Algebra Corso Celentani 2025 (inc. grafi e polinomi)

Logica Proposizionale e Teoria degli Insiemi

Data: 11/03/2025
Argomenti: Connettivi logici, Tavole di verità, Tautologie, Contraddizioni, Quantificatori, Teoria degli Insiemi di base, Prodotto Cartesiano, Relazioni, Funzioni.

#tag/logica #tag/settheory #tag/algebra-avanzata #tag/fondamenti

---

1. Logica Proposizionale: I Mattoncini del Ragionamento

La logica ci aiuta a capire come costruire ragionamenti validi. Iniziamo con le basi: le proposizioni e come collegarle. Una **proposizione** è un'affermazione che può essere VERA (V) o FALSA (F).

1.1 Connettivi Logici Fondamentali

I connettivi logici sono come la "colla" che unisce le proposizioni semplici per crearne di più complesse.

- **Negazione (NOT):** Inverte il valore di verità.
  - Simbolo: $\neg$ (si legge "non")
  - Esempio: Se P è "Oggi piove", $\neg P$ è "Oggi non piove".

Tavola di Verità (Negazione):

P	$\neg P$
V	F
F	V

- **Congiunzione (AND):** È vera solo se *entrambe* le proposizioni sono vere.
  - Simbolo: $\wedge$ (si legge "e")
  - Esempio: Se P è "Studio logica" e Q è "Ascolto musica", $P \wedge Q$ è "Studio logica e ascolto musica".

Tavola di Verità (Congiunzione):

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

- **Disgiunzione Inclusiva (OR):** È vera se *almeno una* delle proposizioni è vera.
  - Simbolo: $\vee$ (si legge "o")
  - Esempio: Se P è "Prendo il caffè" e Q è "Prendo il tè", $P \vee Q$ è "Prendo il caffè o prendo il tè (o entrambi)".

Tavola di Verità (Disgiunzione Inclusiva):

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

> **Nota Bene: Questa è la "o" inclusiva, significa che va bene anche se entrambe sono vere. Nelle tue note c'era scritto "non disgiuntiva", ma in realtà $\vee$ *è* la disgiunzione standard (inclusiva). Forse intendevi la disgiunzione *esclusiva*? Ne parliamo tra poco!** 1.5 Disgiunzione Esclusiva (XOR)

- **Implicazione Materiale (SE... ALLORA):** È falsa solo se la prima proposizione (antecedente) è vera e la seconda (conseguente) è falsa.

- Simbolo: $\implies$ (o $\rightarrow$, si legge "implica" o "se... allora")
- Esempio: Se P è "Studio" e Q è "Passo l'esame", $P \implies Q$ è "Se studio, allora passo l'esame".

Tavola di Verità (Implicazione):

P	Q	$P \implies Q$
V	V	V
V	F	F
F	V	V
F	F	V

Suggerimento: Pensa all'implicazione come a una promessa. $P \implies Q$ significa "Se P è vera, prometto che Q è vera". L'unico caso in cui la promessa è infranta è quando P è vera, ma Q è falsa. Se P è falsa, la promessa non è stata messa alla prova, quindi l'implicazione è considerata vera.

- **Bicondizionale (SE E SOLO SE):** È vera solo se le proposizioni hanno lo *stesso* valore di verità.
  - Simbolo: $\iff$ (o $\leftrightarrow$, si legge "se e solo se" o "è equivalente a")
  - Esempio: Se P è "Il triangolo ha 3 lati uguali" e Q è "Il triangolo ha 3 angoli uguali", $P \iff Q$ è "Un triangolo ha 3 lati uguali se e solo se ha 3 angoli uguali".

Tavola di Verità (Bicondizionale):

P	Q	$P \iff Q$
V	V	V
V	F	F
F	V	F
F	F	V

1.2 Equivalenze Logiche Importanti

Alcune formule complesse sono equivalenti, cioè hanno sempre lo stesso valore di verità.

- **Implicazione e Disgiunzione:** L'implicazione $P \implies Q$ è equivalente a $\neg P \lor Q$.
  - Formula: $(P \implies Q) \iff (\neg P \lor Q)$

Verifica Equivalenza (Implicazione $\iff$ Disgiunzione Negata):

P	Q	$P \implies Q$	$\neg P$	$\neg P \lor Q$	$(P \implies Q) \iff (\neg P \lor Q)$
V	V	V	F	V	V
V	F	F	F	F	V
F	V	V	V	V	V
F	F	V	V	V	V

Questa equivalenza è super utile per trasformare le implicazioni! Equivalenza Implicazione-Disgiunzione

- **Doppia Negazione:** Negare due volte riporta alla proposizione originale.
  - Formula: $\neg(\neg P) \iff P$
  - Legge della Doppia Negazione
- **Contrapposizione:** L'implicazione $P \implies Q$ è equivalente alla sua contrapposta $\neg Q \implies \neg P$.
  - Formula: $(P \implies Q) \iff (\neg Q \implies \neg P)$

Verifica Equivalenza (Implicazione $\iff$ Contrapposta):

P	Q	$P \implies Q$	$\neg Q$	$\neg P$	$\neg Q \implies \neg P$	$(P \implies Q) \iff (\neg Q \implies \neg P)$
V	V	V	F	F	V	V
V	F	F	V	F	F	V
F	V	V	F	V	V	V
F	F	V	V	V	V	V

- Legge di Contrapposizione

1.3 Tautologie e Contraddizioni

- **Tautologia:** Una proposizione composta che è **sempre VERA**, indipendentemente dal valore di verità delle proposizioni semplici che la compongono.
  - Esempi (dalle tue note!):
    $P \vee \neg P$ *(Principio del terzo escluso)*
    $P \implies P$ (Identità)
    $\star$ $((P \implies Q) \wedge P) \implies Q$ (Modus Ponens)

    > **Le tautologie rappresentano le leggi fondamentali del pensiero logico.**

  - #tag/tautologia Tautologia
- **Contraddizione:** Una proposizione composta che è **sempre FALSA**. È la negazione di una tautologia.
  - Esempio (dalle tue note!): $P \wedge \neg P$ (Principio di non contraddizione)
  - Formula: $P \wedge \neg P \iff \neg(P \vee \neg P)$
  - #tag/contraddizione Contraddizione

1.4 Leggi Logiche (Proprietà Tautologiche)

Queste sono equivalenze logiche fondamentali che valgono sempre (sono tautologie). Usiamo a, b, c come proposizioni generiche. Leggi Logiche

1. **Idempotenza:** Ripetere una proposizione con $\wedge$ o $\vee$ non cambia nulla.
   - $a \wedge a \iff a$
   - $a \vee a \iff a$
   - Legge di Idempotenza
2. **Associatività:** Puoi raggruppare come vuoi con lo stesso connettivo ($\wedge$, $\vee$, $\iff$).
   - $(a \wedge b) \wedge c \iff a \wedge (b \wedge c)$
   - $(a \vee b) \vee c \iff a \vee (b \vee c)$
   - $(a \iff b) \iff c \iff a \iff (b \iff c)$ (*Attenzione: l'associatività per $\implies$ non vale in generale!*)
   - Legge Associativa
3. **Commutatività:** Puoi scambiare l'ordine delle proposizioni con $\wedge$, $\vee$, $\iff$.
   - $a \wedge b \iff b \wedge a$
   - $a \vee b \iff b \vee a$
   - $a \iff b \iff b \iff a$
   - Legge Commutativa
4. **Distributività:** Come la moltiplicazione si distribuisce sulla somma in aritmetica.
   - $a \wedge (b \vee c) \iff (a \wedge b) \vee (a \wedge c)$ ($\wedge$ si distribuisce su $\vee$)
   - $a \vee (b \wedge c) \iff (a \vee b) \wedge (a \vee c)$ ($\vee$ si distribuisce su $\wedge$)

Verifica Legge Distributiva ($\wedge$ su $\vee$):

a	b	c	$b \vee c$	$a \wedge (b \vee c)$	$a \wedge b$	$a \wedge c$	$(a \wedge b) \vee (a \wedge c)$	**Equivalenza**
V	V	V	V	V	V	V	V	V
V	V	F	V	V	V	F	V	V
V	F	V	V	V	F	V	V	V
V	F	F	F	F	F	F	F	V
F	V	V	V	F	F	F	F	V
F	V	F	V	F	F	F	F	V
F	F	V	V	F	F	F	F	V
F	F	F	F	F	F	F	F	V

- Legge Distributiva

5. **Leggi di De Morgan:** Utili per negare $\wedge$ e $\vee$.
   - $\neg(a \wedge b) \iff (\neg a \vee \neg b)$
   - $\neg(a \vee b) \iff (\neg a \wedge \neg b)$
   - Leggi di De Morgan
6. **Transitività dell'Implicazione:** Se a implica b e b implica c, allora a implica c.
   - Formula: $((a \implies b) \wedge (b \implies c)) \implies (a \implies c)$

Verifica Transitività Implicazione:

a	b	c	$b \implies c$	$a \implies b$	$(a \implies b) \land (b \implies c)$	$a \implies c$	**Transitività**
V	V	V	V	V	V	V	V
V	V	F	F	V	F	F	V
V	F	V	V	F	F	V	V
V	F	F	V	F	F	F	V
F	V	V	V	V	V	V	V
F	V	F	F	V	F	V	V
F	F	V	V	V	V	V	V
F	F	F	V	V	V	V	V

- Legge di Transitività (Sillogismo Ipotetico)

1.5 Disgiunzione Esclusiva (XOR)

Questo è l'"o" che significa "uno o l'altro, ma non entrambi".

- Simbolo: $\oplus$ (o $\veebar$, a volte indicato come $\dot{\vee}$ nelle tue note)
- Significato: $a \oplus b$ è vera se *esattamente una* tra a e b è vera.
- Equivalenza (dalle tue note!): $a \oplus b \iff (\neg a \land b) \lor (a \land \neg b)$
- Equivalenza alternativa: $a \oplus b \iff (a \lor b) \land \neg(a \land b)$

Tavola di Verità (XOR):

P	Q	$P \oplus Q$
V	V	F
V	F	V
F	V	V
F	F	F

- #tag/xor Disgiunzione Esclusiva (XOR)

1.6 Operatori NAND e NOR

Questi sono interessanti perché *ciascuno* di essi può essere usato per costruire tutti gli altri connettivi logici! Sono chiamati **operatori funzionalmente completi**.

- **NAND (NOT AND):** È la negazione di AND.
  - Simbolo: $\uparrow$ (Freccia di Sheffer)
  - Definizione: $P \uparrow Q \iff \neg(P \land Q)$
- **NOR (NOT OR):** È la negazione di OR.
  - Simbolo: $\downarrow$ (Freccia di Peirce)
  - Definizione: $P \downarrow Q \iff \neg(P \lor Q)$
- #tag/nand #tag/nor Operatore NAND Operatore NOR Completezza Funzionale

Domanda Rapida: Riesci a vedere perché $(P \land \neg P)$ è una contraddizione usando la tavola di verità? E perché $(P \lor \neg P)$ è una tautologia?

---

2. Logica dei Predicati: Parlare di Proprietà e Quantità

A volte, le proposizioni dipendono da variabili. #tag/logica-predicati

2.1 Predicati e Variabili

- **Predicato:** Una proprietà o relazione che coinvolge una o più variabili. Diventa una proposizione (V o F) quando alle variabili viene assegnato un valore specifico da un certo **universo del discorso** (dominio).
  - Esempio (dalle tue note!): $P(x) : x > 10$.
    - Qui $P(x)$ è il predicato. x è la **variabile**.
    - Se l'universo sono i numeri interi $\mathbb{Z}$:
      - $P(12)$ (cioè $12 > 10$) è VERA.
      - $P(2)$ (cioè $2 > 10$) è FALSA.
  - Predicato Variabile Universo del Discorso

- **Formula Ben Formata (FBF):** Un'espressione costruita correttamente usando variabili, predicati, connettivi logici e quantificatori (vedi sotto). Le tue note mostrano esempi come "$3 + x = 10$" o "$x + 3 > 10$", che sono predicati (o formule aperte). L'esempio "$3 + +x - =$" non è ben formato. Formula Ben Formata (FBF)

2.2 Quantificatori

I quantificatori ci dicono *quanti* elementi nell'universo soddisfano un predicato. Quantificatori

- **Quantificatore Universale (PER OGNI):** Afferma che il predicato è vero per *tutti* gli elementi dell'universo.
  - Simbolo: $\forall$ (si legge "per ogni" o "per tutti")
  - Esempio: $\forall x \in \mathbb{R}, x^2 \geq 0$ ("Per ogni numero reale x, il suo quadrato è maggiore o uguale a zero").
  - Nelle tue note: $\forall x (x > 1)$ (Questa affermazione dipende dall'universo! Se l'universo sono i numeri reali $\mathbb{R}$, è Falsa. Se l'universo sono i numeri reali maggiori di 1, $(1, +\infty)$, è Vera).
  - #tag/quantificatore-universale Quantificatore Universale
- **Quantificatore Esistenziale (ESISTE ALMENO UN):** Afferma che il predicato è vero per *almeno un* elemento dell'universo.
  - Simbolo: $\exists$ (si legge "esiste almeno un" o "per qualche")
  - Esempio: $\exists x \in \mathbb{R}, x^2 = 4$ ("Esiste almeno un numero reale x il cui quadrato è 4" - Vero, x=2 e x=-2).
  - #tag/quantificatore-esistenziale Quantificatore Esistenziale
- **Quantificatore Esistenziale Unico (ESISTE UN UNICO):** Afferma che il predicato è vero per *esattamente un* elemento dell'universo.
  - Simbolo: $\exists!$ (si legge "esiste un unico")
  - Definizione (dalle tue note!): $\exists! x P(x) \iff \exists x (P(x) \land \forall y (P(y) \implies x = y))$
    - **Spiegazione Semplice:** "Esiste un x che ha la proprietà P, e se qualcos'altro (y) ha la proprietà P, allora quel qualcos'altro deve essere proprio x".
  - #tag/quantificatore-unico Quantificatore di Unicità

2.3 Variabili Libere e Vincolate, Formule Chiuse

- **Variabile Vincolata:** Una variabile che è "controllata" da un quantificatore ($\forall$ o $\exists$) che agisce su di essa.
- **Variabile Libera:** Una variabile che non è vincolata da nessun quantificatore.
- **Formula Aperta:** Una formula che contiene almeno una variabile libera. Il suo valore di verità dipende dal valore assegnato alle variabili libere (es. $x > 10$).
- **Formula Chiusa (o Enunciato):** Una formula che non contiene variabili libere. Ha un valore di verità definito (V o F) indipendentemente da assegnazioni esterne (es. $\forall x (x > 1)$, $\exists x (x > 10)$).

Esempio dalle tue note (Pagina 17):

- `a: x > 1` (Formula aperta, x è libera)
- `b: ∀x(x > 1)` (Formula chiusa, x è vincolata da $\forall$)
- `c: ∀x(x > 1) ∧ x = 7` (Questa è un po' ambigua come scritta. Probabilmente si intende `(∀y(y > 1)) ∧ (x = 7)`. Qui, la y nel primo pezzo è vincolata (ho cambiato nome per chiarezza), ma la x nel secondo pezzo è libera. Quindi è una formula aperta.)
  Se sostituiamo $x = 3$ in `a`, otteniamo $3 > 1$ (Vero).
  Se sostituiamo $x = 3$ in `c` (nell'interpretazione sopra), otteniamo $(\forall y (y > 1)) \land (3 = 7)$. Il valore di verità di $(\forall y (y > 1))$ dipende dall'universo scelto per y. Ma poiché $(3 = 7)$ è Falso, l'intera congiunzione $\land$ sarà Falsa, indipendentemente dal primo pezzo.

- Variabile Libera Variabile Vincolata Formula Aperta Formula Chiusa

---

3. Teoria degli Insiemi: Collezioni di Oggetti

Un **insieme** è una collezione di oggetti distinti (senza ordine e senza ripetizioni), chiamati **elementi**. #tag/settheory Teoria degli Insiemi

- Notazione: $A = \{a, b, c\}$, $x \in A$ (x è un elemento di A), $y \notin A$ (y non è un elemento di A).
- **Insieme Vuoto:** L'insieme che non contiene alcun elemento. Simbolo: $\emptyset$ (o $\{\}$). Insieme Vuoto
- **Sottoinsieme:** $S \subseteq A$ significa che ogni elemento di S è anche un elemento di A. Sottoinsieme

3.1 Prodotto Cartesiano

Dati due insiemi A e B, il loro prodotto cartesiano è l'insieme di tutte le **coppie ordinate** (a, b) dove a proviene da A e b proviene da B.

