso

Esempio - Intervallo

Intervalli chiusi

- $[3, 12]_{(\mathbb{N}, \leq)} = \{3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
- $[3, 12]_{(\mathbb{N}, \mid)} = \{3, 6, 12\}$

Intervalli aperti

- $]3, 12[_{(\mathbb{N}, \leq)} = \{4, 5, 6, 7, 8, 9, 10, 11\}$
- $]3, 12[_{(\mathbb{N}, \mid)} = \{6\}$

Copertura

Definizione - Copertura

Sia A un'insieme e $\alpha \in OL(A)$ con (A, α) insieme ordinato, allora definiamo la relazione binaria in A chiamata "Copertura"

$$\forall x, y \in A (y \gamma x \Leftrightarrow (x \alpha_{\neq} y \wedge]x, y[= \emptyset))$$

Quindi solo se sono rispettate queste tre condizioni

1. Non ci sono elementi tra x e y, ovvero $x\alpha_{\neq}y \wedge \forall z \in A(x \not\alpha_{\neq} z \vee z \not\alpha_{\neq} y))$
2. x è il più grande tra gli elementi più piccoli di y, ovvero x è un elemento massimale in $\{z \in A \mid z\alpha_{\neq}y\}$
3. y è il più piccolo tra gli elementi più grandi di x, ovvero y è minimale in $\{z \in A \mid x\alpha_{\neq}z\}$

Esempio - Copertura

Osserviamo la relazione di copertura per diversi insiemi ordinati

- $(\mathbb{Z}, \leq)$ sappiamo che 6 copre 5
- $(\mathbb{Q}, \leq)$ sappiamo che nessun numero copre 5 perché preso $5+\epsilon$ esisterà sicuramente $\frac{5+\epsilon}{2}$ nell'intervallo $]5, 5+\epsilon[$
- $(P(\mathbb{Z}), \subseteq)$ tutti i singleton coprono $\emptyset$, tutti i singletono sono coperti da insiemi di due elementi che contengono il singleton e così via...

Teorema - La copertura descrive l'insieme finito

Sia A finito e $\alpha \in OL(A)$ con γ relazione di copertura definita da α in questo modo

$$\forall x, y \in A(x\alpha y \Leftrightarrow \exists n \in \mathbb{N}(\exists c_o, c_1, c_2, ..., c_n \in A(x = c_0 \wedge y = c_n \wedge \forall i \in \{1, 2, ..., n\}(c_i \gamma c_{i-1}))))$$

Dimostrazione

- "$\Leftarrow$"
  - Se $n = 0$ allora $x = y$ e $x\alpha y$
  - Se $n > 0$ allora $x\alpha c_1$ perché $c_1 \gamma x$
    - Se $n = 1$ allora $c_1 = y$ quindi $x\alpha y$
    - Se $n > 2$ essendo α transitiva (non γ) e $c_2 \gamma c_1$ otteniamo che $(x\alpha c_1 \wedge c_1 \alpha c_2) \Rightarrow (x \alpha c_2)$ e sapendo che $y \gamma c_{n-1}$ per transitività abbiamo $x\alpha y$
- "$\Rightarrow$" (qui facciamo uso di A finito perché sappiamo ha minimale)
  - Se $x = y$ allora poniamo $n = 0$ ottenendo $x = c_0 = y$
  - Se $x \neq y$ abbiamo che l'intervallo $]x, y] \neq \emptyset$ perché al suo interno c'è almeno y ed essendo un insieme finito ordinato ha un minimale c_1 tale che $c_1 \gamma x$
    - Se $c_1 = y$ poniamo $n = 1$
    - Se $c_1 \neq y$ allora $]c_1, y] \neq \emptyset$ e basta reiterare il ragionamento

Diagramma di Hasse

Definizione - Diagramma di Hasse

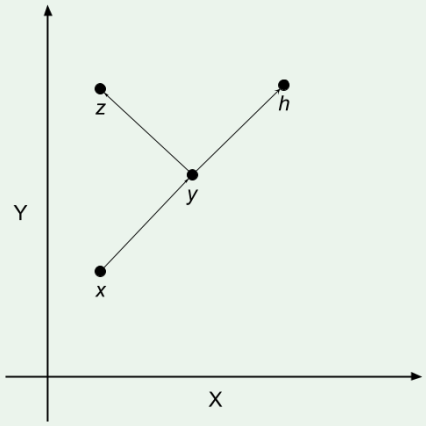
Si tratta di una tecnica per rappresentare in maniera grafica gli insiemi ordinati, permettendo di leggere a vista alcune proprietà come

- **Minimo e minimali** osservando i punti più bassi che rappresentano i minimali, se unico allora è il minimo
- **Massimo e massimale** osservando i punti più alti che rappresentano i massimali, se unico allora è il massimo

NOTA basta capovolgere il grafico per ottenere la relazione capovolta

Esempio - Diagramma di Hasse

Sia $A = \{x, y, z, h\}$ e il suo diagramma di Hasse dove tracciamo linee seguendo la relazione α

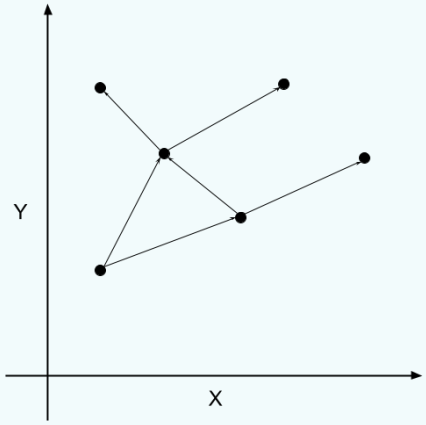


Da questo diagramma si evince che

- $x \leq y, x \leq z, x \leq h$
- $y \leq h, y \leq z$
- $h \leq h$
- $z \leq z$

Domanda - Come funziona il Diagramma di Hasse?

Immaginiamo di disegnare dei punti sul piano cartesiano ed unirli con delle linee se non si trovano alla stessa altezza, unendo i punti in questo modo abbiamo stabilito una relazione d'ordine, ovvero due punti sono in relazione quando coincidono oppure uno hanno altezze diverse, altra cosa fondamentale da ricordare è che le linee che abbiamo tracciato possono essere percorse solo dal basso verso l'alto!



Siamo sicuri che questa sia una relazione d'ordine perché

- **Riflessiva** scelto un punto A se voglio raggiungere lo stesso punto A basta non percorrere alcuna linea
- **Anti-simmetrica** scelti due punti A e B se dal punto A posso raggiungere il punto B e viceversa allora sono lo stesso punto
- **Transitiva** scelti tre punti A, B e C se dal punto A posso raggiungere il punto B e dal punto B posso raggiungere il punto C allora dal punto A posso raggiungere il punto C

Nota - Ma quindi l'ordinamento come va letto?

Secondo le regole stabilite prima, se sul Diagramma di Hasse, scelto un punto A posso raggiungere un punto B allora nel mio ordinamento avrò che $A \leq B$

Inoltre se si tratta di un insieme totalmente ordinato posso rappresentarlo con un Diagramma di Hasse tramite una linea verticale partendo dal punto più basso che rappresenta il minimo fino ad arrivare al punto più alto che rappresenta il massimo

Definizione - Isomorfismo del Diagramma di Hasse

Sia A finito e $\alpha \in OL(A)$ allora disegno sul piano cartesiano tanti punti quanti sono gli elementi dell'insieme, unisco poi con una linea due punti su altezze diverse quando il punto più alto copre quello più in basso.

Questa relazione d'ordine sul disegno e isomorfa all'insieme A rappresentando esattamente la relazione α perché due elementi x e y sono in relazione quando esiste una sequenza di elementi tali che ciascuno copra il precedente, avendo delle linee che possiamo percorrere da x fino ad arrivare a y

!ATTENZIONE! questo ci dice che due insiemi sono isomorfi quando si possono rappresentare con lo stesso Diagramma di Hasse

Esempio - Isomorfismo del Diagramma di Hasse

$(\mathbb{N}, |)$ l'insieme dei $Div(3)$ è isomorfo a $(P(\{0\}), \subseteq)$

- 1 è associato $\emptyset$
- 3 è associato a $\{0\}$

$(\mathbb{N}, |)$ l'insieme dei $Div(6)$ è isomorfo a $(P(\{0,1\}), \subseteq)$

- 1 è associato $\emptyset$
- 2 è associato a $\{0\}$
- 3 è associato a $\{1\}$
- 6 è associato a $\{0,1\}$

Nota - Non devono essere presenti linee orizzontali, ma le linee possono sovrapporsi

In un Diagramma di Hasse non devono apparire linee orizzontali, questo perché gli elementi alla stessa altezza sono sicuramenti non controntabili, ovviamente le linee che uniscono due punti possono intrecciarsi e prendere percosi "panoramici" a discrezione della sanità mentale di chi li disegna...

Anelli

Definizione - Anello

Un anello è una struttura algebrica che usa due operazioni binarie, chiamate l'addizione e la moltiplicazione dell'anello, la struttura $(R, +, \cdot)$ è un anello se:

- $+$ e $\cdot$ sono operazioni associative
- $(R, +)$ è un gruppo commutativo
- $\cdot$ è distributiva rispetto a $+$

Gli elementi neutri dell'anello sono due, uno per ogni operazione, e sono chiamati:

- **Zero dell'anello**: ovvero l'elemento neutro rispetto l'addizione, viene indicato con 0_R
- **Unità dell'anello**: ovvero l'elemento neutro rispetto la moltiplicazione, viene indicato con 1_R

Esempio - Anelli

Sono anelli $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$ ma non lo è $(\mathbb{N}, +, \cdot)$ perché $(\mathbb{N}, +)$ non è un gruppo.

Definizione - Proprietà degli Anelli

- **Anello commutativo**: $(R, +, \cdot)$ è commutativo $\Leftrightarrow$ $\cdot$ è commutativa
- **Anello unitario**: $(R, +, \cdot)$ è unitario $\Leftrightarrow$ $(R, \cdot)$ è un monoide
- **Anello integro**: $(R, +, \cdot)$ non ha divisori dello zero e vale la legge di annullamento del prodotto
- **Dominio di Integrità**: $(R, +, \cdot)$ è un anello integro commutativo
- **Anello fattoriale**: è un dominio di integrità unitario tale che $(R \setminus \{0_R\}, \cdot, 1_R)$ è un monoide fattoriale

- **Corpo**: $(R, +, \cdot)$ è un corpo se $|R| > 1$ e $\forall a \in R \setminus \{0_R\}$($a$ è invertibile)
- **Campo**: è un corpo commutativo

Nota - É sempre un anello unitario

Otterremo sempre un anello unitario con l'insieme delle parti, infatti $\forall S$ $(P(S),\ \triangle\ , \cap)$ è un anello unitario e i suoi neutri sono lo zero dell'anello $(0_{P(S)} = \emptyset)$ e l'unità dell'anello $(1_{P(S)} = S)$

Esempio - Anelli unitari

Sono anelli unitari $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$

Esempio - Dominio di integrità

$\mathbb{Z}$ è un dominio di integrità ma non un campo

Esempio - Anello fattoriale

$\mathbb{Z}$ è un anello fattoriale

Tutti i campi sono anelli fattoriali!

Esempio - Campo (anche finito)

Sia S un'insieme e $|S| = 1$ e $P(S) = \{\emptyset, S\}$ e allora $(P(S),\ \triangle\ , \cap)$ è un campo finito

Nota - Un anello integro finito è sempre un campo

Sia $(R, +, \cdot)$ un anello integro finito allora tutti i suoi elementi diversi da 0_R sono cancellabili, allora rientra nella definizione di corpo, ma tutti i corpi finiti sono campi.

Definizione - Anello opposto e Anello inverso

- **Anello opposto**: simmetrici di $(R, +)$
- **Anello simmetrico**: simmetrici di $(R, \cdot)$

Definizione - Sotto-Anello

Un sotto-anello è una parte chiusa rispetto alle operazioni indotte, quindi sia un sotto-gruppo per l'addizione e chiuso rispetto la moltiplicazione.

Nota - Non sempre i sotto-anelli conservano la proprietà unitaria

Sia $(R, +, \cdot)$ un anello e $(S, +, \cdot)$ un suo sotto-anello, allora abbiamo tre casi possibili:

1. **Conserva l'unità dell'anello**: S è un sotto-anello unitario di R perché $1_R = 1_S$
2. **Non conserva l'unità dell'anello**: S non è un sotto-anello unitario di R perché $1_R \neq 1_S$
3. **Cambia l'unità dell'anello**: S è anello unitario ma non un sotto-anello di R perché $1_{P(T)} \neq 1_{P(S)}$

Esempio - Sotto-anelli unitari

Esistono tre casi possibili:

1. $\mathbb{Z}$ in $\mathbb{Q}$ è un sotto-anello unitario
2. $\mathbb{Z} \times \mathbb{Z}$ in $\mathbb{Z}$ non è un sotto-anello
3. $T \subseteq P$ allora $P(T)$ in $P(S)$ è un anello unitario ma non un sotto-anello unitario

Definizione - Omomorfismo per anelli

L'omomorfismo ha sempre le stesse proprietà ma nel caso degli anelli vale per entrambe le operazioni.