- Simbolo: $A \times B$
- Definizione (dalle tue note!): $A \times B = \{(a, b) \mid a \in A \land b \in B\}$

- Esempio (dalle tue note!): Se $A = \{a, b, c\}$ e $B = \{1, 2, 3, 4\}$, allora $A \times B$ contiene coppie come $(a, 1), (b, 3), (c, 4)$, ecc. In totale $|A| \times |B| = 3 \times 4 = 12$ coppie.
  - Nota: L'ordine conta! $(a, 1) \in A \times B$, ma $(1, a) \notin A \times B$ (a meno che $1 \in A$ e $a \in B$). $(1, a) \in B \times A$.
- Proprietà (dalle tue note!): $A \times B = \emptyset \iff A = \emptyset \vee B = \emptyset$. (Il prodotto cartesiano è vuoto se e solo se almeno uno dei due insiemi è vuoto).
- #tag/prodotto-cartesiano Prodotto Cartesiano

3.2 Relazioni

Una **relazione** (o corrispondenza) ρ tra un insieme A (dominio o insieme di partenza) e un insieme B (codominio o insieme di arrivo) è semplicemente un **sottoinsieme** del prodotto cartesiano $A \times B$.

- Notazione: $\rho \subseteq A \times B$. Spesso si indica una relazione con il suo **grafo**, cioè l'insieme delle coppie $G = \rho \subseteq A \times B$.
- Si scrive $a \rho b$ o $(a, b) \in G$ per dire che a è in relazione con b.
- Esempio (dalle tue note!): $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$.
  - $S = \{(a, 1), (b, 4)\}$ è una relazione tra A e B. Qui, a è in relazione con 1, e b è in relazione con 4. c non è in relazione con nessuno, e $2, 3$ non sono in relazione con nessuno tramite S.
  - $T = \{(a, 1), (b, 1), (a, 4), (b, 4)\}$ è un'altra relazione. Qui a è in relazione sia con 1 che con 4.
- #tag/relazione Relazione Binaria Grafo di una Relazione

3.3 Funzioni (o Applicazioni)

Una **funzione** f da A a B è un tipo *speciale* di relazione in cui **ogni** elemento di A è associato a **esattamente un** elemento di B.

- Notazione: $f : A \to B$
- Definizione formale (usando il grafo $G \subseteq A \times B$):
  1. **Dominio totale (Esistenza):** Per ogni $a \in A$, esiste almeno un $b \in B$ tale che $(a, b) \in G$. ($\forall a \in A, \exists b \in B : (a, b) \in G$)
  2. **Univalenza (Unicità):** Per ogni $a \in A$, se $(a, b_1) \in G$ e $(a, b_2) \in G$, allora $b_1 = b_2$. ($\forall a \in A, \forall b_1, b_2 \in B : ((a, b_1) \in G \wedge (a, b_2) \in G) \implies b_1 = b_2$)
- Combinando le due condizioni (dalle tue note!): $\forall a \in A, \exists! b \in B$ tale che $(a, b) \in G$.
- Notazione funzionale: Se $(a, b) \in G$, scriviamo $f(a) = b$. b è detta **immagine** di a tramite f. a è una **controimmagine** di b.

> **Differenza Chiave: In una relazione generica, un elemento di A può essere collegato a zero, uno o molti elementi di B. In una funzione, ogni elemento di A *deve* essere collegato a *esattamente un* elemento di B.**

- **Esempi (dalle tue note - Pagine 24-27):**
  - Consideriamo relazioni $G \subseteq \mathbb{Z} \times \mathbb{Z}$. Quali sono funzioni $f : \mathbb{Z} \to \mathbb{Z}$?
    - $G_1 = \{(a, b) \mid a = |b|\}$: **NO**. Se $a = 1$, b può essere 1 o -1 (manca unicità). Se $a = -1$, non esiste b (manca esistenza).
    - $G_2 = \{(a, b) \mid |a| = b\}$: **SÌ**. Per ogni $a \in \mathbb{Z}$, $|a|$ è un unico intero $b \geq 0$. $f_2(a) = |a|$.
    - $G_3 = \{(a, b) \mid |a| = |b|\}$: **NO**. Se $a = 1$, b può essere 1 o -1 (manca unicità).
    - $G_4 = \{(a, b) \mid a^2 = b\}$: **SÌ**. Per ogni $a \in \mathbb{Z}$, a^2 è un unico intero $b \geq 0$. $f_4(a) = a^2$.
    - $G_5 = \{(a, b) \mid a = b^2\}$: **NO**. Se $a = 1$, b può essere 1 o -1 (manca unicità). Se $a = -1$ o $a = 2$, non esiste $b \in \mathbb{Z}$ (manca esistenza per alcuni a).
  - Consideriamo $A = \{a, b, c\}, B = \{1, 2, 3\}$.
    - $G = \{(a, 1), (b, 1), (c, 1)\}$: **SÌ**. È una funzione costante. $f(a) = 1, f(b) = 1, f(c) = 1$.
    - $G = \{(a, 1), (b, 2), (a, 3)\}$: **NO**. L'elemento a è associato a due valori diversi (1 e 3, manca unicità). Inoltre, c non è associato a nessun valore (manca esistenza).
  - Consideriamo relazioni $G \subseteq \mathbb{N} \times \mathbb{N}$ (assumiamo $\mathbb{N} = \{1, 2, 3, \dots\}$).
    - $G_1 = \{(a, b) \mid a = 2^b\}$: **NO** (come funzione $f : \mathbb{N} \to \mathbb{N}$). Se $a = 3$, non esiste $b \in \mathbb{N}$ tale che $3 = 2^b$. (Manca esistenza per molti a).
    - $G_2 = \{(a, b) \mid b = 2^a\}$: **SÌ**. Per ogni $a \in \mathbb{N}$, 2^a è un unico numero naturale b. $f_2(a) = 2^a$.
- #tag/funzione Funzione (matematica) Dominio (matematica) Codominio Immagine (matematica)

3.4 Altre Operazioni e Concetti sugli Insiemi

- **Unione:** $A \cup B = \{x \mid x \in A \vee x \in B\}$ (elementi in A OR in B) Unione di Insiemi
- **Intersezione:** $A \cap B = \{x \mid x \in A \wedge x \in B\}$ (elementi in A AND in B) Intersezione di Insiemi
- **Differenza:** $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$ (elementi in A ma NOT in B) Differenza tra Insiemi
- **Complemento:** $A^c = U \setminus A = \{x \in U \mid x \notin A\}$ (elementi non in A, rispetto a un universo U) Insieme Complementare
- **Differenza Simmetrica (XOR per insiemi):**

- Simbolo: $A \Delta B$
- Definizione 1 (dalle tue note!): $A \Delta B = (A \setminus B) \cup (B \setminus A)$ (Elementi che sono in A ma non in B, oppure in B ma non in A)
- Definizione 2 (equivalente, dalle tue note!): $A \Delta B = (A \cup B) \setminus (A \cap B)$ (Elementi che sono nell'unione, ma non nell'intersezione)
- Proprietà (dalle tue note!): La differenza simmetrica è **associativa**: $(A \Delta B) \Delta C = A \Delta (B \Delta C)$. (La dimostrazione può essere complessa, coinvolge l'analisi dei casi o l'uso delle funzioni caratteristiche). #tag/xor-insiemi Differenza Simmetrica Associatività Differenza Simmetrica

---

Riepilogo Veloce

- Abbiamo definito i **connettivi logici** ($\neg, \wedge, \vee, \implies, \iff$) e visto le loro **tavole di verità**.
- Abbiamo esplorato **equivalenze logiche** importanti come De Morgan, contrapposizione e l'equivalenza tra implicazione e disgiunzione.
- Abbiamo distinto **tautologie** (sempre vere) e **contraddizioni** (sempre false).
- Abbiamo introdotto i **predicati** (formule con variabili) e i **quantificatori** ($\forall, \exists, \exists!$) per parlare di quantità.
- Abbiamo definito gli **insiemi**, il **prodotto cartesiano** ($A \times B$), le **relazioni** (sottoinsiemi di $A \times B$) e le **funzioni** (relazioni speciali dove ogni input ha un unico output).
- Abbiamo visto le operazioni fondamentali tra insiemi ($\cup, \cap, \setminus, \Delta, ^c$).

Prossimi Passi

- Rileggi questi appunti con calma. Ci sono parti che non sono chiare? Usa i link `[[...]]` per creare nuove note o collegarti a note esistenti per approfondire!
- Prova a fare qualche esempio tu stesso/a. Crea piccole tavole di verità o elenca gli elementi di un prodotto cartesiano.
- Pensa a come questi concetti si collegano. Ad esempio, come useresti i quantificatori per definire l'unione di due insiemi? ($x \in A \cup B \iff (x \in A) \vee (x \in B)$).

Lezione 2: Logica Avanzata, Funzioni e Partizioni

Data: 14/03/2025 (come da note)
Argomenti: Tautologie (implicazione, bicondizionale), Analisi argomentazioni, Negazione e ordine quantificatori, Immagine e Controimmagine di funzioni, Funzioni Iniettive, Partizioni.

#tag/logica #tag/logica-predicati #tag/quantificatori #tag/settheory #tag/functions #tag/injectivity #tag/partitions #tag/algebra-avanzata

---

1. Ancora Qualche Tautologia e Equivalenza Logica

Riprendiamo e approfondiamo alcune importanti leggi logiche.

- **Non-Associatività dell'Implicazione:**

  Attenzione! L'implicazione NON è associativa in generale.
  $(a \implies b) \implies c$ **NON** è logicamente equivalente a $a \implies (b \implies c)$.
  Non-Associatività Implicazione

- **Transitività dell'Implicazione (Sillogismo Ipotetico):** (Già visto, ma fondamentale!)
  - Formula: $((a \implies b) \wedge (b \implies c)) \implies (a \implies c)$
  - Questa formula è una **tautologia**. Significa: Se a implica b, e b implica c, allora a implica c.
  - *Dimostrazione alternativa (usando equivalenza $P \implies Q \iff \neg P \vee Q$):*
    1. Partiamo da: $((a \implies b) \wedge (b \implies c))$
    2. Sostituiamo le implicazioni: $((\neg a \vee b) \wedge (\neg b \vee c))$
    3. Vogliamo dimostrare che questo implica $(a \implies c)$, cioè $(\neg a \vee c)$.
    4. L'intera espressione è: $((\neg a \vee b) \wedge (\neg b \vee c)) \implies (\neg a \vee c)$
    5. Questa implicazione è una tautologia (si può verificare con tavola di verità o altri metodi come la risoluzione). L'idea intuitiva è che se valgono le premesse, o $\neg a$ è vera (e quindi $\neg a \vee c$ è vera), oppure a è vera. Se a è vera, dalla prima premessa $(\neg a \vee b)$ otteniamo b. Dalla seconda premessa $(\neg b \vee c)$ otteniamo c. Quindi in ogni caso otteniamo $(\neg a \vee c)$.
  - Legge di Transitività (Sillogismo Ipotetico)
- **Bicondizionale come Doppia Implicazione:**
  - Formula: $(a \iff b) \iff ((a \implies b) \wedge (b \implies a))$

- Questa è una **tautologia** e spesso è la *definizione* del bicondizionale. Significa che $a \iff b$ è vero se e solo se a implica b E b implica a.

Verifica Equivalenza (Bicondizionale $\iff$ Doppia Implicazione):

a	b	$a \iff b$	$a \implies b$	$b \implies a$	$(a \implies b) \land (b \implies a)$	$(a \iff b) \iff ((a \implies b) \land (b \implies a))$
V	V	V	V	V	V	V
V	F	F	F	V	F	V
F	V	F	V	F	F	V
F	F	V	V	V	V	V

- Bicondizionale
- **Contrapposizione (Ripasso):**
  - Formula: $(a \implies b) \iff (\neg b \implies \neg a)$
  - Questa è una **tautologia** fondamentale. Un'implicazione è equivalente alla sua contrapposta.

Verifica Equivalenza (Implicazione $\iff$ Contrapposta): (Già vista, ma utile ripeterla)

a	b	$a \implies b$	$\neg b$	$\neg a$	$\neg b \implies \neg a$	$(a \implies b) \iff (\neg b \implies \neg a)$
V	V	V	F	F	V	V
V	F	F	V	F	F	V
F	V	V	F	V	V	V
F	F	V	V	V	V	V

- Legge di Contrapposizione

1.1 Analisi di un Argomento Logico (Esempio "Multiplo di")

Consideriamo le seguenti proposizioni:

- p: "essere multiplo di 2" (cioè essere pari)
- q: "essere multiplo di 3"
- r: "essere multiplo di 6"

Analizziamo le implicazioni numerate nelle tue note (Pag 4):

1. **(1)** $(p \land q) \implies r$
   - Traduzione: "Se un numero è multiplo di 2 E multiplo di 3, allora è multiplo di 6".
   - **Valore di Verità: VERO**. Questa è una proprietà aritmetica fondamentale (poiché 2 e 3 sono coprimi).
2. **(2)** $(\neg p \land \neg q) \implies \neg r$
   - Traduzione: "Se un numero NON è multiplo di 2 E NON è multiplo di 3, allora NON è multiplo di 6".
   - **Valore di Verità: VERO**. Se non è multiplo di 2, non può essere multiplo di 6. Se non è multiplo di 3, non può essere multiplo di 6. Quindi se non è né multiplo di 2 né di 3, a maggior ragione non è multiplo di 6.
   - **Attenzione: Questa NON è la contrapposta di (1)! La contrapposta di $(p \land q) \implies r$ è $\neg r \implies \neg(p \land q)$, che per De Morgan diventa $\neg r \implies (\neg p \lor \neg q)$.**
3. **(3)** $(\neg p \lor \neg q) \implies \neg r$
   - Traduzione: "Se un numero NON è multiplo di 2 OPPURE NON è multiplo di 3, allora NON è multiplo di 6".
   - **Valore di Verità: VERO**. Se non è multiplo di 2, non può essere multiplo di 6. Se non è multiplo di 3, non può essere multiplo di 6. Quindi, se vale almeno una delle due negazioni, non può essere multiplo di 6.
   - **Questa è equivalente alla contrapposta di (1), cioè $\neg r \implies (\neg p \lor \neg q)$. Quindi, poiché (1) è vera, anche (3) deve essere vera.**
4. **(4)** $\neg r \implies (\neg p \land \neg q)$
   - Traduzione: "Se un numero NON è multiplo di 6, allora NON è multiplo di 2 E NON è multiplo di 3".
   - **Valore di Verità: FALSO**. Controesempio: il numero 4. Non è multiplo di 6, ma è multiplo di 2 (quindi $\neg p$ è falso). Controesempio: il numero 9. Non è multiplo di 6, ma è multiplo di 3 (quindi $\neg q$ è falso).
5. **(5)** $\neg r \implies (\neg p \lor \neg q)$
   - Traduzione: "Se un numero NON è multiplo di 6, allora NON è multiplo di 2 OPPURE NON è multiplo di 3".
   - **Valore di Verità: VERO**. Questa è la contrapposta di (1) e anche equivalente a (3). Se un numero non è multiplo di 6, significa che gli manca almeno uno dei fattori primi 2 o 3. Quindi o non è multiplo di 2, o non è multiplo di 3 (o entrambi).

Analisi Argomento

- L'implicazione (1) è vera per definizione di multiplo di 6.
- L'implicazione (2) è vera, ma non è legata a (1) da regole semplici come la contrapposizione.
- L'implicazione (3) è vera ed è equivalente alla contrapposta di (1).
- L'implicazione (4) è falsa.
- L'implicazione (5) è vera ed è la contrapposta di (1).

---

2. Quantificatori: Negazione e Ordine

Riprendiamo i quantificatori e vediamo come negarli e quanto sia importante il loro ordine.

2.1 Variabili Libere e Vincolate (Ripasso con Esempi)

Ricorda: una variabile è **vincolata** se è sotto l'azione di un quantificatore ($\forall$ o $\exists$). Altrimenti è **libera**.

- Esempio 1 (Pag 6): $(\forall x(x^2 < x)) \vee (|x| > 1)$
  - Nel primo pezzo `∀x(x² < x)`, la `x` è **vincolata** dal $\forall$.
  - Nel secondo pezzo `|x| > 1`, la `x` è **libera**.
  - Poiché c'è una variabile libera, l'intera formula è **aperta**. Il suo valore di verità dipende da cosa sostituiamo alla `x` libera.
  - Se l'universo è $\mathbb{R}$:
    - Se $x = 5$, la formula diventa $(\forall y(y^2 < y)) \vee (|5| > 1)$. Il primo pezzo è Falso (non tutti i reali y soddisfano $y^2 < y$), il secondo è Vero ($5 > 1$). Falso $\vee$ Vero = **Vero**.
    - Se $x = 0.5$, la formula diventa $(\forall y(y^2 < y)) \vee (|0.5| > 1)$. Il primo pezzo è Falso, il secondo è Falso ($0.5 \not> 1$). Falso $\vee$ Falso = **Falso**.
- Esempio 2 (Pag 7): $\forall x(xy = y)$
  - La `x` è **vincolata** dal $\forall$.
  - La `y` è **libera**.
  - Formula **aperta**. Dipende dal valore di `y`.
  - Se l'universo è $\mathbb{R}$:
    - Se $y = 0$, diventa $\forall x(x \cdot 0 = 0)$, che è **Vero**.
    - Se $y = 1$, diventa $\forall x(x \cdot 1 = 1)$, che è **Falso** (vero solo per $x = 1$).
- Esempio 3 (Pag 7): $\forall x(\exists y(xy = y))$
  - La `x` è **vincolata** dal $\forall$.
  - La `y` è **vincolata** dal $\exists$.
  - Non ci sono variabili libere. Formula **chiusa**. Ha un valore di verità definito.
  - Significato: "Per ogni x, esiste almeno un y tale che xy = y".
  - Se l'universo è $\mathbb{R}$: **Vero**. Per qualsiasi x, possiamo scegliere $y = 0$. Allora $x \cdot 0 = 0$, quindi l'uguaglianza è soddisfatta.