Regole di calcolo per anelli

Definizione - Regole di calcolo per anelli

In un anello $(R, +, \cdot)$ valgono le seguenti regole

1. Dato il neutro 0_R si ha la regola $\forall a \in R(a0_R = 0_R = 0_R a)$
2. Definito $a - b := a + (-b)$ (ovvero $a +$ opposto di b) sappiamo che $\forall a, b \in R(-(ab) = (-a)b = a(-b))$
3. La distributività della moltiplicazione rispetto la sottrazione $\forall a, b \in R(a(b-c) = ab - ac \wedge (b-c)a = ba - ca)$
4. Se l'anello è unitario allora $\forall a \in R\ \forall n \in \mathbb{Z}(na = (n1_R)a)$

Teorema - Regole di calcolo per anelli

Dimostrazioni

1. Teniamo a mente che $0_R = 0_R + 0_R$ e anche $a0_R = a(O_R + 0_R) = aO_R + a0_R$ e sviluppiamo la seguente uguaglianza:

$$a0_R = a0_R + 0_R$$

$$aO_R + a0_R = a0_R + 0_R$$

$$a0_R = 0_R$$

2. Sfruttando l'associatività dimostriamo che $(-a)b$ e $a(-b)$ sono simmetrici sinistri di ab:

$$(-a)b + ab = ((-a) + a)b = O_R b = 0_R$$

$$a(-b) + ab = a((-b) + b) = a0_R = 0_R$$

3. Sfruttiamo l'associatività e la definizione di opposto per dimostrare la distributività della moltiplicazione rispetto alla sottrazione:

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

$$(b-c)a = (b + (-c))a = ba + (-c)a = ba + (-(ca)) = ba - ca$$

4. Sappiamo che l'operazione na non è interna all'anello perché $n \notin R$, quindi portiamo entrambi i membri $\in R$:

$$na = (n1_R)a = (1_R + 1_R + 1_R + 1_R + ...)a = a + a + a + a + ...$$

Legge di Annullamento del Prodotto (LAP)

Definizione - Legge di Annullamento del Prodotto

Questa legge è valida solo per gli anelli integri! Sappiamo che $\forall a, b \in R((ab = 0_R) \Rightarrow (a = 0_R \vee b = 0_R))$ ovvero $R \setminus \{0_R\}$ è chiuso rispetto a $\cdot$

Esempio - Non vale la LAP

$(P(\mathbb{N}),\ \triangle\ , \cap)\ \{1\} \cap \{2\} = \emptyset = 0_{P(\mathbb{N})}$

$(\mathbb{Z} \times \mathbb{Z}, +, \cdot)\ (0,1) \cdot (1,0) = (0,0) = 0_{\mathbb{Z}\times\mathbb{Z}}$

Divisori e Cancellabili

Teorema - Divisori dello Zero

Sia $(R, +, \cdot)$ un anello, allora $\forall a \in R$ valgono le seguenti proprietà:

- a è divisore-sinistro-dello-zero in $R \Leftrightarrow \exists b \in R \setminus \{0_R\}(ab = 0_R)$
- a è divisore-destro-dello-zero in $R \Leftrightarrow \exists b \in R \setminus \{0_R\}(ba = 0_R)$
- a è divisore-dello-zero in $R \Leftrightarrow$ vale una delle proprietà precedenti

Teorema - Cancellabilità negli Anelli

Sia $(R, +, \cdot)$ un anello, allora $\forall a \in R$ valgono le seguenti proprietà:

- a è divisore-sinistro-dello-zero in $R \Leftrightarrow a$ non è cancellabile a sinistra in $(R, \cdot)$
- a è divisore-destro-dello-zero in $R \Leftrightarrow a$ non è cancellabile a destra in $(R, \cdot)$
- a è divisore-dello-zero in $R \Leftrightarrow a$ non è cancellabile in $(R, \cdot)$

Dimostrazione solo per a divisore-sinistro-dello-zero in R perché analogamente si dimostra per il divisore-destro-dello-zero:

- $\Rightarrow$ se a divisore-sinistro-dello-zero in R allora $\exists b \in R \setminus \{0_R\}(ab = 0_R)$ e per definizione di non cancellabilità abbiamo che a non è cancellabile a sinistra perché $\exists u, v \in R(au = av \wedge u \neq v)$
- $\Leftarrow$ se a non è cancellabile a sinistra in R allora $\exists u, v \in R(au = av \wedge u \neq v)$ e per tali u e v abbiamo che $au - av = 0_R$, ovvero che $a(u - v) = 0_R$ quindi è un divisore-sinistro-dello-zero

Nota - La cancellabilità di applica sempre all'operazione $+$ negli anelli

All'interno degli anelli tutti gli elementi sono cancellabili rispetto all'operazione $+$

Teorema - Lo zero dell'anello è sicuramente divisore-dello-zero

Sia $(R, +, \cdot)$ un anello con più di un elemento, allora lo zero dell'anello è sicuramente divisore-dello-zero perché:

$$|R| > 1\ \exists b \in R \setminus \{0_R\}(0_R b = 0_R = b0_R)$$

Nota - Se l'anello ha un solo elemento l'addizione e la moltiplicazione dell'anello coincidono

Sia $(R, +, \cdot)$ un anello con la proprietà che $|R| = 1$ allora possiamo certamente dire che $+$ e $\cdot$ sono la stessa operazione.

Reticoli

Definizione - Reticoli

Sia A un'insieme e $\alpha \in OL(A)$ con (A, α), si tratta di un reticolo $\Leftrightarrow \forall x, y \in A(\exists inf\{x, y\} \wedge \exists sup(\{x, y\}))$

Reticolo completo ogni parte, di qualsiasi cardinalità, ha estremo superiore ed inferiore

Reticolo limitato se (A, α) è un reticolo con $A \neq \emptyset$ e finito (perché ha sicuramente estremo superiore ed inferiore)

Reticolo complementato A è limitato e $\forall a \in A(a$ ha almeno un complemento)

Reticolo duale basta scambiare le operazioni reticolari ovvero (A, α) $(\vee, \wedge)$ ha come duale $(A, \overset{\frown}{\alpha})$ $(\wedge, \vee)$

Reticolo distributivo ovvero se $\vee$ è distributivo rispetto a $\wedge$ e viceversa

Nota - La distributività è una proprietà puramente algebrica

Per questo motivo se si passa ad un sotto-reticolo la proprietà di distributività si trasferisce al sotto-reticolo, perché viene definita come una parte chiusa

Questo però non è sempre vero se prendiamo una parte arbitraria che è sempre un reticolo ma non un sotto-reticolo

Esempio - Reticoli distributivi

L'insieme $(\mathbb{N}^*, \mid)$ è un reticolo distributivo e tutti i sotto-reticolo formati in questo modo $\forall n \in N^*$ $Div(n)$ sono sotto-reticoli distributivi perché fanno parte di un intervallo chiuso, ovvero dei numeri coprimi fra 1 ed n

Se però prendiamo $Div(12) \setminus \{2\}$ questo è ancora un reticolo ma non più un sotto-reticolo di $Div(12)$ ed in quanto tale non distributivo (anche perché non rispetta il teorema di Birckhoff)

Domanda - Ma anche un'insieme infinito non è un Reticolo?

Stando alla definizione se si tratta il caso in cui A è finito e non ha estremo superiore o inferiore non è un reticolo ma se A fosse un'insieme infinito questo non vale, alcuni esempi sono: $(Z, \leq)$ che non ha estremo superiore o inferiore e $(\mathbb{N}^*, \mid)$ che non ha estremo superiore ma ha estremo inferiore ma entrambi sono reticoli.

Nota - Minimo e Massimo nel Reticolo e il suo duale

In un reticolo minimale e massimale sono necessariamente minimo e massimo, questo vale anche per dualità nei reticoli opposti infatti capovolgendo la relazione d'ordine e il Diagramma di Hasse si ottiene sempre un reticolo.

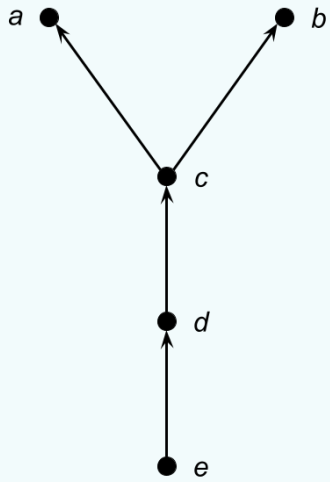
Esempio - Reticoli

- Insiemi totalmente ordinati
- $(\mathbb{N}, \mid)$
  - I maggioranti sono i multipli comuni quindi l'estremo superiore è l'MCM

  - I minoranti sono i divisori comuni quindi l'estremo inferiore è l'MCD
- $\forall S\ (P(S), \subseteq)\ \forall X \subseteq P(S)$ (sono anche reticoli completi)
  - $inf(X) = \bigcap X$
  - $sup(X) = \bigcup X$
  - Se $X = \emptyset$ allora $inf(X) = S = sup(X)$

Domanda - Come faccio a verificare se un'insieme sia un Reticolo?

Guardando il Digramma di Hasse verifichiamo che questo sia un Reticolo, ovviamente lo stiamo verificano anche per la duale perché rovesciando il diagramma invertiremmo estremo superiore e inferiore.



Per velocizzare la verifica possiamo evitare di prendere elementi che sono confrontabili tra di loro, perché ovviamente sono dotati di estremo inferiore e superiore, quindi verifichiamo soltanto gli elementi non confrontabili tra di loro.

In questo caso gli elementi a e b non sono confrontabili tra di loro e quindi vado ad osservare i minoranti e i maggioranti dai quali ricavo il massimo e il minimo, di conseguenza l'estremo superiore e inferiore.

- $\{a, b\}^{\uparrow} = \emptyset$
- $\{a, b\}^{\downarrow} = \{c, d, e\}$

Non essendoci maggioranti sappiamo che non esiste l'estremo superiore, quindi questo non è un reticolo nonostante abbiamo estremo inferiore, ovvero $inf(\{a, b\}) = max(\{a, b\}^{\downarrow}) = \{c\}$

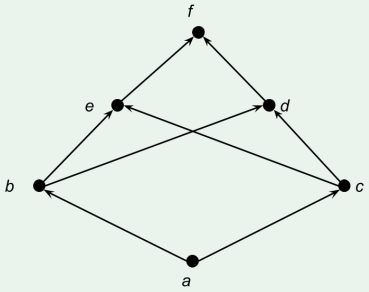
Nota - Negli insiemi ordinati più massimali e minimali implicano nessun maggiorante o minorante

Se ci troviamo in un'insieme ordinato e abbiamo due elementi distinti tra di loro, a e b, analizziamo i casi possibili

1. a e b sono entrambi massimali ma per definizione di maggiorante $\{a\}^{\uparrow} = \{a\}$ e $\{b\}^{\uparrow} = \{b\}$ ma questo però ci dice che $\{a, b\}^{\uparrow} = \{a\}^{\uparrow} \cap \{b\}^{\uparrow} = \emptyset$
2. a e b sono entrambi minimali ma per definizione di minorante $\{a\}^{\downarrow} = \{a\}$ e $\{b\}^{\downarrow} = \{b\}$ ma questo però ci dice che $\{a, b\}^{\downarrow} = \{a\}^{\downarrow} \cap \{b\}^{\downarrow} = \emptyset$

Esempio - Verificare sia un Reticolo

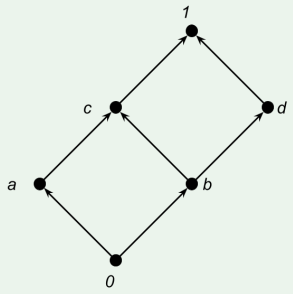
Analizzando il Diagramma di Hasse se vogliamo verificare che questo sia un Reticolo controlliamo che gli elementi non confrontabili abbiano estremo superiore ed estremo inferiore.



Possiamo notare che gli elementi b e c non sono confrontabili tra di loro quindi verifichiamo che rispettino la definizione di Reticolo

- $\{b,c\}^{\downarrow} = \{a\} = inf(\{b,c\})$
- $\{b,c\}^{\uparrow} = \{d,e,f\}$ non essendo minimo tra i maggioranti abbiamo che $\nexists sup(\{b,c\})$

Quindi questo insieme pur essendo finito ed avendo estremo superiore ed inferiore non è un Reticolo



Passando ad analizzare quest'altro Diagramma di Hasse, verifichiamo che anche questo sia un Reticolo, controlliamo come sempre soltanto gli elementi non confrontabili assicurandoci che abbiamo estremo superiore e inferiore.

Possiamo notare che gli elementi non confrontabili sono a e b, c e d quindi andiamo a verificare che queste coppie rispettino la definizione di Reticolo

- $a \wedge b = 0 = inf(\{a,b\})$
- $a \vee b = c = sup(\{a,b\})$
- $a \wedge d = 0 = inf(\{a,d\})$
- $a \vee d = 1 = sup(\{a,d\})$
- $c \wedge d = b = inf(\{c,d\})$
- $c \vee d = 1 = sup(\{c,d\})$

Questo insieme invece è finito, ha estremo superiore ed inferiore ed è anche un Reticolo

Definizione - Operazioni Reticolari

Sia (A,α) un reticolo definiamo operazioni reticolari le seguenti applicazioni

- **Unione reticolare** $\wedge : (a,b) \in A \times A \longmapsto inf(\{a,b\}) \in A$
- **Intersezione reticolare** $\vee : (a,b) \in A \times A \longmapsto sup(\{a,b\}) \in A$

Queste due applicazioni hanno le seguenti proprietà

- **Commutativa** per definizione
- **Associativa** perché $\forall a,b,c \in A$
  - $(a \wedge b) \wedge c = inf(\{a,b\}) \wedge inf(\{c\}) = inf(\{a,b,c\}) = inf(\{a\}) \wedge inf(\{b,c\}) = a \wedge (b \wedge c)$
  - $(a \vee b) \vee c = sup(\{a,b\}) \vee sup(\{c\}) = sup(\{a,b,c\}) = sup(\{a\}) \vee sup(\{b,c\}) = a \vee (b \vee c)$
- **Legge di Assorbimento** Se considero $\forall a,b \in A$
  - $a \vee b = b \Leftrightarrow a \alpha b$
  - $a \wedge b = a \Leftrightarrow a \alpha b$

Allora ottengo che $a \wedge (a \vee b) = a \wedge b = a = a \vee a = a \vee (a \wedge b)$

- **Idempotenza** $\forall a \in A(a \wedge a = a = a \vee a)$

Definizione - Sotto-Reticolo

Sia (A, α) un reticolo, sappiamo che T è un sotto-reticolo di (A, α) se $T \neq \emptyset$ ed è chiuso rispetto a $(\vee, \wedge)$

Esempio - Sotto-Reticolo

Dati i reticoli $Div(12)$ e $Div(12) \setminus \{2\}$ sappiamo che $Div(12) \setminus \{2\}$ non è un sotto-reticolo di $Div(12)$

Infatti non è una parte chiusa rispetto a $(\vee, \wedge)$ perché ad esempio

- $Div(12) : 6 \vee 4 = 2$
- $Div(12) \setminus \{2\} : 6 \vee 4 = 1$

Teorema - di Birckhoff

Un reticolo è distributivo $\Leftrightarrow$ non ha sotto-reticoli isomorfi al trirettangolo o al pentagonale

NOTA Questo ci permette di osservare dal Diagramma di Hasse se un reticolo è distributivo

Nota - Si tratta sempre di un Sotto-Reticolo

$\forall a, b \in A(a \alpha b \Rightarrow [a, b]_{(A,\alpha)})$ questo intervallo è un sotto-reticolo perché $\forall x, y \in [a, b]$ otteniamo che

- $a \in \{x, y\}^{\downarrow}$ quindi $a \leq x \vee y$
- $b \in \{x, y\}^{\uparrow}$ quindi $x \wedge y \leq b$

Questo ci porta a dire che $a \leq x \vee y \leq x \leq x \wedge y \leq b$ e concludiamo che $x \vee y, x \wedge y \in [a, b]$

In maniera del tutto analoga posso dire che $\forall a \in A(\{a\}^{\downarrow}$ e $\{a\}^{\uparrow}$ sono sotto-reticoli di $(A, \alpha))$

Teorema - In un Reticolo il minimo ed il massimo sono unici

Sia (A, α) un reticolo andiamo ad analizzare separatamente i casi di minimo e massimo

1. Sia x un elemento minimale di A allora sappiamo che $x = min(A, \alpha)$ ed è unico perché se x è minimale
   - Otteniamo che $\forall y \in A(\exists i = x \wedge y)$
   - Sappiamo quindi $i \alpha y$ e $i \alpha x$
   - Ma x è minimale quindi $i = x \Rightarrow x \alpha y$

   Concludo $\forall y \in A(x \alpha y)$ ovvero $x = min(A, \alpha)$
2. Sia x un elemento massimale di A allora sappiamo che $x = max(A, \alpha)$ ed è unico perché se x è massimale
   - Otteniamo che $\forall y \in A(\exists i = y \vee x)$
   - Sappiamo quindi $y \alpha i$ e $x \alpha i$
   - Ma x è massimale quindi $i = x \Rightarrow y \alpha x$

   Concludo $\forall y \in A(y \alpha x)$ ovvero $x = max(A, \alpha)$

Teorema - Un Reticolo finito non vuoto è un Reticolo completo

Sia (A, α) un'insieme ordinato e facciamo due supposizioni

1. Sia $X \subseteq A$ con $inf(X) = a$ quindi $X^{\downarrow} = \{a\}^{\downarrow}$
2. Sia $Y \subseteq A$ con $inf(Y) = b$ quindi $Y^{\downarrow} = \{b\}^{\downarrow}$

Allora quando vado a calcolare i minoranti ottengo $(X \cup Y)^{\downarrow} = X^{\downarrow} \cap Y^{\downarrow} = \{a\}^{\downarrow} \cap \{b\}^{\downarrow} = \{a, b\}^{\downarrow}$

Se (A, α) è un reticolo e X ed Y sono parti di A con estremo inferiore allora esiste $inf(X \cup Y) = (inf(X)) \cap (inf(Y))$, quindi ogni parte finita non vuota di (A, α) ha estremo superiore e inferiore

Concludo che un Reticolo finito non vuoto è un Reticolo completo

Nota - Un'insieme infinito non è sempre un Reticolo completo

Prendiamo in esempio il reticolo $(\mathbb{R}, \leq)$ questo non ha estremo superiore o inferiore quindi non è un Reticolo completo

Teorema - Un Reticolo può essere trattato come una struttura algebrica

Sia $f : \alpha \to (\vee, \wedge)$ che ad ogni ordinamento su A che forma un reticolo associa una coppia di operazioni binarie in A che verificano le proprietà delle operazioni reticolari

Quindi siano $\vee, \wedge : A \times A \longmapsto A$ che verificano le proprietà delle operazioni reticolari e definiamo $\leq \ Rel(A)$

$$\leq : \forall a, b \in A(a \leq b \Leftrightarrow a = a \wedge b \Leftrightarrow b = a \vee b)$$

Osserviamo che $\leq \in OL(A)$ verificandone le proprietà

- **Riflessiva** $\forall a \in A(a \leq a \Leftrightarrow a = a \wedge a)$ (vera per l'idempotenza)
- **Anti-Simmetrica** $\forall a, b \in A((a \leq b \text{ e } b \leq a) \Rightarrow (a = b) \Leftrightarrow a \wedge b = b \wedge a = a)$ (vera per la commutatività)
- **Transitiva** $\forall a, b, c \in A((a \leq b \text{ e } b \leq c) \Rightarrow (a \leq c) \Leftrightarrow a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a)$ (vera per l'associatività)

Questo ci mostra che $(\vee, \wedge)$ trasforma A in un'insieme ordinato, osserviamo se sia un reticolo $\forall a, b \in A$

- $a \wedge b \in \{a, b\}^{\downarrow}$
  - $inf(\{a, b\}) \cup inf(\{a\}) = (a \wedge b) \wedge a = (b \wedge a) \wedge a = b \wedge (a \wedge a) = b \wedge a = a \wedge b \Rightarrow a \wedge b \leq a$
  - $inf(\{a, b\}) \cup inf(\{b\}) = (a \wedge b) \wedge b = a \wedge (b \wedge b) = a \wedge b \Rightarrow a \wedge b \leq b$
- $a \vee b \in \{a, b\}^{\uparrow}$
  - $sup(\{a, b\}) \cup sup(\{a\}) = (a \vee b) \vee a = (b \vee a) \vee a = b \vee (a \vee a) = b \vee a = a \vee b \Rightarrow a \vee b \geq a$
  - $sup(\{a, b\}) \cup sup(\{b\}) = (a \vee b) \vee b = a \vee (b \vee b) = a \vee b \Rightarrow a \vee b \geq b$

Sappiamo che sicuramente esiste minorante e maggiorante ma assicuriamoci che siano estremo superiore e inferiore

- $a \wedge b = max(\{a, b\}^{\downarrow})$
  - Notiamo che $\forall c, \in \{a, b\}^{\downarrow}$ abbiamo $c \wedge a = c$ e $c \wedge b = c$ perché $c \leq a$ e $c \leq b$
  - $inf(\{c\}) \cup inf(\{a, b\}) = c \wedge (a \wedge b) = (c \wedge a) \wedge b = c \wedge b = c \Rightarrow c \leq a \wedge b$
- $a \vee b = min(\{a, b\}^{\uparrow})$

- Notiamo che $\forall s, \in \{a,b\}^{\uparrow}$ abbiamo $a \vee s = s$ e $b \vee s = s$ perché $a \leq s$ e $b \leq s$
- $sup(\{s\}) \cup sup(\{a,b\}) = s \vee (a \vee b) = (s \vee a) \vee b = s \vee b = s \Rightarrow s \geq a \vee b$

Verificato che $(A, \leq)$ è un reticolo con $(\vee, \wedge)$ come operazioni reticolari di estremo superiore e inferiore, per essere sicuri possiamo vedere se f ha un'inversa così da renderla biettiva

Se partiamo da α e usando le operazioni reticolari $(\vee, \wedge)$ possiamo arrivare ad $\leq$ in questo modo

$$\forall a, b \in A((a = a \wedge b \Leftrightarrow a \alpha b \Leftrightarrow b = a \vee b) \Leftrightarrow a \leq b)$$

Quindi questo mi dice che l'applicazione $g : (\vee, \wedge) \longmapsto \leq$ e l'inversa di f, quando effettuo le composte ottengo

- $f_o g = id_{\alpha}$
- $g_o f = id_{(\vee,\wedge)}$

Quindi $\alpha = \leq$ e grazie all'applicazione biettiva posso trattare i problemi dei reticoli come quelli di strutture algebriche

Esempio - Reticolo come struttura algebrica

In $(P(S), \subseteq)$ otteniamo che $\forall a, b \in P(S)(a \subseteq b \Leftrightarrow a = a \cap b \Leftrightarrow b = a \cup b)$

Definizione - Isomorfismo tra Reticoli

Siano reticoli (A, α) e (B, β) con le rispettive operazioni reticolari $(\vee, \wedge)$ e $(\vee', \wedge')$

Data l'applicazione biettiva $f : A \longmapsto B$ sappiamo che è un isomorfismo di insiemi ordinati quando $(A, \alpha) \longmapsto (B, \beta) \Leftrightarrow$ è un isomorfismo di strutture algebriche $(A, \vee, \wedge) \longmapsto (B, \vee', \wedge')$

Ovvero quando succede che $\forall a, b \in A(a \ \alpha \ b \Leftrightarrow f(a) \ \beta \ f(b))$ e otteniamo che

- $f : a \vee b \longmapsto f(a) \vee' f(b)$
- $f : a \wedge b \longmapsto f(a) \wedge' f(b)$

Minimo e Massimo nel Reticolo

Definizione - Minimo e Massimo

Sia (A, α) un'insieme ordinato e $(\vee, \wedge)$ le operazioni reticolari abbiamo che

- $\forall a \in A(a = min(A, \alpha) \Leftrightarrow \forall b \in A(a \alpha b) \Leftrightarrow \forall b \in A(b = a \vee b) \Leftrightarrow a$ è neutro rispetto a $\vee)$
- $\forall a \in A(a = max(A, \alpha) \Leftrightarrow \forall b \in A(b \alpha a) \Leftrightarrow \forall b \in A(b = a \wedge b) \Leftrightarrow a$ è neutro rispetto a $\wedge)$

Esempio - Minimo e Massimo nel Reticolo

In $P(A)$ abbiamo

- $min = \emptyset$ che è neutro rispetto a $\vee$
- $max = A$ neutro rispetto a $\wedge$

In $(\mathbb{N}, \ | \ )$ abbiamo

- $min = 1$ neutro rispetto alla scelta dell'MCD

- $max = 0$ neutro rispetto alla scelta dell'MCM

Complemento

Definizione - Complemento

Sia A un'insieme limitato con (A, α) reticolo con operazioni reticolari $(\vee, \wedge)$, posto $0 = min(A, \alpha)$ e $1 = max(A, \alpha)$ definisco due elementi complementari quando

$$\forall a \in A(\exists b \in A(a \text{ è complemento di } b \Leftrightarrow a \wedge b = 0 \Leftrightarrow a \vee b = 1 \Leftrightarrow b \text{ è complemento di } a))$$

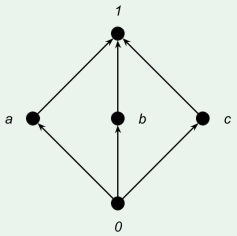
NOTA 0 è l'unico complemento di 1 è viceversa.

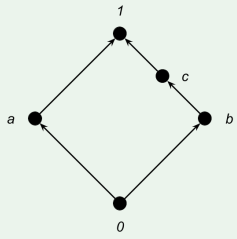
Esempio - Reticoli Complementati

Analizzando il Diagramma di Hasse se vogliamo verificare questo sia un Reticolo complementato controlliamo che gli elementi non confrontabili siamo complementati

- a è complemento di b e c
- b è complemento di a e c
- c è complemento di a e b

NOTA questa figura è chiamata Trirettangolo





Analizzando quest'altro Diagramma di Hasse per effettuare la verifica se sia un Reticolo complementato osserviamo che ci sono più elementi confrontabili, e quindi meno verifiche da effettuare per capire se gli elementi sono complementari

- a è complemento di b e c
- b è complemento di a
- c è complemento di a

NOTA questa figura è chiamata pentagonale

$Div(12)$ non è un reticolo complementato perché abbiamo come esempio

- $2 \wedge 12 = 12 = max(Div(12))$
- $2 \vee 12 = 2 \neq min(Div(12))$

Ma essendo 2 e 12 confrontabili potevamo velocizzare il processo cercando tra gli elementi non confrontabili con 2, come ad esempio 3 e ci saremmo accertati prima che non era un reticolo complementato

Domanda - Come velocizzo la verifica di Reticoli complementati?