2.2 Negazione dei Quantificatori (Leggi di De Morgan per Quantificatori)

Come si nega un'affermazione con $\forall$ o $\exists$?

- **Negazione dell'Universale:** Negare che "tutti hanno una proprietà" significa dire che "esiste almeno uno che NON ha quella proprietà".
  - Formula: $\neg(\forall x P(x)) \iff \exists x(\neg P(x))$
  - Esempio: Negare "Tutti gli studenti hanno passato l'esame" ($\forall x S(x)$) significa "Esiste almeno uno studente che NON ha passato l'esame" ($\exists x(\neg S(x))$).
- **Negazione dell'Esistenziale:** Negare che "esiste almeno uno con una proprietà" significa dire che "tutti NON hanno quella proprietà".
  - Formula: $\neg(\exists x P(x)) \iff \forall x(\neg P(x))$
  - Esempio: Negare "Esiste un numero reale il cui quadrato è negativo" ($\exists x(x^2 < 0)$) significa "Per tutti i numeri reali, il loro quadrato NON è negativo" ($\forall x \neg(x^2 < 0)$, cioè $\forall x(x^2 \geq 0)$).

Queste regole sono fondamentali per fare dimostrazioni per assurdo o per capire cosa significa falsificare un'affermazione universale o esistenziale.

Negazione dei Quantificatori

2.3 Ordine dei Quantificatori

L'ordine in cui appaiono quantificatori diversi è **cruciale** e cambia il significato della frase!

Consideriamo un predicato $\varphi(x,y)$ con due variabili.

- $\forall x \exists y \, \varphi(x,y)$: "Per ogni x, esiste (almeno) un y (che può dipendere da x) tale che $\varphi(x,y)$ è vera."
  - Esempio (Universo $\mathbb{R}$): $\forall x \exists y (y > x)$. ("Per ogni numero reale x, esiste un numero reale y più grande di x"). **VERO** (basta prendere $y = x + 1$). La scelta di y dipende da x.
- $\exists y \forall x \, \varphi(x,y)$: "Esiste (almeno) un y (fisso, lo stesso per tutti) tale che per ogni x, $\varphi(x,y)$ è vera."
  - Esempio (Universo $\mathbb{R}$): $\exists y \forall x (y > x)$. ("Esiste un numero reale y che è più grande di tutti i numeri reali x"). **FALSO**. Non esiste un numero reale massimo.

> ⚠ **In generale:** $\exists y \forall x \, \varphi(x,y) \implies \forall x \exists y \, \varphi(x,y)$
>
> L'implicazione inversa **NON** vale! Se per ogni x trovo un y *diverso*, non è detto che esista un y *unico* che vada bene per tutti gli x.

- Esempio dalle note (Pag 8): $\varphi(x,y)$ è $x \cdot y = x$. Universo $\mathbb{N} = \{1, 2, 3, \dots\}$.
  - **(1)** $\forall x \in \mathbb{N}, \exists y \in \mathbb{N}(x \cdot y = x)$**?**
    - Significato: "Per ogni numero naturale x, esiste un naturale y tale che xy=x".
    - **VERO**. Basta scegliere $y = 1$. $x \cdot 1 = x$ è vero per ogni $x \in \mathbb{N}$.
  - **(2)** $\exists y \in \mathbb{N}, \forall x \in \mathbb{N}(x \cdot y = x)$**?**
    - Significato: "Esiste un numero naturale y (fisso) tale che per tutti i naturali x, si ha xy=x".
    - **VERO**. Possiamo scegliere $y = 1$. Per questo y fisso, vale $x \cdot 1 = x$ per tutti gli $x \in \mathbb{N}$.
  - In questo caso specifico, entrambe le affermazioni sono vere e quindi equivalenti. Ma non è sempre così!

---

3. Funzioni: Immagine e Controimmagine di Insiemi

Data una funzione $f : A \to B$.

3.1 Immagine di un Sottoinsieme del Dominio

- Dato un sottoinsieme $X \subseteq A$, l'**immagine di X tramite f** è l'insieme di tutti gli elementi del codominio B che sono "raggiunti" da almeno un elemento di X.
- Notazione (dalle note): $\vec{f}(X)$ o $f(X)$
- Definizione Formale: $\vec{f}(X) = \{f(x) \mid x \in X\}$
- Proprietà: $\vec{f}(X) \subseteq B$

> ✎ **L'immagine $\vec{f}(X)$ contiene i *risultati* della funzione applicata agli elementi di X.**

- Esempio (Pag 13): $f : \mathbb{Z} \to \mathbb{Z}$ definita da $f(x) = |x|$. Sia $X = \{-2, 5, -5\}$.
  - $\vec{f}(X) = \{f(-2), f(5), f(-5)\} = \{|-2|, |5|, |-5|\} = \{2, 5, 5\} = \{2, 5\}$. (Ricorda: gli insiemi non hanno ripetizioni).
- Proprietà (Pag 14): $\vec{f}(\emptyset) = \emptyset$. (L'immagine dell'insieme vuoto è l'insieme vuoto).
- Esempio (Pag 14): $g : \mathbb{Z} \to \mathbb{N}$ definita da $g(x) = |x|$. (Assumiamo $\mathbb{N} = \{0, 1, 2, \dots\}$ qui).
  - $\vec{g}(\mathbb{Z}) = \{|x| \mid x \in \mathbb{Z}\} = \{0, 1, 2, 3, \dots\} = \mathbb{N}$. (L'immagine dell'intero dominio è l'insieme dei numeri naturali, detto anche **Immagine della funzione**, $Im(g)$).
- Esempio (Pag 14): $h : \mathbb{Z} \to \mathbb{Z}$ definita da $h(x) = 3$. (Funzione costante).
  - $\vec{h}(\mathbb{Z}) = \{h(x) \mid x \in \mathbb{Z}\} = \{3 \mid x \in \mathbb{Z}\} = \{3\}$. (L'immagine dell'intero dominio è solo l'elemento 3).

3.2 Controimmagine (o Preimmagine) di un Sottoinsieme del Codominio

- Dato un sottoinsieme $Y \subseteq B$, la **controimmagine (o preimmagine) di Y tramite f** è l'insieme di tutti gli elementi del dominio A le cui immagini cadono dentro Y.
- Notazione (dalle note): $\overleftarrow{f}(Y)$ o $f^{-1}(Y)$ (Attenzione: f^{-1} qui **non** significa funzione inversa! È solo una notazione per la controimmagine).
- Definizione Formale: $\overleftarrow{f}(Y) = \{x \in A \mid f(x) \in Y\}$
- Proprietà: $\overleftarrow{f}(Y) \subseteq A$

> ✎ **La controimmagine $\overleftarrow{f}(Y)$ contiene gli *input* della funzione che producono risultati appartenenti a Y.**

- Esempio (Pag 13): $f : \mathbb{Z} \to \mathbb{Z}$ definita da $f(x) = |x|$. Sia $Y = \{2, 5\}$.
  - $\overleftarrow{f}(Y) = \{x \in \mathbb{Z} \mid f(x) \in \{2, 5\}\} = \{x \in \mathbb{Z} \mid |x| = 2 \text{ oppure } |x| = 5\}$
  - $\overleftarrow{f}(Y) = \{-2, 2, -5, 5\}$.
- Esempio (Pag 13): $f(x) = |x|$. Sia $Y = \{-2\}$.
  - $\overleftarrow{f}(Y) = \{x \in \mathbb{Z} \mid f(x) \in \{-2\}\} = \{x \in \mathbb{Z} \mid |x| = -2\}$

- $\overleftarrow{f}(Y) = \emptyset$. (Nessun intero ha valore assoluto -2).

- Proprietà (Pag 15): $\overleftarrow{f}(\emptyset) = \emptyset$. (La controimmagine dell'insieme vuoto è l'insieme vuoto).
- Proprietà (Pag 15): $\overleftarrow{f}(B) = \{x \in A \mid f(x) \in B\} = A$. (La controimmagine dell'intero codominio è l'intero dominio).

Immagine di una Funzione Controimmagine

---

4. Funzioni Iniettive (One-to-One)

Una proprietà molto importante delle funzioni.

- **Definizione Intuitiva:** Una funzione è **iniettiva** se manda elementi distinti del dominio in elementi distinti del codominio. Non "schiaccia" mai due input diversi sullo stesso output.
- **Definizione Formale:** Una funzione $f : A \to B$ è iniettiva se:

$$\forall x_1, x_2 \in A, \quad f(x_1) = f(x_2) \implies x_1 = x_2$$

  - **Spiegazione:** Se prendi due elementi qualsiasi nel dominio, x_1 e x_2, e scopri che hanno la stessa immagine ($f(x_1) = f(x_2)$), allora devi concludere che stavi guardando lo stesso elemento fin dall'inizio ($x_1 = x_2$).
- **Forma Contrapposta (Spesso utile per le dimostrazioni):**

$$\forall x_1, x_2 \in A, \quad x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$$

  - **Spiegazione:** Se prendi due elementi *distinti* nel dominio, allora le loro immagini devono essere *distinte*.
- **Negazione (Come dimostrare che una funzione NON è iniettiva):**

$$\exists x_1, x_2 \in A : x_1 \neq x_2 \wedge f(x_1) = f(x_2)$$

  - **Spiegazione:** Basta trovare *almeno una coppia* di elementi distinti nel dominio che vengono mandati dalla funzione nello stesso elemento del codominio.
- **Caratterizzazione tramite Controimmagine (Molto utile! Pag 17-18):**

  Una funzione $f : A \to B$ è iniettiva se e solo se per ogni elemento b del codominio B, la sua controimmagine $\overleftarrow{f}(\{b\})$ contiene **al massimo un elemento**.

$$f \text{ è iniettiva} \iff (\forall b \in B, |\overleftarrow{f}(\{b\})| \leq 1)$$

  - **Spiegazione:** Se una funzione fosse non iniettiva, esisterebbero $x_1 \neq x_2$ con $f(x_1) = f(x_2) = b$. Ma allora la controimmagine di b, $\overleftarrow{f}(\{b\})$, conterrebbe sia x_1 che x_2, e quindi avrebbe cardinalità ≥ 2. Viceversa, se la controimmagine di ogni b ha al massimo un elemento, non possono esistere due x distinti che mappano allo stesso b.

Per dimostrare che f è iniettiva, parti da $f(x_1) = f(x_2)$ e cerca di dedurre $x_1 = x_2$.

Per dimostrare che f NON è iniettiva, trova due $x_1 \neq x_2$ specifici tali che $f(x_1) = f(x_2)$.

Funzione Iniettiva

4.1 Esempi di Iniettività

- **Esempio 1 (Pag 19):** $f : \mathbb{N} \setminus \{0, 1\} \to \mathbb{N}$, dove $a = p_1^{n_1} \cdots p_t^{n_t}$ (fattorizzazione unica in primi) e $f(a) = n_1 + n_2 + \cdots + n_t$ (somma degli esponenti).
  - È iniettiva? **NO**.
  - Controesempio: $a = 4 = 2^2$, $f(4) = 2$. $a = 6 = 2^1 \cdot 3^1$, $f(6) = 1 + 1 = 2$.
  - Abbiamo $4 \neq 6$ ma $f(4) = f(6) = 2$.
- **Esempio 2 (Pag 21):** $A = \{1, 2, 3\}$. $f : A \times A \to \mathbb{N}$ definita da $f((a, b)) = a^b$.
  - È iniettiva? **NO**.
  - Controesempio (dalle note): $(1, 1) \neq (1, 2)$. Ma $f((1, 1)) = 1^1 = 1$ e $f((1, 2)) = 1^2 = 1$.
  - Quindi $f((1, 1)) = f((1, 2))$.
- **Esempio 3 (Pag 22):** $f : \mathbb{N} \to \mathbb{N}$ (qui $\mathbb{N} = \{0, 1, 2, \dots\}$ probabilmente)

$$f(n) = \begin{cases} 2n & \text{se } n \text{ è dispari} \\ n & \text{se } n \text{ è pari} \end{cases}$$

  - È iniettiva? **NO**.
  - Controesempio: $n = 1$ (dispari), $f(1) = 2 \cdot 1 = 2$. $n = 2$ (pari), $f(2) = 2$.
  - Abbiamo $1 \neq 2$ ma $f(1) = f(2) = 2$.
- **Esempio 4 (Pag 23-24):** $f : \mathbb{N} \to \mathbb{Z}$ (qui $\mathbb{N} = \{0, 1, 2, \dots\}$ probabilmente)

$$f(n) = \begin{cases} n/2 & \text{se } n \text{ è pari} \\ -(n+1)/2 & \text{se } n \text{ è dispari} \end{cases}$$

- È iniettiva? **SÌ**. Dimostriamolo per casi, partendo da $f(n) = f(m)$.
  - **Caso 1:** n, m entrambi pari. $f(n) = n/2$, $f(m) = m/2$. Se $n/2 = m/2$, allora $n = m$. OK.
  - **Caso 2:** n, m entrambi dispari. $f(n) = -(n+1)/2$, $f(m) = -(m+1)/2$. Se $-(n+1)/2 = -(m+1)/2$, allora $(n+1)/2 = (m+1)/2$, quindi $n+1 = m+1$, e $n = m$. OK.
  - **Caso 3:** n pari, m dispari. $f(n) = n/2$, $f(m) = -(m+1)/2$. Se $f(n) = f(m)$, allora $n/2 = -(m+1)/2$. Poiché $n \geq 0$, $n/2 \geq 0$. Poiché $m \geq 0$ e dispari, $m+1 > 0$, quindi $-(m+1)/2 < 0$. Non è possibile che $n/2 = -(m+1)/2$. Questo caso non può verificarsi se $f(n) = f(m)$. OK.
  - In tutti i casi possibili in cui $f(n) = f(m)$, abbiamo dedotto che $n = m$. Quindi la funzione è iniettiva.
- **Esempio 5 (Pag 25):** Sia S un insieme non vuoto. $f : P(S) \to P(S)$ definita da $f(X) = S \setminus X$ (complemento relativo a S).
  - È iniettiva? **SÌ**.
  - Dimostrazione: Supponiamo $f(X) = f(Y)$. Questo significa $S \setminus X = S \setminus Y$. Vogliamo dimostrare che $X = Y$.
  - Prendiamo il complemento rispetto a S di entrambi i lati: $S \setminus (S \setminus X) = S \setminus (S \setminus Y)$.
  - Ma il complemento del complemento di un insieme è l'insieme stesso: $S \setminus (S \setminus A) = A$.
  - Quindi otteniamo $X = Y$. Poiché $f(X) = f(Y)$ implica $X = Y$, la funzione è iniettiva.
- **Esempio 6 (Pag 29):** $f : \mathbb{N} \to \mathbb{N}$ (assumiamo $\mathbb{N} = \{0, 1, 2, \dots\}$) definita da $f(a) = \text{rest}(a, 3)$ (resto della divisione di a per 3).
  - È iniettiva? **NO**.
  - Controesempio: $f(3) = \text{rest}(3, 3) = 0$. $f(6) = \text{rest}(6, 3) = 0$.
  - Abbiamo $3 \neq 6$ ma $f(3) = f(6) = 0$.

---

5. Partizioni di un Insieme

Un modo per "dividere" un insieme in pezzi disgiunti.

- Sia S un insieme non vuoto ($S \neq \emptyset$).
- Una **partizione** di S è una **famiglia** (un insieme) $\mathcal{F}$ di sottoinsiemi di S (cioè $\mathcal{F} \subseteq P(S)$) che soddisfa le seguenti tre condizioni:
  1. **Nessun pezzo è vuoto:** Ogni sottoinsieme nella famiglia $\mathcal{F}$ deve essere non vuoto.
  $$\forall X \in \mathcal{F}, \quad X \neq \emptyset$$
  2. **I pezzi sono disgiunti a due a due:** L'intersezione di due sottoinsiemi *distinti* qualsiasi nella famiglia $\mathcal{F}$ deve essere vuota.
  $$\forall X, Y \in \mathcal{F}, \quad X \neq Y \implies X \cap Y = \emptyset$$
  3. **I pezzi ricoprono tutto l'insieme:** L'unione di tutti i sottoinsiemi nella famiglia $\mathcal{F}$ deve dare l'insieme originale S.
  $$\bigcup_{X \in \mathcal{F}} X = S$$

Immagina di rompere un piatto S. I frammenti X_i formano una partizione: nessun frammento è vuoto, due frammenti diversi non si sovrappongono (a parte i bordi, che qui ignoriamo), e rimettendo insieme tutti i frammenti ottieni il piatto originale.

- **Esempi (Pag 27):** Sia $S = \{a, b, c\}$.
  - **Partizioni Banali:**
    - $\mathcal{F}_1 = \{\{S\}\} = \{\{a, b, c\}\}$. (Un solo pezzo: l'insieme intero).
    - $\mathcal{F}_2 = \{\{a\}, \{b\}, \{c\}\}$. (Ogni pezzo è un singolo elemento).
  - **Altre Partizioni:**
    - $\mathcal{F}_3 = \{\{a\}, \{b, c\}\}$
    - $\mathcal{F}_4 = \{\{b\}, \{a, c\}\}$
    - $\mathcal{F}_5 = \{\{c\}, \{a, b\}\}$
  - La famiglia $\mathcal{L} = \{\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3, \mathcal{F}_4, \mathcal{F}_5\}$ è l'insieme di *tutte* le possibili partizioni di $S = \{a, b, c\}$.
- **Esempio Funzione (Pag 28):** Sia $\mathcal{L}$ l'insieme di tutte le partizioni di $S = \{a, b, c\}$. Definiamo $g : \mathcal{L} \to \{1, 2, 3\}$ dove $g(\mathcal{F}) = |\mathcal{F}|$ (la cardinalità della partizione, cioè il numero di pezzi).
  - $g(\mathcal{F}_1) = |\{\{a, b, c\}\}| = 1$.
  - $g(\mathcal{F}_2) = |\{\{a\}, \{b\}, \{c\}\}| = 3$.
  - $g(\mathcal{F}_3) = |\{\{a\}, \{b, c\}\}| = 2$.
  - $g(\mathcal{F}_4) = |\{\{b\}, \{a, c\}\}| = 2$.

- $g(\mathcal{F}_5) = |\{\{c\}, \{a, b\}\}| = 2$.
- Consideriamo la controimmagine:
  - $\overleftarrow{g}(\{1\}) = \{\mathcal{F} \in \mathcal{L} \mid |\mathcal{F}| = 1\} = \{\mathcal{F}_1\}$.
  - $\overleftarrow{g}(\{2\}) = \{\mathcal{F} \in \mathcal{L} \mid |\mathcal{F}| = 2\} = \{\mathcal{F}_3, \mathcal{F}_4, \mathcal{F}_5\}$.
  - $\overleftarrow{g}(\{3\}) = \{\mathcal{F} \in \mathcal{L} \mid |\mathcal{F}| = 3\} = \{\mathcal{F}_2\}$.
  - $\overleftarrow{g}(\{0\}) = \emptyset$.

Partizione di un insieme

Riepilogo Veloce Lezione 2

- Abbiamo rivisto tautologie importanti come la **transitività** e la **contrapposizione** dell'implicazione, e l'equivalenza del **bicondizionale**.
- Abbiamo analizzato un'argomentazione logica concreta.
- Abbiamo imparato a **negare i quantificatori** ($\neg\forall \iff \exists\neg$, $\neg\exists \iff \forall\neg$).
- Abbiamo visto l'importanza cruciale dell'**ordine dei quantificatori**.
- Abbiamo definito l'**immagine** $\vec{f}(X)$ e la **controimmagine** $\overleftarrow{f}(Y)$ di insiemi tramite una funzione f.
- Abbiamo definito la **funzione iniettiva** (diversi input $\implies$ diversi output) e visto diversi modi per caratterizzarla (definizione formale, contrapposta, negazione, tramite controimmagine di singleton).
- Abbiamo introdotto il concetto di **partizione** di un insieme (divisione in pezzi non vuoti e disgiunti che ricoprono tutto).

Prossimi Passi

- Assicurati di aver compreso bene la differenza tra immagine e controimmagine. Prova a calcolarle per funzioni semplici.
- Fai pratica nel dimostrare se una funzione è iniettiva o meno. Trovare un controesempio è spesso il modo più rapido per dimostrare la non-iniettività.
- Rifletti sul legame tra partizioni e relazioni di equivalenza (lo vedremo presto!).

Lezione 3: Logica, Funzioni (Iniettività, Suriettività, Immagine/Controimmagine), Restrizioni

Data: 18/03/2025 (come da note)
Argomenti: Negazione formule logiche, Verifica tautologie, Proprietà immagine/controimmagine, Funzioni iniettive (recap), Funzioni suriettive, Funzione caratteristica, Uguaglianza funzioni, Restrizione e Prolungamento.

#tag/logica #tag/logica-predicati #tag/functions #tag/injectivity #tag/surjectivity #tag/settheory #tag/algebra-avanzata

---

1. Esercizi e Approfondimenti di Logica

Vediamo come negare formule più complesse e analizziamo qualche altra tautologia.

- **Negazione dell'Implicazione:** Ricordiamo che $p \implies q \iff \neg p \vee q$.
  - Quindi, $\neg(p \implies q) \iff \neg(\neg p \vee q)$.
  - Applicando De Morgan: $\neg(\neg p \vee q) \iff (\neg(\neg p) \wedge \neg q)$.
  - Applicando la doppia negazione: $(\neg(\neg p) \wedge \neg q) \iff (p \wedge \neg q)$.

    Regola di Negazione dell'Implicazione:

    $$\neg(p \implies q) \iff p \wedge \neg q$$

    Spiegazione: Negare "Se piove allora prendo l'ombrello" significa affermare che "Piove E non prendo l'ombrello". È l'unico caso che rende falsa l'implicazione originale.

  - Negazione Implicazione
- **Esercizio 2 (Pag 1):** L'equivalenza $p \implies (q \vee r) \iff ((p \implies q) \vee (p \implies r))$ è una tautologia?
  - Proviamo a usare le equivalenze:
    - Lato sinistro: $p \implies (q \vee r) \iff \neg p \vee (q \vee r)$
    - Lato destro: $(p \implies q) \vee (p \implies r) \iff (\neg p \vee q) \vee (\neg p \vee r)$
    - Usando associatività e idempotenza della $\vee$: $(\neg p \vee q) \vee (\neg p \vee r) \iff \neg p \vee q \vee \neg p \vee r \iff \neg p \vee q \vee r$
  - Confrontiamo i risultati: $\neg p \vee (q \vee r)$ è effettivamente equivalente a $\neg p \vee q \vee r$.
  - **Risposta: SÌ, è una tautologia.** Significa che "Se P implica (Q o R)" è la stessa cosa di "(Se P implica Q) o

(Se P implica R)".
    - Distributività Implicazione su Disgiunzione
- **Esercizio 3 (Pag 1):** Negare $p \implies (q \vee r)$.
    - Usando la regola $\neg(A \implies B) \iff A \wedge \neg B$:
    - $\neg(p \implies (q \vee r)) \iff p \wedge \neg(q \vee r)$
    - Applicando De Morgan a $\neg(q \vee r)$:
    - $p \wedge (\neg q \wedge \neg r)$
- **Esercizio 4 (Pag 1):** Negare $p \implies (q \wedge r)$.
    - $\neg(p \implies (q \wedge r)) \iff p \wedge \neg(q \wedge r)$
    - Applicando De Morgan:
    - $p \wedge (\neg q \vee \neg r)$
- **Esercizio 5 (Pag 1):** Negare $(p \vee q) \implies r$.
    - $\neg((p \vee q) \implies r) \iff (p \vee q) \wedge \neg r$
- **Esercizio 6 (Pag 1):** Negare $(p \wedge q) \implies r$.
    - $\neg((p \wedge q) \implies r) \iff (p \wedge q) \wedge \neg r$
- **Esercizio 7 (Pag 1):** Negare $\forall x(\exists y(\varphi(x,y) \implies \psi(x,y)))$.
    - Applichiamo le regole di negazione passo passo, dall'esterno verso l'interno:
    1. $\neg[\forall x(\dots)] \iff \exists x\neg[(\dots)]$
        - $\exists x\neg(\exists y(\varphi(x,y) \implies \psi(x,y)))$
    2. $\neg[\exists y(\dots)] \iff \forall y\neg[(\dots)]$
        - $\exists x(\forall y\neg(\varphi(x,y) \implies \psi(x,y)))$
    3. $\neg[A \implies B] \iff A \wedge \neg B$
        - $\exists x(\forall y(\varphi(x,y) \wedge \neg\psi(x,y)))$
    - **Risultato:** $\exists x\forall y(\varphi(x,y) \wedge \neg\psi(x,y))$
- **Esercizio 8 (Pag 1):** L'equivalenza $((p \implies q) \implies (q \implies r \wedge s)) \iff ((\neg q) \vee (r \wedge s))$ è una tautologia?
    - Analizziamo il lato sinistro: $(p \implies q) \implies (q \implies (r \wedge s))$
    - Questo **NON** sembra una tautologia standard o facilmente riconducibile. Potrebbe essere un errore di trascrizione o un'affermazione da verificare con una tavola di verità (che sarebbe molto lunga!). Sembra improbabile che sia una tautologia generale senza ulteriori condizioni su p, q, r, s. La nota "è tautologia?" suggerisce che sia una domanda, non un'affermazione.

> **Verifica: Questa equivalenza è corretta o era una domanda da verificare? A prima vista non sembra una tautologia standard.**

---

2. Funzioni: Chiarimenti e Proprietà

2.1 Errore Comune sull'Iniettività (Pag 2)

> **Attenzione a non confondere la definizione di funzione con quella di iniettività!**
>
> - Per **definizione di funzione**, se prendi lo stesso input x, otterrai sempre lo stesso output $f(x)$. Quindi, l'implicazione $x = y \implies f(x) = f(y)$ è **SEMPRE VERA** per qualsiasi funzione.
> - La **definizione di iniettività** richiede l'implicazione inversa: $f(x) = f(y) \implies x = y$. Questo **NON** è vero per tutte le funzioni, ma solo per quelle iniettive.

2.2 Proprietà dell'Immagine $\vec{f}(X)$ (Pag 3)

Sia $f : A \to B$ una funzione e $X \subseteq A$.

- $\vec{f}(\emptyset) = \emptyset$. (L'immagine del vuoto è vuota).
- Se $X \neq \emptyset$, è possibile che $\vec{f}(X) \neq \emptyset$? **Sì, sempre!** Se X contiene almeno un elemento x, allora $\vec{f}(X)$ contiene almeno $f(x)$, quindi non è vuoto.

> **La nota $\vec{f}(X) \neq \emptyset$ nella pagina 3 sembra ridondante se $X \neq \emptyset$. Forse si intendeva qualcos'altro?**

- $\vec{f}(A)$ è l'**immagine dell'intera funzione**, spesso denotata $Im(f)$.
- In generale, $\vec{f}(A) \subseteq B$.
- $\vec{f}(A) = B$ se e solo se f è **suriettiva**. (Lo vedremo meglio tra poco).

2.3 Proprietà della Controimmagine $\overleftarrow{f}(Y)$ (Pag 4)

Sia $f: A \to B$ una funzione e $Y \subseteq B$.

- $\overleftarrow{f}(\emptyset) = \emptyset$. (Gli input la cui immagine è nel vuoto... non esistono!).
- È possibile che $\overleftarrow{f}(Y) = \emptyset$ anche se $Y \neq \emptyset$? **SÌ**.
  - Questo accade se nessun elemento di Y viene "raggiunto" dalla funzione, cioè se Y è disgiunto dall'immagine della funzione ($Y \cap Im(f) = \emptyset$).
  - Esempio: $f(x) = |x|$ da $\mathbb{Z}$ a $\mathbb{Z}$. $\overleftarrow{f}(\{-1, -2\}) = \emptyset$ perché nessun intero ha valore assoluto negativo.
- La nota "solo se è suriettiva" (Pag 4) riferita a $\overleftarrow{f}(Y) \neq \emptyset$ se $Y \neq \emptyset$ **non è corretta** in generale. È vero il contrario per la *suriettività*: f è suriettiva se e solo se $\overleftarrow{f}(\{b\}) \neq \emptyset$ per ogni *singleton* $\{b\}$ con $b \in B$.

2.4 Iniettività e Controimmagine (Recap) (Pag 5)

Come visto nella Lezione 2, una caratterizzazione molto utile:

- $f: A \to B$ è **iniettiva** $\iff$ per ogni $b \in B$, l'insieme $\overleftarrow{f}(\{b\})$ (la controimmagine del singolo elemento b) contiene **al massimo un elemento** (cioè è vuoto o è un singleton).

---

3. Funzioni Suriettive (Onto)

Un'altra proprietà fondamentale delle funzioni.

- **Definizione Intuitiva:** Una funzione è **suriettiva** se ogni elemento del codominio B viene "raggiunto" da almeno un elemento del dominio A. L'immagine della funzione coincide con l'intero codominio.
- **Definizione Formale:** Una funzione $f: A \to B$ è suriettiva se:

$$\forall b \in B, \exists a \in A \text{ tale che } f(a) = b$$

  - **Spiegazione:** Per ogni possibile output b nel codominio, devi essere in grado di trovare almeno un input a nel dominio che produce quell'output.
- **Caratterizzazioni Equivalenti (Pag 25-26):**
  1. Tramite Immagine: f è suriettiva $\iff \vec{f}(A) = B$. (L'immagine dell'intero dominio coincide con l'intero codominio).
  2. Tramite Controimmagine di Singleton: f è suriettiva $\iff \forall b \in B, \overleftarrow{f}(\{b\}) \neq \emptyset$. (La controimmagine di ogni singolo elemento del codominio non è mai vuota).
  3. Tramite Controimmagine di Sottoinsiemi Non Vuoti: f è suriettiva $\iff \forall C \subseteq B \text{ con } C \neq \emptyset$, si ha $\overleftarrow{f}(C) \neq \emptyset$. (Se prendi un qualsiasi sottoinsieme non vuoto del codominio, ci deve essere almeno un elemento nel dominio la cui immagine cade in quel sottoinsieme).

Per dimostrare che f è suriettiva, prendi un generico $b \in B$ e dimostra che esiste un $a \in A$ (spesso trovando una formula per a in termini di b) tale che $f(a) = b$.

Per dimostrare che f NON è suriettiva, trova uno specifico $b \in B$ per cui non esiste nessun $a \in A$ tale che $f(a) = b$.

Funzione Suriettiva

---

4. Esercizi su Iniettività e Suriettività

Analizziamo gli esempi dalle note.

- **Esempio 1 (Pag 5-8):** $S = \{a, \{a\}, b\}$. $P(S) = \{\emptyset, \{a\}, \{\{a\}\}, \{b\}, \{a, \{a\}\}, \{a, b\}, \{\{a\}, b\}, S\}$.
  $f: P(S) \times P(S) \to \{0, 1, \dots, 6\}$ definita da $f(X, Y) = |X \Delta Y|$.
  - **Iniettiva? NO.** (Come mostrato a Pag 6).
    - Sia $X_1 = \{a\}$, $Y_1 = \{b\}$. $X_1 \Delta Y_1 = (X_1 \setminus Y_1) \cup (Y_1 \setminus X_1) = \{a\} \cup \{b\} = \{a, b\}$. $|X_1 \Delta Y_1| = 2$.
    - Sia $X_2 = \{b\}$, $Y_2 = \{a\}$. $X_2 \Delta Y_2 = \{b\} \cup \{a\} = \{a, b\}$. $|X_2 \Delta Y_2| = 2$.
    - Abbiamo $(X_1, Y_1) \neq (X_2, Y_2)$ ma $f(X_1, Y_1) = f(X_2, Y_2) = 2$.
    - La nota a Pag 6 mostra $f(\{\{a\}\}, \{b\}) = f(\{b\}, \{\{a\}\})$. Calcoliamo:
      - $\{\{a\}\} \Delta \{b\} = \{\{a\}, b\}$. Cardinalità 2.
      - $\{b\} \Delta \{\{a\}\} = \{b, \{a\}\}$. Cardinalità 2.
      - Quindi $f(\{\{a\}\}, \{b\}) = f(\{b\}, \{\{a\}\}) = 2$. Conferma la non iniettività.
  - **Suriettiva? NO.** (Come mostrato a Pag 7).

- Il codominio è $\{0,1,2,3,4,5,6\}$. L'insieme S ha 3 elementi. La cardinalità massima di un sottoinsieme di S è 3. La cardinalità massima di $X \Delta Y = (X \cup Y) \setminus (X \cap Y)$ è $|X \cup Y|$, che è al massimo $|S| = 3$.
- Quindi $|X \Delta Y|$ può valere al massimo 3. Non potrà mai valere 4, 5, o 6.
- Ad esempio, non esiste nessuna coppia (X, Y) tale che $f(X, Y) = 4$.
- La controimmagine $\overleftarrow{f}(\{4\})$ è $\emptyset$. Poiché esiste un elemento del codominio (4) con controimmagine vuota, la funzione non è suriettiva.