Sia (A, α) un reticolo e $\forall a, b \in A(a \text{ e } b \text{ sono confrontabili} \Rightarrow (a \text{ è complemento di } b \Leftrightarrow \{a, b\} = \{min(A), max(A)\}))$

Quindi nel caso due elementi siano confrontabili e non siano il minimo è il massimo non ha senso valutare se sono complementati, bisogna invece guardare gli elementi non confrontabili per velocizzare la ricerca del complemento.

Nota - (A, α) se è totalmente ordinato, non sempre è un reticolo complementato

Se (A, α) è totalmente ordinato allora è un reticolo complementato $\Leftrightarrow 0 < |A| \leq 2$ perché gli elementi sono tutti confrontabili tra loro e gli unici complementati sono $min(A, \alpha)$ e $max(A, \alpha)$

Teorema - Un Reticolo distributivo limitato per ogni elemento ha al massimo un complemento

Sia A limitato e $(A, \leq, \vee, \wedge)$ un reticolo distributivo sappiamo che $\forall a \in A$ a ha al massimo un complemento

Dimostrazione $\forall a \in A$ siano b e c complementi di a per i quali considero

- $b \vee a = 1 = max(A, \leq)$
- $a \wedge c = 0 = min(A, \leq)$

Allora se vado ad osservare come è composto ogni elemento ottengo che

- $b = b \vee 0 = b \vee (c \wedge a) = (b \vee c) \wedge (b \vee a) = (b \vee c) \wedge 1 = b \vee c$
- $c = c \vee 0 = c \vee (a \wedge b) = (c \vee b) \wedge (c \vee a) = (c \vee b) \wedge 1 = c \vee b$

Concludo che per la proprietà commutatività $(b \vee c = c \vee b) \Rightarrow (c = b)$

Nota - $P(A)$ è sempre un reticolo complementato

$\forall A$ sappiamo che $P(A)$ ha $min(P(A)) = \emptyset$ e $max(P(A)) = A$ inoltre è un reticolo complementato perché $\forall x \in P(A)$

- $x \cap (A \setminus x) = \emptyset = min(P(A))$
- $x \cup (A \setminus x) = A = max(P(A))$

Quindi $A \setminus x$ è il complemento di x (il nome "complementare" viene da questa nozione)

Reticoli Booleani, Algebra di Boole e Anelli Booleani

Definizione - Reticolo Booleano

Sia (A, α) un reticolo, questo è detto booleano $\Leftrightarrow$ è distributivo e complementato

NOTA Ogni elemento ha esattamente un solo complemento perché distributivo e complementato

Esempio - Reticolo Booleano

$\forall S$ $(P(S), \subseteq)$ è distributivo e complementato, infatti $\forall x \in P(S)(S \setminus x$ è l'unico complemento di $x)$

Anche $(Div(6), |)$ e $(P(\{0, 1\}), \subseteq)$ sono reticoli complementati è distributivi (Teorema di Birckhoff)

Algebra di Boole

Definizione - Algebra di Boole

L'Algebra di Boole è una struttura algebrica $(B, \vee, \wedge, 0, 1, ')$ struttura in questo modo

- $\vee$ e $\wedge$ operazioni binarie (reticolari)
- 0 e 1 neutri associati alle operazioni binarie (minimo e massimo)
- $'$ operazione unaria (complementi)

Questa struttura viene definita seguendo queste regole

1. $(B, \vee, 0)$ e $(B, \wedge, 1)$ sono monoidi commutativi
2. Leggi di Assorbimento $\forall a, b \in B(a \vee (b \wedge a) = a = a \wedge (b \vee a))$
3. Distributività
4. Definizione dei complementi $\forall a \in B(a \wedge a' = 0$ e $a \vee a' = 1)$

NOTA Le regole ① e ② formano un reticolo limitato, ③ lo rende distributivo e ④ booleano

Algebra di Boole duale Basta scambiare le operazioni reticolari e minimo e massimo

Nota - Algebra di Boole è isomorfa con la sua duale

Sappiamo che B e $\overleftarrow{B}$ sono isomorfe perché esiste l'applicazione $x \in B \longmapsto x' \in \overleftarrow{B}$ che è biettiva perché $a'' = a$

Nota - L'Algebra di Boole è equivalente a un Reticolo Booleano

Infatti partendo da un'Algebra di Boole $(B, \vee, \wedge, 0, 1, ')$ possiamo definire un Reticolo Booleano $(B, \leq)$ in questo modo

$$\forall a, b \in B(a \leq b \Leftrightarrow a = a \wedge b \Leftrightarrow b = a \vee b)$$

Domanda - Quali sono le identità nell'Algebra di Boole?

Sia $(B, \vee, \wedge, 0, 1, ')$ sappiamo che valgono le seguenti identità

- $\forall a \in B(a'' = a)$ perché essendo equivalente ad un reticolo booleano, il complemento è unico
- $\forall a, b \in B(a \wedge 0 = 0$ e $a \vee 1 = 1)$ perché essendo un reticolo booleano è limitato
- $\forall a, b \in B((a \wedge b)' = a' \vee b'$ e $(a \vee b)' = a' \wedge b')$ De Morgan

Dimostrazione (De Morgan) essendo che vale l'unicità del complemento dimostriamolo

- $(a \wedge b)' = a' \vee b'$
  - **Intersezione Reticolare**
    $(a \wedge b)' \wedge (a' \vee b') = a \wedge (b \wedge (a' \vee b')) = a \wedge ((b \wedge a') \vee (b \wedge b')) = a \wedge (b \wedge a') = b \wedge (a \wedge a') = b \wedge 0 = 0$
  - **Unione Reticolare**
    $(a \wedge b)' \vee (a' \vee b') = ((a \wedge b) \vee a') \vee b' = ((a \vee a') \wedge (b \vee a')) \vee b' = (b \vee a') \vee b' = a' \vee (b \vee b') = a' \vee 1 = 1$
- $(a \vee b)' = a' \wedge b'$
  - **Intersezione Reticolare**
    $(a \vee b)' \wedge (a' \wedge b') = ((a \vee b) \wedge a') \wedge b' = ((a \wedge a') \vee (b \wedge a')) \wedge b' = (b \wedge a') \wedge b' = (b \wedge b') \wedge a' = 0 \wedge a' = 0$

- **Unione Reticolare**
  $(a \vee b) \vee (a' \wedge b') = a \vee (b \vee (a' \wedge b')) = a \vee ((b \vee a') \wedge (b \vee b')) = a \vee (b \vee a') = b \vee (a \vee a') = b \vee 1 = 1$

Nota - Quale oggetto matematico studiare?

Fino ad ora abbiamo i seguenti oggetti matematici

- $(P(S), \subseteq)$ reticolo booleano
- $(P(S), \vee, \wedge)$ reticolo come struttura algebrica (anello)
- $(P(S), \vee, \wedge, \emptyset, S, ')$ algebra di boole

Possiamo affermare che studiare uno di questi tre oggetti è perfettamente equivalente

Definizione - Omomorfismo e Isomorfismo tra Algebre di Boole

Siano $(B, \vee, \wedge, 0, 1, ')$ e $(C, \cup, \cap, \overline{0}, \overline{1}, ^*)$ due Algebre di Boole e sia $f : B \longmapsto C$ un omomorifsmo deve conservare

- **Unione reticolare** $f(x \vee y) = f(x) \cup f(y)$
- **Intersezione reticolare** $f(x \wedge y) = f(x) \cap f(y)$
- **Elementi neutri** $f(0) = \overline{0}$ e $f(1) = \overline{1}$
- **Complemento** $f(x') = f(x)^*$

Isomorfismo è un'omomorfismo biettivo

Definizione - Sotto-Algebra di Boole

Una parte chiusa rispetto a tutte le operazioni, ovvero unione e intersezione reticolare, scelta del complemento

Esempio - Sotto-Algebra di Boole

Data l'Algebra di Boole $(P(S), \vee, \wedge, \emptyset, S, ')$ e sia $T \subset S$ sappiamo che $(P(T), \vee, \wedge, \emptyset, T, ')$ non è una Sotto-Algebra di Boole perché non hanno lo stesso massimo

Notiamo che $P(\mathbb{N})$ non è una Sotto-Algebra di Boole (mentre è un sotto-reticolo) di $P(\mathbb{Z})$ perché non è chiusa rispetto al complemento, infatti

- In $P(\mathbb{N})$ abbiamo che $\{1\}' = \mathbb{N} \setminus \{1\}$
- In $P(\mathbb{Z})$ abbiamo che $\{1\}' = \mathbb{Z} \setminus \{1\}$

Anelli Booleani

Definizione - Anello Booleano

Un anello unitario in cui tutti gli elementi sono idempotenti (ovvero $x^2 = x$)

Esempio - Anello Booleano

$(P(S), \triangle, \cap)$ è un anello booleano, cioè un anello unitario dove ogni elemento è idempotente $(\forall x \in P(S)(x \cap x = x)$

Teorema - Negli anelli booleani vale l'idempotenza

Sia $(R, +, \cdot)$ un anello booleano, allora R è commutativo e $\forall a \in R(2a = a + a = 0_R)$ (ovvero $\forall a \in R(-a = a)$).

Dimostrazione $\forall a, b \in R$ abbiamo che $a^2 = a$ poi $b^2 = b$ infine $(a + b)^2 = a + b$.

Svolgendo il quadrato abbiamo che $(a + b)^2 = a^2 + ab + ba + b^2$ ma per le proprietà enunciate sopra riscriviamo $(a + b)^2 = a + ab + ba + b = a + b + (ab + ba)$, quindi deduciamo che $ab + ba = 0_R$, ovvero $-(ab) = ba$.

Ovvero R è commutativo quindi $ab = y = ba$, ma per la proprietà enunciata sopra abbiamo che $2y = y + y = 0_R$.

Concludiamo quindi che $\forall a, b \in R(ab = -(ab) = ba)$, ma questo deve valere anche quando gli elementi sono uguali quindi $\forall a \in R(-a = -a^2 = -(aa) = aa = a^2 = a)$.

Teorema - Stone

Questo teorema ci dice due cose:

1. Sia $(R, +, \cdot)$ un anello booleano, esiste un insieme S tale che R sia isomorfo ad un sotto-anello unitario di $(P(S), \triangle, \cap)$.
2. Sia $(R, +, \cdot)$ un anello booleano finito, esiste un insieme S tale che $R \simeq (P(S), \triangle, \cap)$.

Domanda - Come conto gli elementi di un anello booleano finito?

Sia $(R, +, \cdot) \simeq P(S)$ allora esiste un'applicazione biettiva che rende gli insiemi equipotenti, cioè $\exists n \in \mathbb{N}(|R| = 2^n)$.

Siano $(R, +, \cdot)$ e $(A, +, \cdot)$ due anelli booleani finiti mentre S e T due insiemi equipotenti tra loro, sappiamo che $R \simeq P(S)$ e $A \simeq P(T)$.

Visto che $|S| = |T|$ allora esiste un'applicazione biettiva da $f : S \longmapsto T$, quindi anche $\overrightarrow{f} : P(S) \longmapsto P(T)$ è biettiva, questo ci dice che $R \simeq A$.

Nota - Isomorfismo e parte chiusa nel caso degli anelli booleani

Essendo che si può passare da una struttura all'altra senza perdita di informazioni sappiamo

- Isomorfismo tra algebre di boole conserva le operazioni reticolari, ma quindi anche le operazioni dell'anello
- Sotto-algebra di boole e chiusa rispetto alle operazioni, conserva i complementi
- Vale il Teorema di Stone per algebre di boole e reticoli booleani

Passare da una struttura all'altra

Domanda - Come passo da un Anello Booleano ad un Algebra di Boole?