- **Esempio 2 (Pag 9-10): Funzione Caratteristica**
  Sia $S \neq \emptyset$ e $A \subseteq S$. La **funzione caratteristica** di A in S è:

$$\chi_A : S \to \{0,1\}$$

$$\chi_A(x) = \begin{cases} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A \text{ (cioè } x \in S \setminus A) \end{cases}$$

  - **Iniettiva?** Dipende. È iniettiva solo se S ha al massimo un elemento. Se S ha due elementi s_1, s_2 e $A = \{s_1\}$, allora $\chi_A(s_1) = 1$, $\chi_A(s_2) = 0$. Se $A = S$, $\chi_A(s_1) = \chi_A(s_2) = 1$ (non iniettiva se $|S| > 1$). Se $A = \emptyset$, $\chi_A(s_1) = \chi_A(s_2) = 0$ (non iniettiva se $|S| > 1$).
  - **Suriettiva?** È suriettiva se e solo se esistono elementi sia dentro A sia fuori A. Cioè, se $A \neq \emptyset$ AND $A \neq S$.
    - Se $A = \emptyset$, l'immagine è solo $\{0\}$. Non suriettiva (su $\{0,1\}$).
    - Se $A = S$, l'immagine è solo $\{1\}$. Non suriettiva (su $\{0,1\}$).
    - Se $\emptyset \subset A \subset S$, allora esistono $x \in A$ (quindi $\chi_A(x) = 1$) ed esistono $y \notin A$ (quindi $\chi_A(y) = 0$). L'immagine è $\{0,1\}$, quindi è suriettiva.
  - **Controimmagini:**
    - $\overleftarrow{\chi_A}(\{1\}) = \{x \in S \mid \chi_A(x) = 1\} = A$.
    - $\overleftarrow{\chi_A}(\{0\}) = \{x \in S \mid \chi_A(x) = 0\} = S \setminus A$. (Complementare di A in S).
    - $\overleftarrow{\chi_A}(\{0,1\}) = S$.
    - $\overleftarrow{\chi_A}(\emptyset) = \emptyset$.
  - Funzione Caratteristica
- **Esempio 3 (Pag 11-12):** $f : \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{N}^*$ definita da $f(n, m) = n^m$. (Qui $\mathbb{N}^* = \{1, 2, 3, \dots\}$).
  - **Iniettiva? NO.**
    - Controesempio: $f(2,4) = 2^4 = 16$. $f(4,2) = 4^2 = 16$.
    - Abbiamo $(2,4) \neq (4,2)$ ma $f(2,4) = f(4,2) = 16$.
  - **Suriettiva?** Dobbiamo chiederci: per ogni $a \in \mathbb{N}^*$, esistono $n, m \in \mathbb{N}^*$ tali che $n^m = a$?
    - **SÌ**. Per ogni $a \in \mathbb{N}^*$, possiamo sempre scegliere $n = a$ e $m = 1$. Entrambi sono in $\mathbb{N}^*$. Allora $f(a,1) = a^1 = a$.
    - Quindi ogni elemento a del codominio ha almeno una controimmagine (la coppia $(a,1)$). La funzione è suriettiva.
- **Esempio 4 (Pag 13-15):** $S = \{a, b, c\}$. $f : P(S) \times P(S) \to P(S)$ definita da $f(X, Y) = X \setminus Y$.
  - **Iniettiva? NO.**
    - Controesempio (dalle note): $f(\{a\}, \{a\}) = \{a\} \setminus \{a\} = \emptyset$. $f(\{b\}, \{b\}) = \{b\} \setminus \{b\} = \emptyset$.
    - Abbiamo $(\{a\}, \{a\}) \neq (\{b\}, \{b\})$ ma $f(\{a\}, \{a\}) = f(\{b\}, \{b\}) = \emptyset$.
  - **Suriettiva? SÌ.**
    - Dobbiamo dimostrare che per ogni $Z \in P(S)$ (cioè per ogni $Z \subseteq S$), esistono $X, Y \in P(S)$ tali che $X \setminus Y = Z$.
    - Possiamo sempre scegliere $X = Z$ e $Y = \emptyset$. Entrambi sono sottoinsiemi di S (appartengono a $P(S)$).
    - Allora $f(Z, \emptyset) = Z \setminus \emptyset = Z$.
    - Quindi ogni elemento Z del codominio ha almeno una controimmagine (la coppia $(Z, \emptyset)$). La funzione è suriettiva.
  - **Proprietà $X \setminus Y = \emptyset \iff X \subseteq Y$ (Pag 15):**
    - ($\implies$) Se $X \setminus Y = \emptyset$, significa $\{x \in X \mid x \notin Y\} = \emptyset$. Questo vuol dire che non esiste nessun elemento x che sta in X ma non in Y. Quindi, ogni elemento di X deve stare anche in Y. Cioè $X \subseteq Y$.
    - ($\impliedby$) Se $X \subseteq Y$, allora ogni elemento $x \in X$ è anche in Y. Quindi non ci sono elementi x tali che ($x \in X$ e $x \notin Y$). Perciò l'insieme $\{x \in X \mid x \notin Y\}$ è vuoto. Cioè $X \setminus Y = \emptyset$.

---

5. Uguaglianza, Restrizione, Prolungamento

5.1 Uguaglianza tra Funzioni (Pag 16)

Due funzioni f e g sono **uguali** ($f = g$) se e solo se soddisfano **tutte e tre** le seguenti condizioni:

1. Hanno lo stesso **Dominio**.
2. Hanno lo stesso **Codominio**.
3. Hanno la stessa **legge (o grafo)**, cioè $f(x) = g(x)$ per ogni x nel dominio comune.

- Esempio:
  - $f : \mathbb{N} \to \mathbb{N}$ con $f(a) = 2|a| + 1$. Poiché $a \in \mathbb{N}$, $|a| = a$, quindi $f(a) = 2a + 1$.
  - $g : \mathbb{Z} \to \mathbb{N}$ con $g(a) = 2|a| + 1$.
  - $h : \mathbb{Z} \to \mathbb{Z}$ con $h(a) = 2a + 1$.
  - Qui $f \neq g$ (domini diversi). $g \neq h$ (codomini diversi). $f \neq h$ (domini e codomini diversi).
  - Anche se la "formula" sembra simile, le funzioni sono diverse perché dominio e/o codominio cambiano.

5.2 Restrizione di una Funzione (Pag 22)

- Sia $f : A \to B$ una funzione e sia C un sottoinsieme non vuoto del dominio ($\emptyset \neq C \subseteq A$).
- La **restrizione di f a C**, denotata $f|_C$, è una nuova funzione definita come:

$$f|_C : C \to B$$

$$f|_C(x) = f(x) \quad \text{per ogni } x \in C$$

  - **Spiegazione:** È la stessa funzione f, ma consideriamo solo gli input che provengono dal sottoinsieme C. Il codominio rimane B.
- **Proprietà (Iniettività):**
  - Se $f : A \to B$ è **iniettiva**, allora **qualsiasi** sua restrizione $f|_C : C \to B$ è anch'essa **iniettiva**. (Se f non manda input diversi sullo stesso output in tutto A, a maggior ragione non lo farà nel sottoinsieme C).
  - **Il viceversa NON vale:** Se una restrizione $f|_C$ è iniettiva, **non** è detto che la funzione originale f sia iniettiva su tutto A.
    - Esempio: $f(x) = x^2$ da $\mathbb{R}$ a $\mathbb{R}$ non è iniettiva. Ma la sua restrizione $f|_{(0,+\infty)}$ (ai reali positivi) è iniettiva.

5.3 Prolungamento di una Funzione (Pag 23)

- Siano $f : A \to B$ e $g : C \to B$ due funzioni.
- Diciamo che f è un **prolungamento** di g se:
  1. Il dominio di g è un sottoinsieme del dominio di f ($C \subseteq A$).
  2. f coincide con g su tutto il dominio di g (cioè $f(x) = g(x)$ per ogni $x \in C$).
  - In pratica, f "estende" la funzione g a un dominio più grande, comportandosi come g sul dominio originale C. Questo è equivalente a dire che g è la restrizione di f a C ($g = f|_C$).
- **Proprietà (Iniettività):**
  - Se $g : C \to B$ è iniettiva, **non** è detto che un suo prolungamento $f : A \to B$ (con $A \supset C$) sia anch'esso iniettivo. (Potremmo estendere la funzione in modo da creare "collisioni" al di fuori di C).

5.4 Esistenza di Restrizioni Iniettive (Pag 24)

- Data una qualsiasi funzione $f : A \to B$ (con $A \neq \emptyset$), esiste **sempre** almeno una restrizione di f che è iniettiva.
- **Dimostrazione banale:** Basta prendere un qualsiasi elemento $a \in A$ e considerare il sottoinsieme $C = \{a\}$. La restrizione $f|_C : \{a\} \to B$ è definita da $f|_C(a) = f(a)$. Una funzione definita su un dominio con un solo elemento è sempre iniettiva (non ci sono due input distinti da confrontare!).

5.5 Funzione Identità (Pag 25)

- Per ogni insieme non vuoto A, la **funzione identità** su A è:

$$id_A : A \to A$$

$$id_A(a) = a$$

  - Manda ogni elemento in se stesso.
- Il suo grafo è $G = \{(a, a) \mid a \in A\}$.
- La funzione identità è sempre **iniettiva** e **suriettiva** (quindi **biettiva**).

Restrizione di una funzione Prolungamento di una funzione Funzione identità

Riepilogo Veloce Lezione 3

- Abbiamo praticato la **negazione** di formule logiche complesse (implicazioni, quantificatori).
- Abbiamo chiarito un **errore comune sull'iniettività**.
- Abbiamo esplorato le **proprietà dell'immagine e della controimmagine**, collegandole alla suriettività.
- Abbiamo definito formalmente la **funzione suriettiva** e visto le sue caratterizzazioni equivalenti.
- Abbiamo analizzato diversi esempi per determinare **iniettività e suriettività**.
- Abbiamo introdotto la **funzione caratteristica** χ_A.
- Abbiamo definito l'**uguaglianza tra funzioni**.
- Abbiamo definito la **restrizione** $f|_C$ e il **prolungamento** di funzioni, vedendo come si rapportano all'iniettività.

- Abbiamo definito la **funzione identità** id_A.

Prossimi Passi

- Assicurati di saper distinguere bene tra iniettività e suriettività e di conoscere le loro definizioni e caratterizzazioni.
- Prova a creare tu degli esempi di funzioni e a determinarne iniettività e suriettività.
- Rifletti: una funzione può essere sia iniettiva che suriettiva? (Sì, si chiama biettiva!). Può non essere nessuna delle due? (Sì!).

Lezione 4: Biettività, Cardinalità, Composizione, Operazioni

Data: 21/03/2025 (come da note)
Argomenti: Insieme delle Parti (chiarimenti), Partizioni (recap, esempi), Funzioni Biettive, Equipotenza e Cardinalità, Composizione di Funzioni, Funzioni Invertibili, Operazioni (n-arie, binarie, unarie), Strutture Algebriche, Associatività, Esercizi.

#tag/settheory #tag/partitions #tag/functions #tag/bijectivity #tag/cardinality #tag/composition #tag/inverse-function #tag/operations #tag/algebraic-structures #tag/associativity #tag/algebra-avanzata

---

1. Chiarimenti su Insieme delle Parti e Partizioni

1.1 Elementi vs Sottoinsiemi in P(S) (Pag 1)

È cruciale distinguere tra appartenenza ($\in$) e inclusione ($\subseteq$) quando si lavora con l'insieme delle parti $P(S)$.

- Sia $S = \{a, \{a\}, b, \{b\}, c, \{c\}\}$.
- $P(S) = \{X \mid X \subseteq S\}$ è l'insieme di **tutti i sottoinsiemi** di S.
- **Esempi:**
  - $a \in S$ (a è un elemento di S)
  - $a \notin P(S)$ (a *non* è un sottoinsieme di S, è un elemento!)
  - $a \not\subseteq P(S)$ (un elemento non può essere sottoinsieme di un insieme di insiemi in questo modo)
  - $\{a\} \in P(S)$ (l'insieme contenente solo 'a' è un sottoinsieme di S, quindi è un elemento di P(S))
  - $\{a\} \subseteq S$ (questo è vero solo se a è anche un elemento di S, cosa che è vera nel nostro esempio)
  - $\{a\} \not\subseteq P(S)$ (l'insieme {a} non è un sottoinsieme di P(S), perché gli elementi di {a} non sono elementi di P(S))
  - $\{\{a\}\} \in P(S)$ (l'insieme contenente l'elemento {a} è un sottoinsieme di S, quindi è un elemento di P(S))
  - $\{\{a\}\} \subseteq P(S)$ (questo è vero perché l'unico elemento di $\{\{a\}\}$, cioè $\{a\}$, è anche un elemento di $P(S)$).

Fai molta attenzione alla differenza tra x e $\{x\}$ e tra $\in$ e $\subseteq$, specialmente con $P(S)$!

Insieme delle Parti

1.2 Partizioni (Recap ed Esempi) (Pag 2-4)

Ricordiamo la definizione: Una **partizione** di $S \neq \emptyset$ è una famiglia $\mathcal{F} \subseteq P(S)$ tale che:

1. $\forall X \in \mathcal{F}, X \neq \emptyset$ (Nessun pezzo vuoto)
2. $\forall X, Y \in \mathcal{F}, X \neq Y \implies X \cap Y = \emptyset$ (Pezzi disgiunti)
3. $\bigcup_{X \in \mathcal{F}} X = S$ (I pezzi ricoprono tutto)

- **Partizioni Banali:** $\mathcal{F}_1 = \{S\}$ e $\mathcal{F}_2 = \{\{a\} \mid a \in S\}$ (se S è finito).
- **Esempi con $S = \{a, b, c, d\}$ (Pag 3):**
  - $\mathcal{F}_1 = \{\{a\}, \{b, c\}, \{a, d\}\}$: **NON è partizione**. $\{a\} \cap \{a, d\} = \{a\} \neq \emptyset$. (Viola la condizione 2).
  - $\mathcal{F}_2 = \{\{a, b\}, \{d\}\}$: **NON è partizione**. $\{a, b\} \cup \{d\} = \{a, b, d\} \neq S$. (Manca c, viola la condizione 3).
  - $\mathcal{F}_3 = \{\{a, b\}, \{c\}, \{d\}\}$: **SÌ, è partizione**. (Pezzi non vuoti, disgiunti, unione fa S).
  - $\mathcal{F}_4 = \{\{a, b, d\}, \{c\}\}$: **SÌ, è partizione**.
- **Esempio con $S = \mathbb{Z}$ (Pag 4):**
  - Consideriamo $A = \{a \in \mathbb{Z} \mid a^2 > 1\}$ e $B = \{a \in \mathbb{Z} \mid a^2 < 1\}$.
  - $A = \{\dots, -3, -2\} \cup \{2, 3, \dots\}$. $A \neq \emptyset$.
  - $B = \{0\}$. $B \neq \emptyset$.
  - $A \cap B = \emptyset$.
  - $A \cup B = \mathbb{Z} \setminus \{1, -1\}$. **NON ricopre tutto $\mathbb{Z}$**.
  - Quindi $\mathcal{F} = \{A, B\}$ **NON è una partizione** di $\mathbb{Z}$.
  - Consideriamo invece $D = \{a \in \mathbb{Z} \mid a^2 \geq 1\}$ e $C = \{a \in \mathbb{Z} \mid a^2 \leq 1\}$.
  - $D = \mathbb{Z} \setminus \{0\}$. $D \neq \emptyset$.

- $C = \{-1, 0, 1\}$. $C \neq \emptyset$.
- $D \cap C = \{-1, 1\} \neq \emptyset$.
- Quindi $\mathcal{G} = \{D, C\}$ **NON è una partizione** di $\mathbb{Z}$.
- Consideriamo $A = \{a \in \mathbb{Z} \mid a^2 > 1\}$, $C = \{a \in \mathbb{Z} \mid a^2 \leq 1\} = \{-1, 0, 1\}$.
- $A \cap C = \emptyset$? No, $A \cap C = \{-1, 1\}$ non è vuoto.
- Consideriamo $A = \{a \in \mathbb{Z} \mid a^2 > 1\}$, $E = \{1\}$, $F = \{-1\}$, $G = \{0\}$.
- $\mathcal{H} = \{A, E, F, G\}$ **NON è una partizione** perché $A \cap E = \emptyset$, $A \cap F = \emptyset$, $A \cap G = \emptyset$, $E \cap F = \emptyset$, ecc. MA $A \cup E \cup F \cup G = \mathbb{Z}$. Tutti gli elementi sono non vuoti. Tutti disgiunti? No, A contiene $2, -2$, ecc. $E = \{1\}$, $F = \{-1\}$, $G = \{0\}$. Sembra che $A = \mathbb{Z} \setminus \{-1, 0, 1\}$. In questo caso, A, E, F, G sono disgiunti, non vuoti e la loro unione è $\mathbb{Z}$. **SÌ, $\mathcal{H}$ è una partizione.**
- La nota originale $\{A, C\}$ con $A = \{a | a^2 > 1\}$ e $C = \{a | a^2 \leq 1\}$ **è una partizione** se interpretiamo $A = \mathbb{Z} \setminus \{-1, 0, 1\}$ e $C = \{-1, 0, 1\}$. I pezzi sono non vuoti, disgiunti e la loro unione è $\mathbb{Z}$.