Sia $(R, +, \cdot, 0_R, 1_R)$ un anello booleano e usiamo la moltiplicazione dell'anello $(\cdot)$ per l'intersezione reticolare $(\wedge)$ mentre per l'unione reticolare $(\vee)$ dobbiamo sfruttare le due operazioni dell'anello

Per definire l'unione reticolare facciamo guidare dall'esempio dell'anello dell'insieme delle parti

$$\text{In } (P(S), \triangle, \cap, \emptyset, S) \text{ l'unione è così definita } A \vee B = A \cup B = (A \triangle B) \triangle (A \cap B)$$

Quindi definiamo l'unione reticolare $(\vee)$ in R con la seguente applicazione $\vee : (a, b) \in R \longmapsto a + b + ab \in R$

Verifichiamo che la struttura $(R, \vee, \wedge, 0_R, 1_R, ')$ sia un'Algebra di Boole

- $(R, \vee, 0_R)$ e $(R, \wedge, 1_R)$ siano monoidi commutativi
  - **Commutatività**
    - $(R, \vee, 0_R)$ l'addizione $(+)$ e la moltiplicazione $(\cdot)$ dell'anello sono già commutative
    - $(R, \wedge, 1_R)$ la moltiplicazione $(\cdot)$ dell'anello booleano è già commutativa
  - **Associatività**
    - $(R, \vee, 0_R)$ $\forall a, b, c \in R((a \vee b) \vee c = a + b + ab + c + ac + bc + abc = a \vee (b \vee c))$
    - $(R, \wedge, 1_R)$ la moltiplicazione $(\cdot)$ dell'anello booleano è già associativa
  - **Neutro**
    - $(R, \vee, 0_R)$ $\forall a \in R(a \vee 0_R = a)$
    - $(R, \wedge, 1_R)$ la moltiplicazione $(\cdot)$ dell'anello booleano ha già neutro
- **Distributività** (Legge di idempotenza)
  - $\wedge$ sia distributivo rispetto a $\vee$
    - $\forall a, b, c \in R(a \wedge (b \vee a) = a \cdot (b + c) = a \cdot (b + c + bc) = ab + ac + abc = (a \wedge b) \vee (a \wedge c))$
  - $\vee$ sia distributivo rispetto a $\wedge$
    - $\forall a, b, c \in R(a \vee (b \wedge c) = a + (b \cdot c) = a + bc + abc = (a + b + ab) \cdot (a + c + ac) = (a \vee b) \wedge (a \vee c))$
- **Legge di Assorbimento** (Legge di idempotenza)
  - $\forall a, b \in R(a \vee (a \wedge b) = a + (a \cdot b) = a + ab + a^2 b = a)$
  - $\forall a, b \in R(a \wedge (a \vee b) = a \cdot (a + b) = a^2 + ab + a^2 b = a)$
- **Complemento**
  - Per definire il complemento ci rifacciamo all'analogia con l'anello dell'insieme delle parti

    In $(P(S), \triangle, \cap, \emptyset, S)$ definiamo la differenza simmetrica come $S \setminus x = S \triangle x = 1_{P(S)} \triangle x$

    Quindi definiamo l'applicazione $' : a \in R \longmapsto 1_R + a \in R$
    - $\forall a \in R(a \vee a' = a + a' + aa' = a + (1_R + a) + 0_R = a + a = 1_R)$
    - $\forall a \in R(a \wedge a' = a \cdot a' = a(1_R + a) = a + a^2 = a + a = 0_R)$

Concludo che $(B, \vee, \wedge, 0, 1, ')$ è un algebra di boole

Domanda - Come passo da un Algebra di Boole ad un Anello Booleano?

Sia $(B, \vee, \wedge, 0, 1, ')$ un algebra di boole, allora definiamo l'operazione additiva dell'anello aiutandoci sempre con l'analogia dell'insieme delle parti

$$\forall a, b \in P(S)(a \triangle b = (a \cup b) \setminus (a \cap b) = (a \setminus b) \cup (b \setminus a))$$

Verifichiamo che la definizione di differenza simmetrica funzioni

$$\forall a, b \in R((a \vee b) \wedge (a \wedge b)' = (a \wedge b') \vee (b \wedge a') =: a + b)$$

Concludo che $(R, +, \wedge, 0_R, 1_R)$ è un anello booleano

Nota - Stesso oggetto con tre linguaggi differenti

In analogia all'insieme delle parti abbiamo i seguenti punti di vista che ci permettono di passare da una struttura all'altra senza perdere informazioni analizziando un problema con differenti punti di vista

Sintassi	Operazioni	Struttura
$(P(S), \vee, \wedge, \emptyset, S, ')$	$\vee$ e $\wedge$	Algebra di Boole
$(P(S), \triangle, \cap, \emptyset, S)$	$\triangle$ e $\cap$	Anello Booleano
$(P(S), \subseteq)$	$\subseteq$	Reticolo Booleano

Operazioni bit a bit

Definizione - Prodotto diretto tra anelli

Preso il prodotto cartesiano tra anelli definiamo il prodotto diretto tra anelli come un'operazione componente per componente, prendendo una n-upla finita di elementi che indichiamo con R^n definita da $\forall n \in \mathbb{N}^* \; R^n = R \times R \times ... \times R$

NOTA Negli anelli booleani vale l'idempotenza per i suoi elementi, quindi il risultato è ancora un anello booleano

Esempio - Prodotto cartesiano tra Anelli

$\mathbb{Z}_2^5 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = ([0]_2, [0]_2, [1]_2, [0]_2, [1]_2)$

In questo caso possiamo riscrivere la n-upla come 00101 ricordandoci però che questi sono elementi di $\mathbb{Z}_2$ e la loro lunghezza rappresenta quella della n-upla

Definizione - Isomorfismo definito dalla funzione caratteristica

Sia $S = \{1, 2, 3, 4, 5\}$ ad ogni parte associamo la sua funzione caratteristica vista come che la n-upla in $\mathbb{Z}_2$

Il Teorema di Stone ci dice che $\mathbb{Z}_2 \simeq (P(S), \triangle, \cap)$ e quindi

- $+$ in $\mathbb{Z}_2 = \triangle$ in S
- $\cdot$ in $\mathbb{Z}_2 = \cap$ in S

Nota - Le operazioni dell'anello di $\mathbb{Z}_2$ sono le operazioni bit a bit

Prendiamo ad esempio l'addizione e ricordiamo che fanno parte dell'insieme quoziente

$$\begin{array}{ccccccc} 0 & 0 & 1 & 0 & 1 & + \\ 1 & 0 & 0 & 1 & 1 & = \\ \hline 1 & 0 & 1 & 1 & 0 & \end{array}$$

Analogamente possiamo prendere in esempio la moltiplicazione

$$\begin{array}{ccccccc} 0 & 0 & 1 & 0 & 1 & \cdot \\ 1 & 0 & 0 & 1 & 1 & = \\ \hline 0 & 0 & 0 & 0 & 1 & \end{array}$$

Ma noi sappiamo che usando la funzione caratteristica otteniamo

- $\{3, 5\} \to 00101$

- $\{1,4,5\} \to 10011$
- $\{1,3,4\} \to 10110$
- $\{5\} \to 00001$

Confermiamo l'isomorfismo con il Teorema di Stone osservando le operazioni dell'anello delle parti

- $\{3,5\} \triangle \{1,4,5\} = \{1,3,4\}$
- $\{3,5\} \cap \{1,4,5\} = \{5\}$

Da qui possiamo vedere la corrispondenza tra le operazioni delle due strutture

Polinomi

Definizione - Anelli di Polinomi

Sia A un anello commutativo unitario con $|A| > 1$ (così da non risultare vuoto o con solo lo 0_A), chiamiamo $A[x]$ l'anello commutativo unitario di polinomi su A ad una sola indeterminata con le seguenti proprietà

- A è un sotto-anello unitario di $A[x]$ (in modo che abbiano la stessa 1_A)
- $x \in A[x]$
- $\forall P \in A[X](\exists!(a_i)_{i\in\mathbb{N}} \in Map(\mathbb{N}, A)(\exists n \in \mathbb{N}(P = a_o + a_1 x + \ldots + a_n x^n = \sum_{i=0}^{n} a_i x^i) \wedge \forall i \in \mathbb{N}(i > n \Rightarrow a_i = 0_A)))$

Gli elementi di $A[x]$ sono chiamati polinomi a coefficienti su A mentre $(a_i)_{i\in\mathbb{N}}$ è detta successione dei coefficienti di P

NOTA se A è nullo i coefficienti sono tutti 0 ottenendo una successione $(0_A, 0_A, 0_A, 0_A, 0_A, \ldots)$

Esempio - Polinomi

Osserviamo il caso di $P = 3x^5 + 2x^2 + 1 = \sum_{i=0}^{5} a_i x^i \wedge \forall i \in \mathbb{N}(i > 5 \Rightarrow a_i = 0)$

Nota - Gli elementi delle successioni sono infiniti

Possiamo evitare di scrivere ogni elemento della successione essendo che ha un numero finito di elementi diversi da 0_A

Domanda - In quanti modi posso scrivere un polinomio?

Se $|A| > 1$ sappiamo che $A[x]$ è infinito perché tutte le potenze di x corrispondono a successioni diverse (dove anche gli elementi di A appaiono in posizioni diverse) e per ogni elemento di A esiste una successione che lo realizza che ha questa forma

$$\forall a \in A \ (a, 0_A, 0_A, 0_A, 0_A, \ldots)$$

NOTA l'elemento a_0 si chiama termine noto di P

Esiste anche una successione che realizza $x = \sum_{i=0}^{n} a_i x^i$ che conferma $x \notin A$ perché sennò avremmo due modi di scriverlo

$$x = \begin{cases} (0_A, x, 0_A, 0_A, 0_A, \ldots) \\ (x, 0_A, 0_A, 0_A, 0_A, \ldots) \end{cases}$$

!ATTENZIONE! essendo $x \notin A$ il secondo modo è la successione errata per rappresentare x

Definizione - Grado e Coefficiente Direttore

Sia $P \in A[x] \setminus \{0_A\}$ e $(a_i)_{i \in \mathbb{N}}$ la successione dei coefficienti di P allora sappiamo che $S_P = \{i \in \mathbb{N} \mid a_i \neq 0_A\}$

Essendo $S_P \neq 0_A$ e finito so che esistono

- **Grado del Polinomio** $max(P) = \nu(P)$
- **Coefficiente Direttore** $a_{\nu(P)} = cd(P)$

Con l'ausilio del Grado del Polinomio e del Coefficiente Direttore possono individuare diversi tipi di polinomi

- **Polinomio Nullo** si tratta di 0_A dove per convenzione definiamo $\nu(0_A) = -\infty$ e $cd(0_A) = 0_A$
- **Polinomio Costante** ovvero gli elementi di A
- **Polinomio Monico** quando $cd(P) = 1_A$

Esempio - Grado e Coefficiente Direttore

Prendiamo in esempio i seguenti polinomi

- $1 + 3x^2 + 4x^3 \in \mathbb{Z}[x]$
  - Ha grado 3
  - Ha coefficiente direttore 4
- $1 + 3x^3 + 4x^3 + 0x^5 \in \mathbb{Z}[x]$
  - Ha grado 3
  - Ha coefficiente direttore 4
- $\overline{1} + \overline{17}x^4 + \overline{51}x^6 \mathbb{Z}_3[x]$
  - Ha come grado 4
  - Ha coefficiente direttore $\overline{17} \in Z_3$

Possiamo dire che 37 è un polinomio costante in $\mathbb{R}[x]$

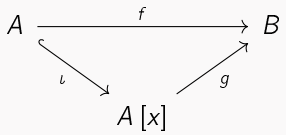
Mentre $\overline{1} + \overline{16}x^4 \in \mathbb{Z}_3[x]$ è un polinomio monico

NOTA tutti i polinomi non nulli in $\mathbb{Z}_2$ sono polinomi monici

Definizione - Proprietà Universale

Sia A anello commutativo unitario non nullo e B un anello commutativo unitario con $c \in B$

Dato l'omomorfismo di anelli unitari $f : A \longmapsto B$ e $A[x]$ anello di polinomi su A otteniamo che



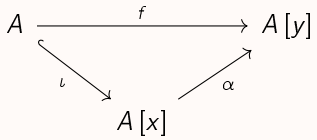
Da questo diagramma possiamo ricavare che ι è l'immersione di A in $A[x]$ ma soprattutto che

$$\forall c \in B(\exists! g(\text{omomorfismo di anelli unitari } A[x] \longmapsto B(g_{|A} = f \text{ e } g(x) = c)))$$

Viene poi così definita $g : \sum_{i=0}^{n} a_i x^i \in A[x] \longmapsto \sum_{i=0}^{n} f(a_i)c^i \in B$

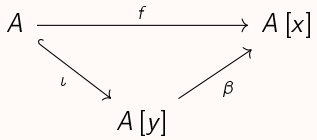
Teorema - L'anello dei polinomi è unico a meno di isomorfismi

Siano $A[x]$ e $A[y]$ anelli di polinomi su A e osservando lo stesso diagramma precedente scelgo $B = A[y]$ e $c = y$



Definendo l'omomorfismo come segue $\alpha : \sum_{i=0}^{n} a_i x^i \in A[x] \longmapsto \sum_{i=0}^{n} a_i y^i \in A[y]$

Similmente posso applicare il ragionamento inverso, scelgo $B = A[x]$ e $c = x$ ottenendo il seguente diagramma

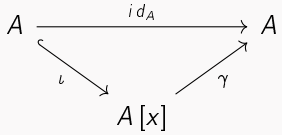


Definendo l'omomorfismo come segue: $\beta : \sum_{i=0}^{n} a_i y^i \in A[y] \longmapsto \sum_{i=0}^{n} a_i x^i \in A[x]$

Concludo che $\alpha^{-1} = \beta$ quindi α è un isomorfismo e quindi l'anello è unico (nonostante il cambio di indeterminata)

Definizione - Omomorfismo di sostituzione

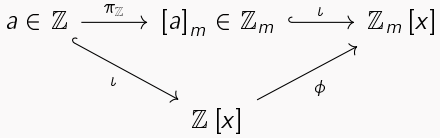
$\forall c \in A$ sia l'applicazione $\gamma : P \in A[x] \longmapsto P(c) \in A$ un omomorfismo di anelli detto "omomorfismo di sostituzione"



Definendo l'omomorfismo come segue: $\gamma : \sum_{i=0}^{n} a_i x^i \in A[x] \longmapsto \sum_{i=0}^{n} a_i c^i \in A$

Definizione - Omomorfismo di sostituzione con la Classe di Resto

$\forall m \in \mathbb{N}^*$ con $c = x$ sia l'applicazione $\phi : P \in \mathbb{Z}[x] \longmapsto \overline{P} \in \mathbb{Z}_m[x]$ un omomorfismo di anelli



Definendo l'omomorfismo come segue: $\phi : \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x] \longmapsto \sum_{i=0}^{n} [a_i]_m x^i \in \mathbb{Z}_m[x]$