> ⚠ **L'insieme vuoto $\emptyset$ e l'insieme totale S non sono MAI partizioni di S (se $|S| > 1$). $\emptyset$ non è una famiglia di sottoinsiemi non vuoti. $\{S\}$ è una partizione (banale), ma S da solo non è una famiglia di sottoinsiemi.**

Partizione di un insieme

---

2. Funzioni Biettive ed Equipotenza

2.1 Funzione Biettiva

- Una funzione $f : A \to B$ si dice **biettiva** (o biunivoca, o una corrispondenza biunivoca) se è **sia iniettiva sia suriettiva**.
- **Caratterizzazione tramite Controimmagine (Pag 9):** f è biettiva $\iff$ per ogni $b \in B$, la controimmagine $\overleftarrow{f}(\{b\})$ è un **singleton** (contiene esattamente un elemento).
  - Iniettività $\implies |\overleftarrow{f}(\{b\})| \leq 1$.
  - Suriettività $\implies |\overleftarrow{f}(\{b\})| \geq 1$.
  - Mettendole insieme: $|\overleftarrow{f}(\{b\})| = 1$.
- **Esempio (Pag 8):** $f : \mathbb{N} \to \mathbb{Z}$ con $f(n) = n/2$ (se n pari) e $f(n) = -(n+1)/2$ (se n dispari). (Assumiamo $\mathbb{N} = \{0, 1, 2, \dots\}$).
  - Abbiamo già visto che è **iniettiva** (Lezione 3).
  - È **suriettiva?** Dobbiamo dimostrare che per ogni $b \in \mathbb{Z}$, esiste $n \in \mathbb{N}$ tale che $f(n) = b$.
    - Se $b \geq 0$: Cerchiamo n pari tale che $n/2 = b$. Basta prendere $n = 2b$. Poiché $b \geq 0$, $n = 2b \geq 0$ ed è pari. $n \in \mathbb{N}$. Trovato!
    - Se $b < 0$: Cerchiamo n dispari tale che $-(n+1)/2 = b$. Moltiplichiamo per -1: $(n+1)/2 = -b$. Poiché $b < 0$, $-b > 0$. Moltiplichiamo per 2: $n + 1 = -2b$. Quindi $n = -2b - 1$. Poiché $-b > 0$, $-2b > 0$, quindi $n = -2b - 1 \geq -1$? No, $n \geq 1$. Essendo $-2b$ pari, $n = -2b - 1$ è dispari. $n \in \mathbb{N}$. Trovato!
  - Poiché per ogni $b \in \mathbb{Z}$ abbiamo trovato un $n \in \mathbb{N}$ tale che $f(n) = b$, la funzione è **suriettiva**.
  - Essendo sia iniettiva che suriettiva, f è **biettiva**.

Funzione Biettiva

2.2 Equipotenza e Cardinalità (Pag 9-10)

- Due insiemi A e B si dicono **equipotenti** (o che hanno la stessa cardinalità) se esiste una funzione **biettiva** $f : A \to B$.
- Notazione: $|A| = |B|$ o $A \approx B$.
- L'equipotenza definisce una relazione di equivalenza sull'insieme di tutti gli insiemi.
- **Cardinalità:** Concetto che generalizza il "numero di elementi".
  - $|\emptyset| = 0$.
  - Se $A = \{1, 2, \dots, n\}$, allora $|A| = n$.
  - Se $A \subseteq B \implies |A| \leq |B|$. (Teorema di Cantor-Schröder-Bernstein per il caso generale, ovvio per insiemi finiti).
- **Proprietà Fondamentale (Insiemi Finiti vs Infiniti):**
  - Se A e B sono **finiti**: $A \subseteq B$ e $|A| = |B| \implies A = B$. (Se un sottoinsieme ha lo stesso numero di elementi dell'insieme, deve coincidere con esso).
  - Questa proprietà **NON VALE** per insiemi **infiniti**!
    - Esempio: $\mathbb{N} = \{0, 1, 2, \dots\}$, $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$. Chiaramente $\mathbb{N} \subset \mathbb{Z}$ (sottoinsieme proprio). Ma abbiamo trovato una funzione biettiva $f : \mathbb{N} \to \mathbb{Z}$, quindi $|\mathbb{N}| = |\mathbb{Z}|$.
    - Questo è un tratto distintivo degli insiemi infiniti: possono essere messi in corrispondenza biunivoca con un loro sottoinsieme proprio.

3. Composizione di Funzioni

Come combinare due funzioni in sequenza.

- **Definizione (Pag 13):** Siano $f: A \to B$ e $g: C \to D$ due funzioni. Se l'immagine di f è contenuta nel dominio di g (cioè $\vec{f}(A) \subseteq C$), allora possiamo definire la **funzione composta** $g \circ f$ (si legge "g composto f"):

$$(g \circ f) : A \to D$$

$$(g \circ f)(x) = g(f(x)) \quad \text{per ogni } x \in A$$

  - **Spiegazione:** Per calcolare $(g \circ f)(x)$:
    1. Applica f a x, ottenendo $f(x) \in B$.
    2. Poiché $f(x)$ appartiene anche a C (per l'ipotesi $\vec{f}(A) \subseteq C$), puoi applicare g a $f(x)$.
    3. Il risultato è $g(f(x)) \in D$.

⚠ **L'ordine è importante! $g \circ f$ significa: prima applichi f, poi applichi g. Il dominio della composizione è il dominio della *prima* funzione applicata (f). Il codominio della composizione è il codominio della *seconda* funzione applicata (g). La condizione $\vec{f}(A) \subseteq C$ è essenziale perché l'output di f deve essere un input valido per g.**

- **Esempio 1 (Pag 14):**
  - $S = \{x \subseteq Z \mid x \neq \emptyset \text{ e finito}\}$? Sembra una definizione strana. Forse $S = P_{fin}(\mathbb{Z}) \setminus \{\emptyset\}$ (sottoinsiemi finiti non vuoti di $\mathbb{Z}$).
  - $f: P(S) \to \mathbb{Z}$ con $f(X) = |X|$? Se S è l'insieme dei sottoinsiemi finiti, $P(S)$ è l'insieme delle famiglie di sottoinsiemi finiti... Forse S era un insieme finito? Rivediamo l'esempio.
  - Assumiamo S un insieme finito. $f: P(S) \to \mathbb{Z}$ con $f(X) = |X|$.
  - $g: \mathbb{Q} \to \mathbb{Q}$ con $g(n) = \frac{3}{2}n$.
  - Il codominio di f è $\mathbb{Z}$. Il dominio di g è $\mathbb{Q}$. Poiché $\mathbb{Z} \subseteq \mathbb{Q}$, la composizione $g \circ f$ è definita.
  - $(g \circ f) : P(S) \to \mathbb{Q}$
  - $(g \circ f)(X) = g(f(X)) = g(|X|) = \frac{3}{2}|X|$.
  - Esempio: Se $S = \{-1, 0, 1, 13\}$, $X = \{-1, 0, 1, 13\}$. $|X| = 4$. $(g \circ f)(X) = \frac{3}{2} \cdot 4 = 6$.
  - Esempio: Se $X = \{-1, 5, 7\}$. $|X| = 3$. $(g \circ f)(X) = \frac{3}{2} \cdot 3 = \frac{9}{2}$.
- **Esempio 2 (Pag 15):**
  - $S = \{a, b, c\}$.
  - $f: P(S) \times P(S) \to P(S)$ con $f(X, Y) = X \cap Y$.
  - $g: P(S) \to P(S) \times P(S)$ con $g(A) = (A, S \setminus A)$.
  - Composizione $g \circ f$: Il codominio di f è $P(S)$, il dominio di g è $P(S)$. Sono uguali, quindi $g \circ f$ è definita.
    - $(g \circ f) : P(S) \times P(S) \to P(S) \times P(S)$
    - $(g \circ f)(X, Y) = g(f(X, Y)) = g(X \cap Y) = (X \cap Y, S \setminus (X \cap Y))$.
    - Esempio: $(g \circ f)(\{a, b\}, \{b, c\}) = g(\{b\}) = (\{b\}, S \setminus \{b\}) = (\{b\}, \{a, c\})$.
  - Composizione $f \circ g$: Il codominio di g è $P(S) \times P(S)$, il dominio di f è $P(S) \times P(S)$. Sono uguali, quindi $f \circ g$ è definita.
    - $(f \circ g) : P(S) \to P(S)$
    - $(f \circ g)(A) = f(g(A)) = f((A, S \setminus A)) = A \cap (S \setminus A) = \emptyset$.
    - Quindi $f \circ g$ è la funzione costante che manda ogni sottoinsieme A nell'insieme vuoto.
- **Esempio 3 (Pag 16):**
  - $f: \mathbb{Z} \to \mathbb{Z}$ con $f(x) = 3x - 1$.
  - $g: \mathbb{Z} \to \mathbb{Z}$ con $g(y) = (y + 1)^2$.
  - Composizione $g \circ f$: Codominio f = Dominio $g = \mathbb{Z}$. Definita.
    - $(g \circ f) : \mathbb{Z} \to \mathbb{Z}$
    - $(g \circ f)(x) = g(f(x)) = g(3x - 1) = ((3x - 1) + 1)^2 = (3x)^2 = 9x^2$.
  - Composizione $f \circ g$: Codominio g = Dominio $f = \mathbb{Z}$. Definita.
    - $(f \circ g) : \mathbb{Z} \to \mathbb{Z}$
    - $(f \circ g)(x) = f(g(x)) = f((x + 1)^2) = 3(x + 1)^2 - 1$.
  - **Non Commutatività (Pag 17):** Come si vede dagli esempi, in generale $g \circ f \neq f \circ g$. La composizione di funzioni **non è commutativa**.
- **Composizione con Identità (Pag 18):**
  - Sia $f: A \to B$. Siano $id_A: A \to A$ e $id_B: B \to B$ le funzioni identità.
  - $f \circ id_A = f$.
    - $(f \circ id_A)(x) = f(id_A(x)) = f(x)$. Dominio A, codominio B.

- $id_B \circ f = f$.
  - $(id_B \circ f)(x) = id_B(f(x)) = f(x)$. Dominio A, codominio B.

Composizione di funzioni Non commutatività della composizione

---

4. Funzioni Invertibili

Quando una funzione può essere "annullata" da un'altra.

- **Definizione (Pag 19):** Una funzione $f : A \to B$ si dice **invertibile** se esiste una funzione $f^{-1} : B \to A$ (chiamata **funzione inversa** di f) tale che:
  1. $f^{-1} \circ f = id_A$ (Comporre f e poi f^{-1} riporta all'identità sul dominio originale A).
  2. $f \circ f^{-1} = id_B$ (Comporre f^{-1} e poi f riporta all'identità sul codominio originale B).

Teorema Fondamentale: Invertibilità e Biettività (Pag 19)

Una funzione $f : A \to B$ è **completamente invertibile se e solo se è biettiva**.

- **Costruzione dell'Inversa:** Se f è biettiva, la sua inversa $f^{-1} : B \to A$ è definita associando a ogni $b \in B$ l'**unico** elemento $a \in A$ tale che $f(a) = b$. L'esistenza e unicità di tale a è garantita dalla biettività di f (poiché $|\overleftarrow{f}(\{b\})| = 1$ per ogni $b \in B$).

- **Esempio 1 (Pag 20):** $f : \mathbb{Z} \to \mathbb{Z}$ con $f(x) = x + 5$.
  - È iniettiva? $f(x) = f(y) \implies x + 5 = y + 5 \implies x = y$. Sì.
  - È suriettiva? Per ogni $b \in \mathbb{Z}$, cerchiamo x tale che $f(x) = b$, cioè $x + 5 = b$. Basta prendere $x = b - 5$. Poiché $b \in \mathbb{Z}$, anche $x = b - 5 \in \mathbb{Z}$. Sì.
  - Essendo biettiva, è invertibile. L'inversa è $f^{-1} : \mathbb{Z} \to \mathbb{Z}$ con $f^{-1}(b) = b - 5$.
  - Verifica:
    - $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(x + 5) = (x + 5) - 5 = x = id_{\mathbb{Z}}(x)$.
    - $(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(b - 5) = (b - 5) + 5 = b = id_{\mathbb{Z}}(b)$.
- **Esempio 2 (Pag 21):** Controesempio per inversa "parziale".
  - $f : \mathbb{Z} \to \mathbb{N}$ con $f(a) = |a|$. (Assumiamo $\mathbb{N} = \{0, 1, 2, \dots\}$).
  - $g : \mathbb{N} \to \mathbb{Z}$ con $g(x) = -x$.
  - Calcoliamo $f \circ g$: $\mathbb{N} \to \mathbb{N}$.
    - $(f \circ g)(x) = f(g(x)) = f(-x) = |-x| = |x|$. Poiché $x \in \mathbb{N}$ (dominio di g), $|x| = x$.
    - Quindi $(f \circ g)(x) = x = id_{\mathbb{N}}(x)$. Sembra che g sia un'inversa destra di f.
  - Calcoliamo $g \circ f$: $\mathbb{Z} \to \mathbb{Z}$.
    - $(g \circ f)(a) = g(f(a)) = g(|a|) = -|a|$.
    - Questo **NON** è $id_{\mathbb{Z}}(a) = a$. Ad esempio, $(g \circ f)(1) = -|1| = -1 \neq 1$.
  - Conclusione: f non è invertibile (infatti non è iniettiva, $f(1) = f(-1) = 1$). g non è l'inversa di f.

Funzione Inversa Teorema di Invertibilità

---

5. Operazioni e Strutture Algebriche

Introduciamo i concetti base dell'algebra.

5.1 Operazioni n-arie, Binarie, Unarie (Pag 22-24)

- Un'**operazione interna n-aria** su un insieme non vuoto A è una funzione $f : A^n \to A$, dove $A^n = A \times A \times \cdots \times A$ (n volte).
- **Operazione Binaria Interna (n=2):** Una funzione $f : A \times A \to A$. Prende due elementi di A e restituisce un elemento di A. Notazione spesso infissa: $a \circ b$ invece di $f(a, b)$.
  - Esempi:
    - $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(a, b) \mapsto a + b$.
    - $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(a, b) \mapsto a - b$.
    - $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, $(a, b) \mapsto a \cdot b$.
    - $/ : \mathbb{Q}^* \times \mathbb{Q}^* \to \mathbb{Q}^*$, $(a, b) \mapsto a/b$. (Qui $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$).
    - $\cap : P(S) \times P(S) \to P(S)$, $(A, B) \mapsto A \cap B$.
    - $\cup : P(S) \times P(S) \to P(S)$, $(A, B) \mapsto A \cup B$.
    - $\Delta : P(S) \times P(S) \to P(S)$, $(A, B) \mapsto A \Delta B$.
    - $\setminus : P(S) \times P(S) \to P(S)$, $(A, B) \mapsto A \setminus B$.
- **Operazione Unaria Interna (n=1):** Una funzione $f : A \to A$. Prende un elemento di A e restituisce un elemento di A.

- Esempi:
  - Opposto: $-:\mathbb{Z}\to\mathbb{Z},\ a\mapsto -a$.
  - Reciproco: $^{-1}:\mathbb{Q}^*\to\mathbb{Q}^*,\ a\mapsto 1/a=a^{-1}$.
  - Complemento: $^{c}:P(S)\to P(S),\ X\mapsto S\setminus X$.
- **Operazione Esterna (Pag 25):** Una funzione $f:S\times T\to T$ (o $S\times T\to S$). Coinvolge due insiemi diversi.
  - Esempio: Prodotto per scalare in $\mathbb{R}^2$. $\cdot:\mathbb{R}\times\mathbb{R}^2\to\mathbb{R}^2,\ (a,(v_1,v_2))\mapsto(av_1,av_2)$.

Operazione Binaria Operazione Unaria

5.2 Strutture Algebriche (Pag 25)

- Una **struttura algebrica** è una coppia $(S,\mathcal{O})$ dove S è un insieme non vuoto (chiamato **sostegno** o supporto) e $\mathcal{O}$ è un insieme di una o più operazioni (interne o esterne) definite su S.
- Notazione: $(S,\circ_1,\circ_2,\dots)$
- Esempi: $(\mathbb{N},+)$, $(\mathbb{Z},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(P(S),\cap,\cup,^c)$, $(\mathbb{R}^2,+,\cdot_{\text{scalare}})$.

Struttura Algebrica

5.3 Proprietà Associativa (Pag 27)

- Un'operazione binaria interna $\circ:S\times S\to S$ si dice **associativa** se:

$$\forall a,b,c\in S,\quad (a\circ b)\circ c=a\circ(b\circ c)$$

  - **Spiegazione:** Non importa come metti le parentesi quando componi tre elementi con un'operazione associativa.
- **Operazioni Associative:** $+$, $\cdot$ (sui numeri), $\cap$, $\cup$, Δ (sugli insiemi), composizione di funzioni $(h\circ(g\circ f)=(h\circ g)\circ f)$.
- **Operazioni NON Associative:** $-$, $/$ (divisione).
  - Controesempio per $-$: $(3-2)-1=1-1=0$. Ma $3-(2-1)=3-1=2$. Poiché $0\neq 2$, la sottrazione non è associativa.

Proprietà Associativa

---

6. Esercizi Proposti (Pag 28-29)

Studiare iniettività, suriettività e determinare eventuale biettività e calcolare immagini/controimmagini per le seguenti funzioni:

1. Definizione della funzione:

$$f:a\in\mathbb{Z}\longrightarrow(a+3,a-3)\in\mathbb{Z}\times\mathbb{Z}$$

   Calcolare:
   - $\vec{f}(\emptyset)$
   - $\overleftarrow{f}(\emptyset)$
   - $\vec{f}(\mathbb{Z})$
   - $\overleftarrow{f}(\mathbb{Z}\times\mathbb{Z})$
   - $\vec{f}(\{3,5,7\})$
   - $\overleftarrow{f}(\{(4,-2)\})$
   - $\overleftarrow{f}(\{(4,0)\})$
2. Definizione della funzione:

$$f:(a,b)\in\mathbb{Z}\times\mathbb{Z}\longrightarrow(a+b,a-b)\in\mathbb{Z}\times\mathbb{Z}$$

   Calcolare:
   - $\vec{f}(\{(3,1),(-5,7)\})$
   - $\overleftarrow{f}(\{(1,1),(3,1)\})$
3. Ripetere esercizio 2 con dominio e codominio $\mathbb{Q}\times\mathbb{Q}$.
   (Studiare $f:(a,b)\in\mathbb{Q}\times\mathbb{Q}\longrightarrow(a+b,a-b)\in\mathbb{Q}\times\mathbb{Q}$ per iniettività, suriettività, biettività)
4. Sia $S=\{a,b,c\}$. Si consideri la funzione:

$$f:(A,B)\in\mathcal{P}(S)\times\mathcal{P}(S)\longrightarrow(A,A\cap B)\in\mathcal{P}(S)\times\mathcal{P}(S)$$

   Determinare (det):
   - $\vec{f}(\{(\{a\},\{b\}),(\{a\},\{c\}),(\{a,b\},S)\})$
   - $\overleftarrow{f}(\{(\{a\},\{b\})\})$
   - $\overleftarrow{f}(\{(\{a\},\{a\})\})$

- $\vec{f}(\emptyset)$
- $\vec{f}(\mathcal{P}(S) \times \mathcal{P}(S))$
- $\overleftarrow{f}(\emptyset)$
- $\overleftarrow{f}(\mathcal{P}(S) \times \mathcal{P}(S))$

Riepilogo Veloce Lezione 4

- Abbiamo chiarito la distinzione tra $\in$ e $\subseteq$ in relazione a $P(S)$.
- Abbiamo rivisto la definizione di **partizione** con esempi.
- Abbiamo definito la **funzione biettiva** (iniettiva + suriettiva) e la sua caratterizzazione tramite controimmagine di singleton.
- Abbiamo introdotto l'**equipotenza** ($|A| = |B|$) tramite funzioni biettive e discusso la differenza tra insiemi finiti e infiniti riguardo ai sottoinsiemi propri.
- Abbiamo definito la **composizione di funzioni** ($g \circ f$) e visto che non è commutativa.
- Abbiamo definito la **funzione invertibile** e il teorema che la lega alla biettività.
- Abbiamo introdotto le **operazioni n-arie, binarie, unarie** (interne ed esterne).
- Abbiamo definito le **strutture algebriche**.
- Abbiamo definito la **proprietà associativa**.

Prossimi Passi

- Prova a svolgere gli esercizi proposti. Sono ottimi per consolidare i concetti di iniettività, suriettività, immagine e controimmagine.
- Rifletti sulle diverse strutture algebriche menzionate. Quali proprietà (oltre all'associatività) potrebbero avere le loro operazioni (es. commutatività, elemento neutro, inverso)? Questo ci porterà ai gruppi!

Lezione 5: Composizione, Invertibilità, Semigruppi e Monoidi

Data: 25/03/2025 (come da note)
Argomenti: Composizione (proprietà), Funzioni invertibili (teorema, unicità), Inversa destra/sinistra, Matrici (introduzione), Semigruppi, Elemento neutro, Monoidi, Esercizi.

#tag/functions #tag/composition #tag/inverse-function #tag/bijectivity #tag/matrices #tag/algebraic-structures #tag/semigroups #tag/monoids #tag/identity-element #tag/associativity #tag/algebra-avanzata

---

1. Composizione di Funzioni: Proprietà Fondamentali

Riprendiamo la composizione $g \circ f$ di $f : A \to B$ e $g : C \to D$, definita quando $\vec{f}(A) \subseteq C$.

- **Definizione:** $(g \circ f) : A \to D$ con $(g \circ f)(x) = g(f(x))$.
  - Nota: Spesso si richiede semplicemente che il codominio di f sia uguale o contenuto nel dominio di g, cioè $B \subseteq C$.
- **Non Commutatività (Recap, Pag 1-2):** In generale, $g \circ f \neq f \circ g$ (anche quando entrambe le composizioni sono definite, ad esempio se $f, g : \mathbb{Z} \to \mathbb{Z}$).
  - Esempio: $f(x) = x + 1$, $g(y) = y^2$.
    - $(g \circ f)(x) = g(f(x)) = g(x+1) = (x+1)^2 = x^2 + 2x + 1$.
    - $(f \circ g)(x) = f(g(x)) = f(x^2) = x^2 + 1$.
    - Chiaramente $(x+1)^2 \neq x^2 + 1$ (tranne per $x = 0$).
- **Associatività (Pag 2):** La composizione di funzioni **è associativa**.
  - Siano $f : A \to B$, $g : B \to C$, $h : C \to D$. (Nota: ho adattato i domini/codomini per rendere le composizioni sempre possibili).
  - Allora $(h \circ g) \circ f = h \circ (g \circ f)$.
  - **Dimostrazione:** Dobbiamo verificare che le due funzioni $(h \circ g) \circ f$ e $h \circ (g \circ f)$ abbiano stesso dominio, stesso codominio e stessa legge.
    - Dominio: Entrambe vanno da A a D. OK.
    - Codominio: Entrambe vanno da A a D. OK.
    - Legge: Sia $x \in A$.
      - $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$.
      - $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$.
      - Le leggi coincidono. OK.
  - Quindi la composizione è associativa.

- Associatività della Composizione
- **Composizione con Identità (Recap, Pag 3):**
  - $f \circ id_A = f$
  - $id_B \circ f = f$
  - Se $f : A \to A$, allora $id_A \circ f = f \circ id_A = f$.

---

2. Funzioni Invertibili e Biettività

2.1 Definizione di Funzione Invertibile (Pag 4)

- Una funzione $f : A \to B$ è **invertibile** se esiste una funzione $f^{-1} : B \to A$ (detta **funzione inversa** di f) tale che:
  1. $f^{-1} \circ f = id_A$
  2. $f \circ f^{-1} = id_B$

2.2 Teorema di Invertibilità (Pag 4)

- **Proposizione:** Una funzione $f : A \to B$ è **invertibile se e solo se è biettiva**.
  - ($\implies$) Se f è invertibile, allora è biettiva (si può dimostrare).
  - ($\impliedby$) Se f è biettiva, allora per ogni $y \in B$ esiste un unico $x_y \in A$ tale che $f(x_y) = y$ (perché $|\overleftarrow{f}(\{y\})| = 1$). Possiamo definire $f^{-1} : B \to A$ come $f^{-1}(y) = x_y$. Si verifica poi che questa f^{-1} soddisfa le condizioni $f^{-1} \circ f = id_A$ e $f \circ f^{-1} = id_B$.

Funzione Inversa Teorema di Invertibilità

2.3 Esempi di Verifica Biettività e Calcolo Inversa

- **Esempio 1 (Pag 5):** $f : \mathbb{Z} \to \mathbb{Z}$ con $f(x) = -x + 5$.
  - Iniettiva? $f(x) = f(y) \implies -x + 5 = -y + 5 \implies -x = -y \implies x = y$. **SÌ**.
  - Suriettiva? Per ogni $a \in \mathbb{Z}$, cerchiamo $x \in \mathbb{Z}$ tale che $f(x) = a$.
    - $-x + 5 = a \implies -x = a - 5 \implies x = -(a - 5) = -a + 5$.
    - Poiché $a \in \mathbb{Z}$, anche $x = -a + 5 \in \mathbb{Z}$. Trovato. **SÌ**.
  - Biettiva? Sì.
  - Inversa: La legge trovata per x in funzione di a ci dà l'inversa. $f^{-1} : \mathbb{Z} \to \mathbb{Z}$ con $f^{-1}(a) = -a + 5$. (Nota: in questo caso $f^{-1} = f$!).
- **Esempio 2 (Pag 6):** $g : \mathbb{Z} \to \mathbb{Z}$ con $g(x) = x - 5$.
  - Iniettiva? $g(x) = g(y) \implies x - 5 = y - 5 \implies x = y$. **SÌ**.
  - Suriettiva? Per ogni $a \in \mathbb{Z}$, cerchiamo $x \in \mathbb{Z}$ tale che $g(x) = a$.
    - $x - 5 = a \implies x = a + 5$.
    - Poiché $a \in \mathbb{Z}$, anche $x = a + 5 \in \mathbb{Z}$. Trovato. **SÌ**.
  - Biettiva? Sì.
  - Inversa: $g^{-1} : \mathbb{Z} \to \mathbb{Z}$ con $g^{-1}(a) = a + 5$.
- **Esempio 3 (Pag 7-8):** $f : \mathbb{N} \to \mathbb{Z}$ con $f(n) = n/2$ (se n pari) e $f(n) = -(n+1)/2$ (se n dispari). (Assumiamo $\mathbb{N} = \{0, 1, 2, \dots\}$).
  - Abbiamo già visto che è **biettiva** (Lezione 4).
  - Calcoliamo l'inversa $f^{-1} : \mathbb{Z} \to \mathbb{N}$. Dobbiamo trovare la formula per n dato $a = f(n)$.
    - Se $a \geq 0$: Sappiamo che l'input n deve essere pari e $n/2 = a$, quindi $n = 2a$.
    - Se $a < 0$: Sappiamo che l'input n deve essere dispari e $-(n+1)/2 = a$, quindi $n + 1 = -2a$, e $n = -2a - 1$.
  - Quindi, l'inversa è:

$$f^{-1}(a) = \begin{cases} 2a & \text{se } a \geq 0 \\ -2a - 1 & \text{se } a < 0 \end{cases}$$

    - Verifichiamo che l'output sia in $\mathbb{N}$: Se $a \geq 0$, $2a \geq 0$. Se $a < 0$, allora $-a > 0$, $-2a > 0$, e $-2a - 1 \geq -1$? No, $-2a \geq 2$ (poiché $a \leq -1$), quindi $-2a - 1 \geq 1$. In entrambi i casi l'output è in $\mathbb{N}$.
  - Verifica composizioni (Pag 8): $f \circ f^{-1} = id_{\mathbb{Z}}$ e $f^{-1} \circ f = id_{\mathbb{N}}$.

2.4 Unicità dell'Inversa (Pag 13)

- **Proposizione:** Se una funzione $f : A \to B$ è invertibile, la sua funzione inversa f^{-1} è **unica**.
- **Dimostrazione:** Supponiamo per assurdo che esistano due funzioni inverse, $g : B \to A$ e $h : B \to A$. Allora devono valere:
  - $g \circ f = id_A$ e $f \circ g = id_B$
  - $h \circ f = id_A$ e $f \circ h = id_B$
  - Consideriamo h. Possiamo scrivere $h = h \circ id_B$.

- Sostituiamo id_B con $f \circ g$: $h = h \circ (f \circ g)$.
- Usiamo l'associatività: $h = (h \circ f) \circ g$.
- Sappiamo che $h \circ f = id_A$: $h = id_A \circ g$.
- Sappiamo che $id_A \circ g = g$.
- Quindi, abbiamo ottenuto $h = g$. Le due inverse devono coincidere.

Unicità della Funzione Inversa

2.5 Inversa Destra e Sinistra (Cenno, Pag 10-12)

Esistono concetti più deboli di invertibilità:

- $g : B \to A$ è **inversa sinistra** di $f : A \to B$ se $g \circ f = id_A$. Si può dimostrare che f ammette inversa sinistra $\iff$ f è **iniettiva**. L'inversa sinistra, se esiste, non è necessariamente unica.
- $h : B \to A$ è **inversa destra** di $f : A \to B$ se $f \circ h = id_B$. Si può dimostrare che f ammette inversa destra $\iff$ f è **suriettiva**. L'inversa destra, se esiste, non è necessariamente unica.

> **Una funzione è invertibile (cioè ha un'inversa "bilatera") se e solo se è biettiva, e in tal caso l'inversa è unica. L'esistenza di solo una delle due (sinistra o destra) è legata solo all'iniettività o solo alla suriettività.**

- Esempio (Pag 11): $f : \mathbb{Z} \to \mathbb{Z}$ con $f(x) = 2x + 1$.
  - Iniettiva? $2x + 1 = 2y + 1 \implies 2x = 2y \implies x = y$. **SÌ**.
  - Suriettiva? Cerchiamo x tale che $2x + 1 = a$. $2x = a - 1$. $x = (a - 1)/2$. Questo è intero solo se $a - 1$ è pari, cioè se a è dispari. Se a è pari (es. $a = 2$), non esiste $x \in \mathbb{Z}$ tale che $f(x) = a$. **NO**.
  - Essendo iniettiva ma non suriettiva, ammette inversa sinistra ma non destra.
  - Candidata inversa sinistra $g : \mathbb{Z} \to \mathbb{Z}$ con $g(a) = (a - 1)/2$ se a dispari, e $g(a) = 0$ (o qualsiasi altra cosa) se a pari. Verifichiamo $g \circ f$:
    - $(g \circ f)(x) = g(f(x)) = g(2x + 1)$. Poiché $2x + 1$ è sempre dispari, usiamo la prima regola per g: $g(2x + 1) = ((2x + 1) - 1)/2 = (2x)/2 = x$.
    - Quindi $g \circ f = id_{\mathbb{Z}}$. g è un'inversa sinistra.

Inversa Sinistra e Destra

---

3. Strutture Algebriche: Semigruppi e Monoidi

3.1 Matrici (Cenno, Pag 14-16)

- Una **matrice** A di dimensione $m \times n$ a coefficienti in un insieme K (es. $\mathbb{R}$) è una tabella rettangolare di elementi di K con m righe e n colonne.
- Notazione: $A = (a_{ij})$ dove i è l'indice di riga $(1 \le i \le m)$ e j è l'indice di colonna $(1 \le j \le n)$. a_{ij} è l'elemento nella riga i e colonna j.
- L'insieme di tutte le matrici $m \times n$ a coefficienti in K si denota $M_{m,n}(K)$.
- **Matrice Trasposta** A^T: si ottiene scambiando le righe con le colonne. Se A è $m \times n$, A^T è $n \times m$, e $(A^T)_{ij} = a_{ji}$.
- **Matrice Quadrata:** Se $m = n$.
- **Operazioni:**
  - **Somma di Matrici** (solo tra matrici della stessa dimensione $m \times n$): $(A + B)_{ij} = a_{ij} + b_{ij}$. L'insieme $(M_{m,n}(\mathbb{R}), +)$ è una struttura algebrica.
  - **Prodotto per Scalare:** $\cdot : \mathbb{R} \times M_{m,n}(\mathbb{R}) \to M_{m,n}(\mathbb{R})$. $(c, A) \mapsto cA$, dove $(cA)_{ij} = c \cdot a_{ij}$. (Operazione esterna).
  - (Vedremo più avanti il prodotto tra matrici).

Matrice (matematica) Matrice Trasposta

3.2 Semigruppi (Pag 18)

- Una struttura algebrica $(S, *)$ dove $*$ è un'operazione binaria interna $(* : S \times S \to S)$ si dice **semigruppo** se l'operazione $*$ è **associativa**.

$$\forall a, b, c \in S, \quad (a * b) * c = a * (b * c)$$

- **Esempi di Semigruppi (Pag 19):**
  1. $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$
  2. $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$
  3. $(P(S), \cap)$, $(P(S), \cup)$, $(P(S), \Delta)$
  4. $(\mathbb{R}^n, +)$ (somma vettoriale componente per componente)

5. $(M_{m,n}(\mathbb{R}), +)$ (somma di matrici)
6. $(A^A, \circ)$, dove $A^A = \{f \mid f : A \to A\}$ è l'insieme di tutte le funzioni da A in A, e $\circ$ è la composizione di funzioni. (L'associatività della composizione garantisce che sia un semigruppo).