Esempio - Omomorfismo di sostituzione con Classe di Resto

Sia $m = 3$ e dato il polinomio $P = x^7 + 5x^4 - 8^3 + 3x + 1$ se eseguiamo $\phi(P) = x^7 + \overline{2}x^4 + x^3 + \overline{1}$

Operazioni tra Polinomi

Definizione - Somma

Siano $P, R \in A[x] \setminus \{0_A\}$ con $P = \sum_{i=0}^{n} a_i x^i$ e $R = \sum_{i=0}^{n} b_i x^i$ definiamo la somma tra due polinomi in questo modo

$$P + R = (a_0 + b_0) + (a_1 + b_1)x^1 + (a_2 + b_2)x^2 + ... + (a_k + b_k)x^k \text{ con } k = max(\nu(P), \nu(R))$$

Indichiamo inoltre con $n = \nu(P)$ e $m = \nu(R)$ e osserviamo i tre casi in cui la somma modifica il grado del polinomio

1. $\nu(P + R) \leq max(n, m)$ perché la somma di due polinomi non può avere un grado maggiore dei polinomi stessi
2. $\nu(P+R) = max(n, m) \Leftrightarrow a_n + b_m \neq 0_A$ il grado della somma è il massimo tra i polinomi se il $cd(P) + cd(R) \neq 0_A$
3. $\nu(P) \neq \nu(R) \Rightarrow \nu(P + R) = max(n, m)$ il grado della somma è il massimo tra i polinomi con grado diverso

NOTA nel caso della sottrazione (che è sempre una somma) otteniamo due casi distinti

1. $\nu(P - R) = max(n, m)$ quando $n \neq m$ oppure se $n = m$ ma abbiamo che $cd(P) \neq cd(R)$
2. $\nu(P - R) < max(n, m)$ quando $n = m$ ed anche $cd(P) = cd(R)$

Esempio - Somma tra Polinomi

Prendiamo in esempio le somme tra questi polinomi

- $(3x^2 + 1) + (4x^5 + 1)$ ha grado 5
- $(3x^2 + 1) + (3x^2 + 1)$ ha grado 3
- $(3x^2 + 1) + (-3x^2 + x)$ ha grado 1

Definizione - Prodotto

Siano $P, R \in A[x] \setminus \{0_A\}$ con $P = \sum_{i=0}^{n} a_i x^i$ e $R = \sum_{i=0}^{n} b_i x^i$ definiamo il prodotto tra due polinomi in questo modo

$$P \cdot R = (a_0 \cdot b_0) + (a_1 \cdot b_0 + a_0 \cdot b_1)x^1 + (a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2)x^2 + ... + (a_k + b_k)x^k \text{ con } k = max(\nu(P), \nu(R))$$

Indichiamo inoltre con $n = \nu(P)$ e $m = \nu(R)$ e osserviamo i tre casi in cui il prodotto modifica il grado del polinomio

1. $\nu(P \cdot R) \leq n + m$
2. $\nu(P \cdot R) < n + m \Leftrightarrow a_n \cdot b_m = 0_A$
3. $\nu(P + R) = n + m \Leftrightarrow a_n \cdot b_m \neq 0_A$

Regola di Addizione dei Gradi (RAG)

Definizione - Regola di Addizione dei Gradi

La Regola di Addizione tra Gradi dice che presi $P, R \in A[x]$ valgono le seguenti formule

- $\nu(P \cdot R) = \nu(P) + \nu(R)$
- $cd(P \cdot R) = cd(P) \cdot cd(R)$

Quando si verifica una tra le seguenti condizioni

1. Se uno tra P e R è il polinomio nullo
2. Se uno tra P e R ha coefficiente direttore cancellabile (non divisore dello zero)

Esempio - Regola di Addizione dei Gradi

Sia $H = \overline{2}x + \overline{1} \in \mathbb{Z}_4[x]$ effettuiamo il prodotto $H \cdot H$

$H \cdot H = H^2 = \overline{2}x^2 + \overline{2}x + \overline{1}^2 = \overline{4}x^2 + \overline{4}x + \overline{1} = 1$

Quindi in questo caso non si applica la RAG quando moltiplichiamo il polinomio per se stesso, partendo da un grado 1 abbiamo ottenuto un grado 0

Teorema - $cd(P)$ cancellabile in $A \Rightarrow P$ cancellabile in $A[x]$

Sia $\forall P \in A[x](cd(P)$ cancellabile in $A \Rightarrow P$ cancellabile in $A[x])$

Dimostrazione

Se l'ipotesi è vera allora $\forall R \in A[x] \setminus \{0_A\}$ vale la RAG per $P \cdot R$

Se $P = 0_A$ allora $cd(P) = 0_A$ e quindi divisore dello zero, ma questo è impossibile per l'ipotesi

Concludo che $P \neq 0_A$ e quindi cancellabile, allora $P \cdot R \neq 0_A$ e vale $\nu(P \cdot R) = \nu(P) + \nu(R) \geq 0_A$

Teorema - A dominio di integrità $\Rightarrow A[x]$ dominio di integrità

Sono equivalenti le seguenti affermazioni

1. A è un dominio di integrità
2. In $A[x]$ vale la RAG perché $\forall P, R \in A[x](\nu(P \cdot R) = \nu(P) + \nu(R))$
3. $A[x]$ è un dominio di integrità
4. $U(A[x]) = U(A)$

Dimostrazione

1. Un sotto-anello di un anello integro è sempre integro
2. Se è sempre valida la RAG allora $\forall P, R \in A[x] \setminus \{0_A\}$ allora $\nu(P \cdot R) = \nu(P) + \nu(R) \geq 0_A$ quindi $P \cdot R \neq 0_A$
3. Preso $P \in A[x]$ abbiamo due casi
   (a) $P = 0_A$ allora vale la RAG

(b) $P \neq 0_A$ allora $cd(P) \neq 0_A$ ma essendo A un dominio di integrità $cd(P)$ è cancellabile e vale la RAG

4. Preso $\forall P \in A[x]$ abbiamo due casi diversi
   (a) Se $P \in U(A)$ allora $\exists R \in A$ tale che $P \cdot R = 1_A = 1_{A[x]}$ quindi $R \in U(A[x])$ ed è l'inverso di P in $A[x]$
   (b) Se $P \in U(A[x])$ allora $\exists R \in A[x]$ tale che $P \cdot R = 1_{A[x]} = 1_A$ quindi $\nu(P \cdot R) = \nu(P) + \nu(R) = \nu(1_A) = 0$ per cui otteniamo che P e Q sono due polinomi costanti non nulli appartenenti ad $U(A)$

Nota - I polinomi invertibili di un campo

Sia K un campo questo vuol dire che $U(K[x]) = K^* = K \setminus \{0_K\}$ cioè gli elementi costanti invertibili escluso 0_K

Esempio - Polinomi costanti invertibili

$U(\mathbb{Z}[x]) = U(\mathbb{Z}) = \{1, -1\}$

Nota - Ci sono sempre elementi non invertibili se A non è nullo

Sia $|A| \neq 1$ con $P \in A[x]$ se abbiamo che $\nu(P) > 0$ e $cd(P)$ è cancellabile in A allora $P \notin U(A[x])$

Sappiamo quindi che $x \notin U(A[x])$ e quindi $A[x]$ non potrà mai essere un campo!

Teorema - Divisione con Resto

Siano $P, S \in A[x]$ se $cd(S) \in U(A)$ allora $\exists!(Q, R) \in A[x](P = Q \cdot S + R \wedge \nu(R) < \nu(S))$

Dimostrazione

- **Unicità** Se (Q, R) e (Q_1, R_1) hanno entrambi le proprietà richieste allora otteniamo che

  $$P = Q \cdot S + R = Q_1 \cdot S + R_1 \text{ dove sia } \nu(R) < \nu(S) \text{ ma anche } \nu(R_1) < \nu(S)$$

  Portiamo da un lato dell'eguaglianza i termini con S ottenendo $(Q - Q_1)S = R - R_1$ e quindi abbiamo
  - $\nu(R_1 - R) < \nu(S)$ la somma tra polinomi non può essere maggior dei polinomi stessi
  - $cd(S)$ è cancellabile e vale la RAG quindi $\nu(Q - Q_1) + \nu(S)$
  - $\nu(Q - Q_1) = -\infty = \nu(0_A)$ quindi sappiamo che $Q - Q_1 = 0_A \Rightarrow Q = Q_1$

  Tornando all'eguaglianza iniziale abbiamo che $R - R_1 = (Q - Q_1)S = 0_A$ quindi $R = R_1$

- **Esistenza** Siano $\nu(P) = n$ e $\nu(S) = m$ e ragioniamo per controesempio minimo su n ottenendo due casi possibili
  - Se $n < m$ allora l'esistenza è ovvia perché poniamo $Q = 0_A$ e $R = P$ ottenendo $P = 0_A \cdot S + P$
  - Se $n \geq m$ allora siano $a = cd(P)$ e $b = cd(S) \in U(A)$ e facciamo delle considerazioni
    - Sia $H = ab^{-1}x^{n-m}$ (esiste perché $a \neq 0_A$ e $b \in U(A)$)
    - Sappiamo che $H \cdot S = (ab^{-1} \cdot b)x^{n-m} \cdot x^m = ax^n$ quindi ha lo stesso grado e coefficiente direttore di P
    - Se prendiamo la differenza $P_1 = P - H$ otteniamo che $\nu(P_1) < n$
    - Essendo n il più piccolo dei controesempi possiamo dividere P_1 per S
    - Quindi so che $\exists!(Q_1, R_1) \in A[x](P_1 = Q_1 \cdot S + R_1 \wedge \nu(R_1) < \nu(S))$
    - Tornando a $P = P_1 + ab^{-1}x^{n-m} \cdot S = Q_1 \cdot S + R_1 + ab^{-1}x^{n-m} \cdot S = (Q_1 + ab^{-1}x^{n-m})S + R_1$

  Quindi ponendo $R = R_1$ e $Q = Q_1 + ab^{-1}x^{n-m}$ ottengo che $P = Q \cdot S + R$

Nota - Se nella Divisione con Resto A fosse stato un campo

Se nel teorema della Divisione con Resto A fosse stato un campo avevamo che $cd(S)$ era già invertibile (essendo non nullo) quindi bastava sostituire l'ipotesi con $S \neq 0_A$

Esempio - Divisione con Resto tra Polinomi

$$\begin{array}{r|l} 2x^3+3 & 3x-1 \\ \hline -2x^3+\frac{2}{3}x^2 & \frac{2}{3}x^2+\frac{2}{9}x+\frac{2}{27} \\ \hline \frac{2}{3}x^3+3 & \\ -\frac{2}{3}x^2+\frac{2}{9}x & \\ \hline \frac{2}{9}x+3 & \\ -\frac{2}{9}x+\frac{2}{27} & \\ \hline \frac{83}{27} & \end{array}$$

Definizione - Applicazione Polinomiale

Sia A anello commutativo unitario non nullo ($|A|>1$) con $P=\sum_{i=0}^{n} a_i x^i \in A[x]$ e fissiamo $P \in A[x]$

Consideriamo l'applicazione $\widetilde{P} : c \in A \longmapsto P(c) \in A$ questa è chiamata applicazione polinomiale definita da P

NOTA Se $P \in A$ allora $\widetilde{P} : c \in A \longmapsto P \in A$ è l'applicazione costante

Definizione - Radice del Polinomio

La radice del polinomio è un'elemento che rende il polinomio stesso nullo, ovvero

$$\forall c \in A(\forall P \in A[x](c \text{ è radice di } P \Leftrightarrow P(c)=0_A))$$

Polinomi Associati $\forall P,R \in A[x](P \sim R \Rightarrow P$ e R hanno le stesse radici)

NOTA $\forall P,R \in A[x](P \mid R \Rightarrow$ Tutte le radici di P sono radici di $R \Leftrightarrow \exists Q \in A[x](R=P\cdot Q))$

Teorema - Radici del Prodotto

Se A è un dominio di integrità le radici di $P\cdot R$ sono tutti e soli gli elementi di A che sono radici di P o di R

Dimostrazione $\forall c \in A(P\cdot R)(c)=P(c)\cdot R(c)=0_A \Leftrightarrow (P(c)=0_A \vee R(c)=0_A)$

Teorema - Numero di Radici di P

$\forall P \in A[x]$ se $P \neq 0_A \Rightarrow P$ ha al massimo $\nu(P)$ radici in A

Dimostrazione Se n elementi di A sono radici di P allora $\prod_{i=1}^{n}(x-c_i) \mid P$, allora P è multiplo del prodotto per cui $\nu(P) \geq n$

Teorema - del Resto

In ogni anello communitativo unitario A questo teorema dice che

$$\forall c \in A(\forall P \in A[x](P(c) \text{ è il resto della divisione di } P \text{ per } x-c))$$

Teorema - di Ruffini

Questo Teorema ci dice che c è radice di $P \Leftrightarrow x-c \mid P$

Dimostrazione Ovvero $\exists!(Q,R) \in A[x](P=(x-c)Q+R \wedge \nu(R) < \nu(x-c))$

Sappiamo quindi che $\nu(R) \leq \nu(x-c) = 0$ ovvero che $\nu(R) = 0_A$ oppure $\nu(R) = -\infty$ e quindi $R \in A$

Concludo che applicando l'omomorfismo di sostituzione ottengo $P(c) = (c-c)Q(c)+R(c) = 0_A \cdot Q(c)+R(c) = R$

Teorema - di Ruffini Generalizzato

Sia A dominio di integrità unitario allora

$$\forall P \in A[x](\forall n \in \mathbb{N}^*(\forall c_1, c_2, ..., c_n \in A(\forall i,j \in \{1,2,...,n\}(i \neq j \Rightarrow c_i \neq c_j))))$$

Sappiamo essere equivalenti

1. $\forall i \in \{1,2,...,n\}$ c_i è radice di P
2. $\prod_{i=1}^{n}(x-c_i) \mid P$

Dimostrazione per induzione su n

- Se $n=1$ allora è verificato per il Teorema di Ruffini
- Se $n>1$ assumiamo il teorema vero per $n-1$
- ② $\Rightarrow$ ① sappiamo che $\prod_{i=1}^{n}(x-c_i)$ divide P, allora ogni c_i è radice di P perché ogni $(x-c_i)$ divide P
- ① $\Rightarrow$ ② Sia c_n radice di P, allora dal Teorema di Ruffini sappiamo che $x-c_n \mid P \Leftrightarrow \exists Q \in A[x](P=(x-c_n)Q)$
  - Adesso $\forall i \in \{1,2,...,n\}$ so che c_i è radice di P ma non di $(x-c_n)$ perché $(c_i - c_n \neq 0_A)$
  - Essendo A un dominio di integrità per ipotesi allora c_i e radice di Q
  - Otteniamo lo stesso enunciato con valore $n-1$ perché $\prod_{i=1}^{n-1} \mid Q \Leftrightarrow \exists H \in A[x](Q = H \cdot \prod_{i=1}^{n-1}(x-c_i))$

  Concludo che la produttoria divide P perché $P = Q(x-c_n) = H(\prod_{i=0}^{n-1}(x-c_i))(x-c_n) = H \cdot \prod_{i=1}^{n}(x-c_i)$

Teorema - Principio di identità dei polinomi

Sia A dominito di integrità infinito allora l'applicazione $P \in A[x] \longmapsto \widetilde{P} \in Map(A,A)$ è iniettiva ovvero

$$\forall P,R \in A[x](P = R \Leftrightarrow \widetilde{P} = \widetilde{R})$$

Dimostrazione

- $\Rightarrow$ Ovviamente se $P=R$ allora $\widetilde{P} = \widetilde{R}$

- $\Leftarrow$ Se $\widetilde{P} = \widetilde{R}$ questo vuol dire che $\forall c \in A(P(c) = R(c))$
  - Sia $H = P - R$ allora si ha che $\forall c \in A(H(c) = P(c) - R(c) = 0_A)$
  - Quindi $\forall c \in A$ sappiamo che c è radice di H
  - Essendo A infinito allora H ha infinite radici dunque $H = 0_A \Rightarrow P = R$

Nota - Il Principio di Identità non vale se A finito

Se A è finito sappiamo che non esistono applicazioni inviettiva da un insieme finito ad un insieme infinito

Domanda - Come ottengo un polinomio che ha n radici?

Se vogliamo un polinomio che ha n radici basta prendere $\prod_{i=1}^{n}(x - i)$ e otterrò un polinomio con tutte queste radici

Teorema - Fattorizzazione

Se A è un anello fattoriale allora $A[x]$ è fattoriale e so che valgono

- Se $P, R \in A[x]$ e $P \sim R$ allora $\nu(P) = \nu(R)$
- Se $P \in A[x]$ e $\nu(P) > 1$ se P ha una radice $c \in A$ allora $(x - c)$ è un divisore non banale e quindi P è riducibile

Sia K un campo e sia $P \in K[x] \setminus \{0_K\}$ con $n = \nu(P)$

1. $n = 0 \Leftrightarrow P \in U(K[x])$ quindi P è costante quindi è invertibile, riducibile e senza radici
2. $n = 1 \Rightarrow P$ ha una radice e P è irriducibile
   - Se P ha una radice $\exists a, b \in K(P = ax + b \wedge a \neq 0_K)$ allora la sua radice è $-a^{-1}b$
   - Se R è un divisore di P e chiamiamo $m = \nu(R)$
     - $m = 0$ allora R è invertibile in $K[x]$ quindi un divisore banale di P
     - $0 < m < n$ allora R è un divisore non banale
     - $m = n$ allora $\exists Q \in K[x](P = R \cdot Q)$
       - Questo vuol dire che $n = m + \nu(Q) \Rightarrow \nu(Q) = 0_K$
       - Ma allora Q è invertibile quindi $P \sim R$
3. Se $n = 2$ oppure $n = 3$ abbiamo che P ha una radice $\Leftrightarrow P$ è riducibile
4. $n > 3$ se P ha una radice $\Rightarrow P$ è riducibile

Dimostrazione ③ Se $n = \nu(P) \in \{2, 3\}$

- $\Rightarrow$ Ovvio che se P è riducibile ha una radice
- $\Leftarrow$ Se P è riducibile allora $\exists R, Q \in K[x](P = R \cdot Q \wedge \nu(R), \nu(Q) < n)$ ma questo ci porta a due casi possibili
  - $n = 2$ allora $\nu(R) = \nu(Q) = 1$
  - $n = 3$ allora $(\nu(R) = 1 \wedge \nu(Q) = 2) \vee (\nu(R) = 2 \wedge \nu(Q) = 1)$

  In ciascun caso P ha un divisore di grado 1 e quindi una radice

Nota - Quando P è irriducibile in $K[x]$?

P è irriducibile in $K[x] \Leftrightarrow P \notin K$ e non ha divisori di grado strettamente compreso tra 0 e $\nu(P)$

Tabella Riducibilità		
$n = 0$	$\Rightarrow$	P è invertibile e privo di radici
$n = 1$	$\Rightarrow$	P è irriducibile ed ha una radice
$n \in \{2, 3\}$	$\Rightarrow$	(P è riducibile $\Leftrightarrow$ P ha radici)
$n > 3$	$\Rightarrow$	(P è riducibile $\Rightarrow$ P ha radici)

Definizione - Polinomi associati

Sia $P \in K[x] \setminus \{0_K\}$ e sia $a = cd(P)$ otteniamo che $\forall b \in K[x] \setminus \{0_K\}$

$$\text{Il polinomio } P \text{ ha esattamente un associato con } cd(b)$$

Dimostrazione gli associati di P sono tutti e soli gli elementi della forma $P \cdot c$ al variare di $c \in U(K[x]) = K \setminus \{0_K\}$

Preso c allora $cd(P \cdot c) = a \cdot c = b \Leftrightarrow c = a^{-1}b$ (essendo $a \neq 0_K$ ed in un gruppo allora è invertibile)

NOTA Se $b = 1_K$ otteniamo un'unico associato monico perché in ogni classe di elementi associati di polinomi è unico

Domanda - Quando due polinomi sono associati?

Due polinomi sono associati quando hanno lo stesso associato monico, inoltre in $\mathbb{Q}[x]$ ogni polinomio ha infiniti associati

Teorema - Decomposizione di Polinomi

Sia K un campo allora $\forall P \in K[x] \setminus K$ otteniamo che P ha questa decomposizione

$$P = u \cdot p_1 + p_2 + ... + p_n \text{ dove } u \in K \setminus \{0_K\} \text{ e } n \in \mathbb{N}^*$$

Inoltre $\forall i \in \{1, 2, ..., n\}$ abbiamo che p_i è irriducibile in $K[x]$ ed anche monico

Dimostrazione Unicità della decomposizione a meno dell'ordine dei fattori

Posso scrivere come prodotto di irriducibili $P = q_1 + q_2 + ... + q_n$ con $n \in \mathbb{N}^*$ allora

- $\forall i \in \{0, 1, 2, ..., n\}$ scelgo $a_i = cd(q_i)$ e pongo $p_i = a^{-1}q_i$
- Ottengo che p_i è monico e allora $P = up_i + up_2 + ... + up_n$ dove $u \in K \setminus \{0_K\}$

Concludo che la scomposizione è unica a meno di fattori perché l'unico associato a p_i è p_i

Nota - Scomporre i Polinomi aiuta a lavorare con questi elementi

Preso un polinomio di grado 6 posso scriverlo come un prodotto di due polinomi di grado 3, perché in un campo se ha radice allora è riducibile, lavorando separatamente su polinomi più piccoli

Domanda - Quali sono gli irriducibili in $R[x]$?

Sia $P \in R[x]$ possiamo osservare il suo grado per capire se è riducibile

- $\nu(P) = 1$ è irriducibile
- $\nu(P) = 2$ è riducibile solo se ha radice
- $\nu(P) > 2$ è sempre riducibile

Nota - Studiare un Polinomio o il suo associato è la stessa cosa

Ogni polinomio a coefficienti razionali può essere moltiplicato per un multiplo comune ai denominatori, restituendo un polinomio a coefficienti interi associato al precedente, conservando le radici e proprietà rispetto alla divisibilità

Teorema - di Eisenstein

Sia $P \in \mathbb{Z}[x] \setminus \{0\}$ con $P = \sum_{i=0}^{n} a_i x^i$ e dato $n = \nu(P)$ Eisenstein afferma che

$$\text{Se esiste } p \in \mathbb{P}(p \mid a_{n-1}, \dots, a_1, a_0 \wedge p \nmid a_n \wedge p^2 \nmid a_o) \Rightarrow P \text{ è irriducibile in } \mathbb{Q}[x]$$

Esempio - Teorema di Eisenstein

$\forall n \in \mathbb{N}^*$ sappiamo che $x^n - 2$ è irriducibile in $\mathbb{Q}[x]$ perché se prendo il numero primo 2 allora viene verificato Eisenstein

$$(2 \mid 2 \wedge 2 \nmid 1 \wedge (2)^2 \nmid 2) \Rightarrow x^n - 2 \text{ è irriducibile in } \mathbb{Q}(x)$$

Nota - Non sempre vale il viceversa

Sappiamo che $x + 1$ è irriducibile ma non esiste primo che verifichi Eisenstein, quindi il viceversa non sempre vale!

Domanda - Come trovo le radici?

Supponiamo di avere il polinomio $(x^6 - 9)$ come procediamo?

- Cominciamo col prodotto notevole otteniamo $(x^6 - 9) = (x^3 - 3)(x^3 + 3)$
- Se siamo in $\mathbb{Q}[x]$ applichiamo Eisenstein che dice che è irriducibile
- Se siamo in $\mathbb{R}[x]$ continuiamo con la fattorizzazione
- In ogni campo in cui 2 è invertibile e Δ è un quadrato in $\mathbb{Q}$
- In $\mathbb{Z}_n$ elenchiamo i quadrati delle classi di resto e vediamo se sono radici (tutti quelli maggiori del modulo sono congrui)

NOTA In $\mathbb{Q}[x]$ ci sono polinomi irriducibili di qualsiasi grado

Teorema - Radici di un polinomio con coefficienti interi

$\forall P \in \mathbb{Z}[x] \setminus \{0\}$ con $P = \sum_{i=0}^{n} a_i x^i$ dove $n = \nu(P)$

Siano u e v due interi coprimi e $P(\frac{u}{v}) = 0$ allora abbiamo che $v \underset{\mathbb{Z}}{\mid} a_n \wedge u \underset{\mathbb{Z}}{\mid} a_0$

Allora se la radice esiste si trova tra le possibili combinazioni di $\frac{u}{v}$

Esempio - Radici di un polinomio con coefficienti interi

Dato il polinomio $7x^4 + 3x + 1$ allora $u \in \{1, -1\}$ e $v \in \{\frac{1}{7}, -\frac{1}{7}\}$ allora se la radice esiste sarà $\frac{u}{v} \in \{-1, 1, \frac{1}{7}, -\frac{1}{7}\}$

Nota - Caso in cui $cd(P) = 1$

Se $v \in \{1, -1\}$ allora $\frac{u}{v}$ è un numero intero, inoltre i polinomi a coefficienti interi monici se hanno radice in R è intera

Grafi

Definizione - Grafo

Si tratta di una rappresentazione grafica di una relazione binaria, infatti il Diagramma di Hasse è un tipo di grafo orientato, in questo caso invece le linee che congiungono i vertici hanno verso di percorrenza bidirezionale

Grafo Completo è detto completo quando $G = (V, P_2(V))$

Grafo Complementare è detto complementare quando $\overline{G} = (V, P_2(V) \setminus L)$

Grafo Connesso quando ogni coppia di vertici è connessa

NOTA Il disegno differisce dall'oggetto matematico

Definizione - Grafo Semplice

Un grafo semplice è una coppia ordinata $G = (V, L)$ con $V \neq \emptyset$ e con $L \subseteq P_2(V)$ dove chiamo

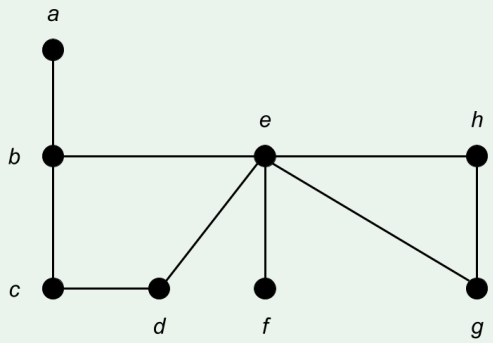
- Vertici: gli elementi di V
- Lati: gli elementi di L
- Lati incidenti: hanno un vertice in comune
- Estremi del Lato: elementi del lato

Nota - Il numero di lati di un grafo semplice

In un grafo semplice il numero dei lati non può essere maggiore delle coppie di vertici, ovvero $|L| \leq \binom{|V|}{2} = |P_2(V)|$

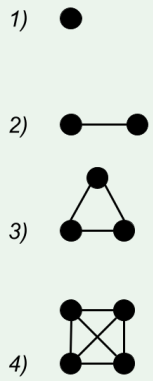
Esempio - Grafo Semplice

Sia $V = \{a, b, c, d, e, f\}$ allora potremmo disegnare il suo grafo così data una certa relazione

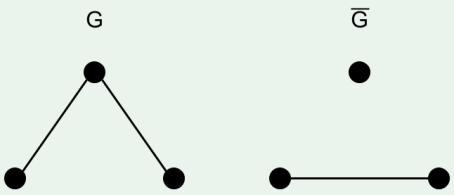


Dal grafo possiamo vedere che il lato $\{a, b\} \in L$ mentre $\{a, e\} \notin L$

Esempio - Grafo Completo



Esempio - Grafo Complementare



Definizione - Grado di un vertice

Si tratta di quante linee partono da quel vertici ed assume questa definizione

$$\forall v \in V(d(v) = |\{l \in L \mid v \text{ è estremo di } l\}|)$$

Domanda - Come si disegna un grafo?

Se V è finito allora posso considerare un'applicazione biettiva tra V e un sotto-insieme del piano per disegnare tutti i vertici ma attenzione a tracciare un lato tra due punti, infatti

$$\text{Posso tracciare una lato tra due punti} \Leftrightarrow \forall x, y \in V(\{x, y\} \in L)$$

Definizione - Adiecenza

Sia $\rho \in Rel(V)$ con le seguente definizione $\forall x, y \in V(x \rho y \Leftrightarrow \{x, y\} \in L)$ sappiamo che ha le seguenti proprietà

- **Simmetrica** per definizione
- **Anti-riflessiva** perché i singleton non compongono un lato

Otteniamo quindi $\{\{x, y\} \mid x \rho y\} =: L \subseteq P_2(V)$

Definizione - Multi-grafo

Un grafo che ha più lati tra due vertici, quindi otteniamo una terna ordinata $G = (V, L, f)$ con $V \neq \emptyset \neq L$

Per avere più lati tra due vertici usiamo la funzione $f : L \longmapsto P_2(V)$ che ad ogni lato associa una coppia

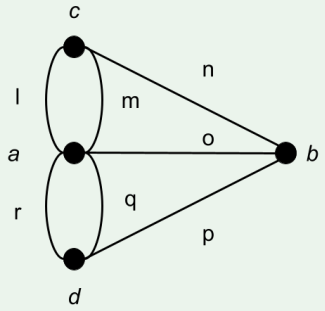
NOTA Se f è iniettiva allora grafo è multi-grafo coincidono

Nota - Multi-grafo e Grafo finiti

Un grafo semplice è finito quando V finito $\Rightarrow L$ finito, mentre per il multi-grafo va richiesto che V e L siano finiti

Esempio - Multi-grafo

Siano $V = \{a, b, c, d\}$ e $L = \{l, m, n, o, p, q, r\}$ allora possiamo disegnare il multi-grafo in questo modo data una certa relazione



Teorema - La somma dei gradi dei vertici è il doppio del numero dei lati

Sia $G = (V, L, f)$ un multi-grafo possiamo ricavare il numero dei lati usando questa formula

$$\sum_{v \in V} d(v) = 2|L|$$

Dimostrazione usando la tecnica del doppio conteggio, sia $S = \{(v, l \in V \times L \mid v \text{ sia estremo di } l)\}$

Se immaginiamo una tabella che ha come colonne i lati e come vertici le righe, possiamo contare le caselle barrate

- Se contiamo per colonna, sappiamo che ha due estremi che sono il numero di caselle barrate
  - Allora $\forall l \in L(\exists_2 v \in V((v, l) \in V \times L))$ allora otteniamo che $|S| = 2|L|$
- Se contiamo per riga, sappiamo che ha tante caselle barrate pari al suo grado
  - Allora $|S| = \sum_{v \in V} d(v)$

Concludo $|S| = 2|L| = \sum_{v \in V} d(v)$

Nota - In un grafo il numero di vertici dispari deve essere un numero pari

In un grafo il numero dei vertici con grado dispari deve essere pari, perché la somma dei gradi dei vertici coincide col doppio del numero dei lati che è un numero pari

Definizione - Sotto-Grafo

Sia $G = (V, L)$ un grafo semplice, definiamo un suo sotto-grafo $G_1 = (V_1, L_1)$ rispettando le seguenti richieste

1. $V_1 \subseteq V$
2. $L_1 \subseteq L$
3. $L_1 \subseteq P_2(V_1)$

Il punto ③ ci serve per avere gli stremi dei lati che ho conservato e eliminare i lati dei vertici che cancello

NOTA analogamente per i multi-grafi con $f_{|L_1}^{|P_1(V_1)}$

Definizione - Grafo Palanare

Un grafo o multi-grafo è detto palanare se si può rappresentare il suo disegno senza far intersecare i suoi lati

Teorema - Simile a Birckhoff

Un grafo è detto planare se non ha come sotto-grafo isomorfo ai propri sotto-grafi K_5 o $K_{3,3}$

Isomorfismo tra Grafi

Definizione - Isomorfismo tra grafi semplici

Questo isomorfismo ci permette di rappresentare più grafi con lo stesso disegno, infatti siano $G = (V, L)$ e $H = (W, M)$

Abbiamo l'isomorfismo con l'applicazione biettiva $\varphi : V \longmapsto W$ tale che $\forall x, y \in V(\{x, y\} \in L \Leftrightarrow \{\varphi(x), \varphi(y)\} \in M)$

NOTA L'isomorfismo conserva vertici, lati e gradi

Definizione - Isomorfismo tra Multi-Grafi

Tra Multi-Grafi l'isomorfismo è una coppia ordinata di applicazioni biettive (φ, ψ) con le proprietà

- $\varphi : V \longmapsto W$ isomorfismo tra vertici
- $\psi : L \longmapsto M$ isomorfismo tra lati

Siano $G = (V, L, f)$ e $H = (W, M, g)$ abbiamo che

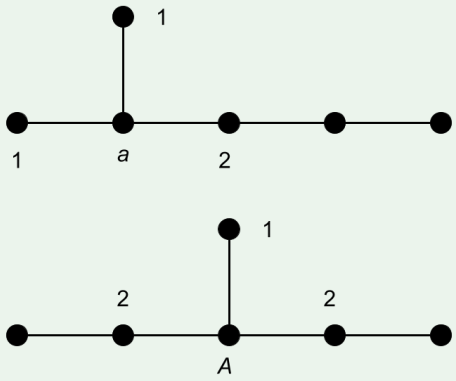
- $\forall l \in L(\psi(l) \in M)$
- $g(\psi(l)) = \overrightarrow{\varphi}(f(l))$

Nota - Risulta complicato verificare gli isomorfismi

Anche per grafi con con circa 20 vertici risulta complesso verificare se sono isomorfi, una tecnica per ridursi il lavoro e cercare di connettere i vertici aventi gli stessi gradi all'interno dei grafi

Esempio - Isomorfismo tra Grafi

Possiamo notare che non si tratti di un isomorfismo perché non posso associare gli stessi vertici di a ad A perché hanno gradi diversi



Cammini e Circuiti

Definizione - Cammino

Sia $G = (V, L, f)$ un multi-grafo dove $a, b \in V$ e $n \in \mathbb{N}^*$ allora chiamo cammino da a verso b una n-upla di lati

Questa n-upla ha le seguenti caratteristiche

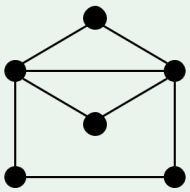
- La sua lunghezza è n
- I lati al suo interno non si ripetono e sono a due a due disgiunti
- Esiste una $(n+1)$-upla di vertici di G tali che $a = v_0$ e $b = v_1$
- $\forall i \in \{1, 2, ..., n\}$ gli estremi di l_i sono esattamente v_{i-1} e v_i

Possiamo identificare diversi tipi di cammini

- **Circuito** cammino in cui gli estremi coincidono
- **Cammino euleriano** cammino che attraversa tutti i lati
- **Circuito euleriano** cammino euleriano che è anche un circuito

NOTA il cammino di lunghezza 0 è la n-upla vuota

Esempio - Circuti euleriano



Definizione - Relazione di Connessione

$\forall a, b \in V$ a e b si dicono connessi quando esiste un cammino da a a b, questa relazione è di equivalenza

- **Riflessiva** $a = b$ allora il cammino è vuoto
- **Simmetrica** basta invertire il cammino da b ad a
- **Transitiva** bisogna prendere il cammino più breve senza ripetizioni di vertici e lati

Teorema - Esistenza del cammino euleriano

Sia un multi-grafo connesso esiste un cammino euleriano tra un vertiici diversi a e $b \Leftrightarrow$ a e b hanno grado dispari e tutti gli altri sono pari

Dimostrazione Partendo da un vertice a e effettuando un cammino euleriano cancello i lati percorsi dalle possibilità, quindi per ogni vertice tra a e b so sicuramente che ha grado pari (perché arrivo e riparto da quel vertice)

Teorema - Esistenza del circuito euleriano

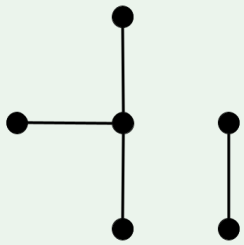
In un multi-grafo connesso finito esistono circuiti euleriani $\Leftrightarrow$ tutti i vertici hanno grafo pari

Foreste e Alberi

Definizione - Foreste

Una foresta è un multi-grafo in cui l'unico circuito ha lunghezza 0

Esempio - Foresta



Teorema - Esistenza delle foreste

Un multi-grafo è una foresta $\Leftrightarrow \forall a, b \in V$(esiste al massimo un cammino da a verso b)

Dimostrazione

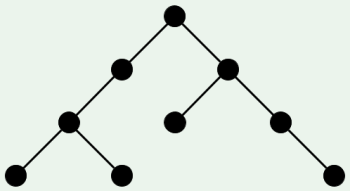
- $\Rightarrow$ Supponiamo ci siano due cammini distinti da a verso b, allora posso costruire un circuito ed il multi-grafo non risulta più essere una foresta
- $\Leftarrow$ Se il multi-grafo non è una foresta allora contiene almeno un circuito di lunghezza maggiore di 0, questo vuol dire che esiste più di un cammino da a verso b

Definizione - Albero

Si tratta di una foresta connessa dove $\forall a, b \in V$(esiste un solo cammino da a verso b)

NOTA gli alberi in informatica vengono usati con la rappresentazione radicale (i nodi con grado 1 si chiamano foglie)

Esempio - Albero con rappresentazione radicale



Teorema - Rimuovendo le foglie resta un albero

Sia $T = (V, L)$ un albero finito e $v \in V$ tale che $d(v) = 1$, questo mi assicura che sia una foglia del mio albero, sia estremo di l allora ottengo che $T' = (V \setminus \{v\}, L \setminus \{l\})$ è ancora un albero

Dimostrazione Per induzione su $|L|$ e supponiamo il teorema verificato per $n - 1$

- Base induttiva: $|L| = 0 \Rightarrow |V| = 0 + 1$
- Passo induttivo $|V| - 1 = |V \setminus \{v\}| = |L \setminus \{l\}| - 1 = |L|$

Concludo Che $|V| = (|L \setminus \{l\}| + 1) + 1 = |L| + 1$

Definizione - Sotto-albero Massimale

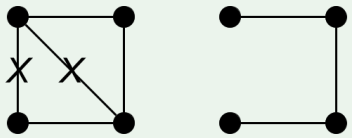
Sia G un multi-grafo connesso finito allora definiamo un sotto-albero massimale di G un albero ottenuto cancellando dui lati ma senza eliminarne i vertici

$$G \text{ è un sotto-albero massimale} \Leftrightarrow G \text{ è connesso}$$

Dimostrazione

- $\Rightarrow$ Se cancello un lato è il multi-grafo resta connesso allora era già connesso a priori
- $\Leftarrow$ Se è connesso è non ha circuito allora è una foresta

Esempio - Sotto-albero Massimale



Teorema - Finale sulle foreste

Sia $G = (V, L)$ un multi-grafo con k componenti connesse allora

1. G è connesso $\Rightarrow |L| \geq |V| - 1$
2. Generalmente vale $|L| \geq |V| - k$
3. Sono equivalenti
   (a) G è un albero
   (b) G è connesso e vale $|V| = |L| + 1$
   (c) G è una foresta e vale $|V| = |L| + 1$
4. Sono equivalenti
   (a) G è una foresta
   (b) $|L| = |V| - k$

Dimostrazione

- ③ (a) Se G è un albero allora deve essere una foresta connessa
- ③ (b) Se G è connesso e vale $|V| = |L| + 1$ allora G è sotto-albero massimale di se stesso
- ③ (c) Se G è una foresta e vale $|V| = |L| + 1$ allora la componente connessa è unica quindi è un albero
- ④ (a) Se G è un albero allora vale l'uguaglianza
- ④ (b) Se vale l'uguaglianza ogni componente connessa è un albero, allora il multi-grafo è una foresta