- **Esempio di NON Semigruppo (Pag 18):** $(\mathbb{Z}, *)$ con $a * b = 2a + b$.
  - $a * (b * c) = a * (2b + c) = 2a + (2b + c) = 2a + 2b + c$.
  - $(a * b) * c = (2a + b) * c = 2(2a + b) + c = 4a + 2b + c$.
  - Le due espressioni non sono uguali in generale (es. $a = b = c = 1$). Non è associativa.

Semigruppo

3.3 Elemento Neutro (Pag 20)

Sia $(S, *)$ un semigruppo (o anche solo una struttura con operazione binaria).

- Un elemento $u \in S$ si dice **elemento neutro** (o identità) se:

$$\forall a \in S, \quad a * u = u * a = a$$

- $u_L \in S$ è **neutro a sinistra** se $\forall a \in S, u_L * a = a$.
- $u_R \in S$ è **neutro a destra** se $\forall a \in S, a * u_R = a$.
- Un elemento è neutro (bilatero) se è neutro sia a sinistra sia a destra.
- **Esempi (Pag 21):**
  - $(\mathbb{Z}, -)$: 0 è neutro a destra ($a - 0 = a$), ma non a sinistra ($0 - a = -a \neq a$ se $a \neq 0$).
  - $(P(S), \setminus)$: $\emptyset$ è neutro a destra ($A \setminus \emptyset = A$), ma non a sinistra ($\emptyset \setminus A = \emptyset \neq A$ se $A \neq \emptyset$).
- **Proposizione (Unicità dell'Elemento Neutro, Pag 21):** Se in un semigruppo $(S, *)$ esiste un elemento neutro, allora esso è **unico**.
- **Dimostrazione:** Siano u_1 e u_2 due elementi neutri.
  - Consideriamo u_1. Poiché u_2 è neutro (in particolare a destra), $u_1 = u_1 * u_2$.
  - Consideriamo u_2. Poiché u_1 è neutro (in particolare a sinistra), $u_1 * u_2 = u_2$.
  - Mettendo insieme le due uguaglianze: $u_1 = u_1 * u_2 = u_2$. Quindi $u_1 = u_2$.

Elemento Neutro Unicità dell'Elemento Neutro

3.4 Monoidi (Pag 22)

- Un semigruppo $(S, *)$ si dice **monoide** se **esiste** l'elemento neutro $u \in S$.
- Un monoide è quindi una struttura $(S, *, u)$ con $*$ associativa e u elemento neutro per $*$.
- **Esempi di Monoidi (Pag 22):**
  - $(\mathbb{N}, +, 0)$
  - $(\mathbb{N}, \cdot, 1)$ (Anche $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$)
  - $(M_{m,n}(\mathbb{R}), +, 0)$ (dove 0 è la matrice nulla)
  - $(\mathbb{R}^n, +, \vec{0})$ (dove $\vec{0} = (0, \ldots, 0)$ è il vettore nullo)
  - $(P(S), \cap, S)$ (S è neutro per $\cap$: $A \cap S = A$)
  - $(P(S), \cup, \emptyset)$ ($\emptyset$ è neutro per $\cup$: $A \cup \emptyset = A$)
  - $(P(S), \Delta, \emptyset)$ ($\emptyset$ è neutro per Δ: $A \Delta \emptyset = A$)
  - $(A^A, \circ, id_A)$ (L'insieme delle funzioni da A in A con la composizione e l'identità come neutro).

Monoide

---

4. Esercizi Proposti (Pag 23-24)

1. Verificare che le seguenti applicazioni sono biettive e determinarne l'inversa:
   - $f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \times \mathbb{Q}$ con $f(x, y) = (x + y, x - y)$. (Ripetizione es. 2 Lez 4, ma su $\mathbb{Q}$).
   - $f : \mathbb{Q} \to \mathbb{Q}$ con $f(x) = 3x - 7$.
   - $S = \{a, b, c\}$, $A = \{a\}$. $f : P(S) \to P(S)$ con $f(X) = X \Delta A$.
   - $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ con $f(a, b) = (a + b, -b)$.
2. Quali delle seguenti operazioni $*$ sono associative?
   - $(\mathbb{N}, *)$ con $a * b = a \cdot |b|$. (Qui $|b| = b$ in $\mathbb{N}$, quindi $a * b = ab$. Sì).
   - $(\mathbb{Z}, *)$ con $a * b = a \cdot |b|$.
   - $(\mathbb{Z}, *)$ con $a * b = |a \cdot b|$.
   - $(\mathbb{Z}, *)$ con $a * b = a + b + a \cdot b$.

Riepilogo Veloce Lezione 5

- La composizione di funzioni **non è commutativa** ma **è associativa**.
- Una funzione è **invertibile se e solo se è biettiva**, e l'inversa è **unica**.
- L'esistenza di inverse sinistre/destre è legata all'iniettività/suriettività.
- Abbiamo introdotto le **matrici** e alcune operazioni base.
- Un **semigruppo** è $(S, *)$ con $*$ associativa.
- L'**elemento neutro**, se esiste in un semigruppo, è unico.
- Un **monoide** è un semigruppo con elemento neutro.

Prossimi Passi

- Prova a svolgere gli esercizi proposti sulla biettività/inversa e sull'associatività. Sono fondamentali per prendere confidenza.
- Il prossimo passo logico in algebra è introdurre l'ultimo ingrediente per i gruppi: l'**elemento inverso**.

Lezione 6: Monoidi Commutativi, Elementi Invertibili e Gruppi

Data: 28/03/2025 (come da note)
Argomenti: Operazioni (non associative, neutro dx/sx), Prodotto tra matrici (definizione, esempio, non commutatività, associatività, elemento neutro), Monoidi commutativi, Elementi invertibili (simmetrici) in un monoide, Unicità dell'inverso, Gruppo degli elementi invertibili U(S), Inversa della composizione, Definizione di Gruppo, Gruppi Abeliani, Esempi.

#tag/algebraic-structures #tag/monoids #tag/matrices #tag/identity-element #tag/inverse-element #tag/groups #tag/abelian-groups #tag/algebra-avanzata

---

1. Strutture Algebriche: Esempi e Proprietà

1.1 Operazione di Esponenziazione (Pag 1)

- Consideriamo $(\mathbb{N}^*, *)$ dove $\mathbb{N}^* = \{1, 2, 3, \dots\}$ e l'operazione è $a * b = a^b$.
- **Associatività?**
  - $a * (b * c) = a * (b^c) = a^{(b^c)}$
  - $(a * b) * c = (a^b) * c = (a^b)^c = a^{bc}$
  - In generale, $a^{(b^c)} \neq a^{bc}$. Esempio: $2 * (3 * 2) = 2 * (3^2) = 2^9 = 512$. $(2 * 3) * 2 = (2^3) * 2 = 8 * 2 = 8^2 = 64$.
  - Quindi, l'operazione **non è associativa**. $(\mathbb{N}^*, *)$ non è un semigruppo.
- **Elemento Neutro?**
  - Cerchiamo u tale che $a * u = a$ e $u * a = a$ per ogni $a \in \mathbb{N}^*$.
  - $a * u = a \implies a^u = a$. Questo vale per $u = 1$. Quindi 1 è **neutro a destra**.
  - $u * a = a \implies u^a = a$. Questo non vale per un u fisso per tutti gli a. Se $u = 1$, $1^a = 1 \neq a$ (se $a \neq 1$). Quindi 1 **non è neutro a sinistra**.
  - Non esiste un elemento neutro bilatero.

1.2 Prodotto tra Matrici (Pag 2-6)

- **Prodotto Righe per Colonne:** Il prodotto tra una matrice A di dimensione $m \times n$ e una matrice B di dimensione $n \times p$ è definito. (Il numero di colonne di A deve essere uguale al numero di righe di B).
- Il risultato è una matrice $C = A \cdot B$ di dimensione $m \times p$.
- L'elemento c_{ij} della matrice prodotto C (che si trova nella riga i e colonna j) si calcola facendo il prodotto scalare tra la riga i di A e la colonna j di B:

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}$$

- **Esempio (Pag 4):**

  Matrice A (2×3):

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$$

  Matrice B (3×2):

$$B = \begin{pmatrix} 7 & 8 \\ 9 & 10 \\ 11 & 12 \end{pmatrix}$$

Il prodotto $A \cdot B$ è una matrice C (2x2).

$$A \cdot B = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$$

- $c_{11} = (\text{riga 1 di A}) \cdot (\text{colonna 1 di B}) = (1 \cdot 7) + (2 \cdot 9) + (3 \cdot 11) = 7 + 18 + 33 = 58$
- $c_{12} = (\text{riga 1 di A}) \cdot (\text{colonna 2 di B}) = (1 \cdot 8) + (2 \cdot 10) + (3 \cdot 12) = 8 + 20 + 36 = 64$
- $c_{21} = (\text{riga 2 di A}) \cdot (\text{colonna 1 di B}) = (4 \cdot 7) + (5 \cdot 9) + (6 \cdot 11) = 28 + 45 + 66 = 139$
- $c_{22} = (\text{riga 2 di A}) \cdot (\text{colonna 2 di B}) = (4 \cdot 8) + (5 \cdot 10) + (6 \cdot 12) = 32 + 50 + 72 = 154$

$$A \cdot B = \begin{pmatrix} 58 & 64 \\ 139 & 154 \end{pmatrix}$$

- **Prodotto $B \cdot A$ (Pag 5):** Ora B è (3x2) e A è (2x3). Il prodotto è definito e sarà una matrice D (3x3).

$$B \cdot A = \begin{pmatrix} d_{11} & d_{12} & d_{13} \\ d_{21} & d_{22} & d_{23} \\ d_{31} & d_{32} & d_{33} \end{pmatrix}$$

  - $d_{11} = (\text{riga 1 di B}) \cdot (\text{colonna 1 di A}) = (7 \cdot 1) + (8 \cdot 4) = 7 + 32 = 39$
  - $d_{12} = (\text{riga 1 di B}) \cdot (\text{colonna 2 di A}) = (7 \cdot 2) + (8 \cdot 5) = 14 + 40 = 54$
  - ... e così via.

  > **Si vede subito che $A \cdot B \neq B \cdot A$ (non sono nemmeno delle stesse dimensioni in questo caso!). Il prodotto tra matrici non è commutativo.**

- **Matrici Quadrate e Monoide (Pag 6):** Consideriamo l'insieme delle matrici quadrate $n \times n$ a coefficienti reali, $M_{n,n}(\mathbb{R})$ o $M_n(\mathbb{R})$.
  - Il prodotto tra matrici è un'operazione binaria interna su $M_n(\mathbb{R})$.
  - Il prodotto è **associativo**: $(A \cdot B) \cdot C = A \cdot (B \cdot C)$. (Dimostrazione non banale).
  - Esiste l'**elemento neutro**: la **matrice identità** I_n, che ha 1 sulla diagonale principale e 0 altrove.

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

    Vale $A \cdot I_n = I_n \cdot A = A$ per ogni $A \in M_n(\mathbb{R})$.
  - Quindi, $(M_n(\mathbb{R}), \cdot, I_n)$ è un **monoide**.
  - Poiché il prodotto non è commutativo (in generale), è un **monoide non commutativo**.

Prodotto tra Matrici Matrice Identità Monoide non Commutativo

---

2. Monoidi Commutativi

- **Definizione (Pag 9):** Un monoide $(S, *, u)$ si dice **commutativo** (o **abeliano**) se l'operazione $*$ è commutativa:

$$\forall a, b \in S, \quad a * b = b * a$$

- **Esempi di Monoidi Commutativi (Pag 9):**
  - $(\mathbb{N}, +, 0)$, $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$
  - $(\mathbb{N}, \cdot, 1)$, $(\mathbb{Z}, \cdot, 1)$, $(\mathbb{Q}, \cdot, 1)$, $(\mathbb{R}, \cdot, 1)$
  - $(P(S), \cap, S)$
  - $(P(S), \cup, \emptyset)$
  - $(P(S), \Delta, \emptyset)$
- **Esempi di Monoidi NON Commutativi (Pag 9):**
  - $(A^A, \circ, id_A)$ (se $|A| \geq 3$)
  - $(M_n(\mathbb{R}), \cdot, I_n)$ (se $n \geq 2$)
- **Esempio: Monoide Commutativo su $\mathbb{R} \times \mathbb{R}$ (Pag 10-11):**
  - Sia $S = \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$. Definiamo l'operazione $*$:

$$(a, b) * (c, d) = (a + c, b \cdot d)$$

  - Verifichiamo le proprietà:
    1. **Associatività:**
       - $[(a, b) * (c, d)] * (e, f) = (a + c, b \cdot d) * (e, f) = ((a + c) + e, (b \cdot d) \cdot f) = (a + c + e, bdf)$
       - $(a, b) * [(c, d) * (e, f)] = (a, b) * (c + e, d \cdot f) = (a + (c + e), b \cdot (d \cdot f)) = (a + c + e, bdf)$
       - I risultati coincidono. **SÌ, è associativa.**
    2. **Commutatività:**

- $(a,b) * (c,d) = (a+c, b \cdot d)$
- $(c,d) * (a,b) = (c+a, d \cdot b)$
- Poiché $+$ e $\cdot$ sono commutative in $\mathbb{R}$, $a+c=c+a$ e $b \cdot d = d \cdot b$.
- **SÌ, è commutativa.**

3. **Elemento Neutro:** Cerchiamo $(u,v) \in \mathbb{R}^2$ tale che $(a,b) * (u,v) = (a,b)$ per ogni (a,b).
   - $(a,b) * (u,v) = (a+u, b \cdot v)$
   - Vogliamo $(a+u, b \cdot v) = (a,b)$. Questo richiede:
     - $a+u=a \implies u=0$ (per ogni a)
     - $b \cdot v = b \implies v=1$ (per ogni b, attenzione se $b=0$, ma $0 \cdot v = 0$ vale per ogni v. Per $b \neq 0$, $v=1$).
   - L'elemento neutro è $(u,v)=(0,1)$. **SÌ, esiste.**

- Conclusione: $(\mathbb{R}^2, *, (0,1))$ è un **monoide commutativo**.

- **Esempio: $(\mathbb{Z}, *)$ con $a * b = a+b+2ab$ (Pag 12-13):**
  - **Associatività?**
    - $a * (b * c) = a * (b+c+2bc) = a + (b+c+2bc) + 2a(b+c+2bc) = a+b+c+2bc+2ab+2ac+4abc$.
    - $(a * b) * c = (a+b+2ab) * c = (a+b+2ab) + c + 2(a+b+2ab)c = a+b+2ab+c+2ac+2bc+4abc$.
    - I risultati coincidono. **SÌ, è associativa.**
  - **Commutatività?**
    - $a * b = a+b+2ab$
    - $b * a = b+a+2ba$
    - Poiché $+$ e $\cdot$ sono commutative in $\mathbb{Z}$. **SÌ, è commutativa.**
  - **Elemento Neutro?** Cerchiamo $u \in \mathbb{Z}$ tale che $a * u = a$ per ogni a.
    - $a * u = a + u + 2au = a$
    - $u + 2au = 0$
    - $u(1+2a) = 0$
    - Questa equazione deve valere per *ogni* $a \in \mathbb{Z}$. Se $a=0$, $u(1)=0 \implies u=0$. Se $a=1$, $u(3)=0 \implies u=0$. Se $a=-1$, $u(-1)=0 \implies u=0$.
    - Verifichiamo $u=0$: $a * 0 = a+0+2a(0) = a$. Funziona.
    - Poiché è commutativa, $0 * a = a$ vale automaticamente.
    - L'elemento neutro è $u=0$. **SÌ, esiste.**
  - Conclusione: $(\mathbb{Z}, *, 0)$ è un **monoide commutativo**.

Monoide Commutativo

---

3. Elementi Invertibili (Simmetrici) in un Monoide

Sia $(S, *, u)$ un monoide.

- **Definizione (Pag 15):** Un elemento $a \in S$ si dice **invertibile** (o **simmetrizzabile**) se esiste un elemento $a' \in S$ (chiamato **inverso** o **simmetrico** di a) tale che:

$$a * a' = a' * a = u$$

- a' è **inverso destro** se $a * a' = u$.
- a' è **inverso sinistro** se $a' * a = u$.
- a' è inverso (bilatero) se è sia inverso destro sia sinistro.
- **Unicità dell'Inverso (Pag 16):** Se un elemento a in un monoide ammette un inverso a', allora questo inverso è **unico**.
- **Dimostrazione:** Supponiamo che a' e a'' siano entrambi inversi di a.
  - $a * a' = u$ e $a' * a = u$.
  - $a * a'' = u$ e $a'' * a = u$.
  - Consideriamo a'. Possiamo scrivere $a' = a' * u$.
  - Sostituiamo u con $a * a''$: $a' = a' * (a * a'')$.
  - Usiamo l'associatività: $a' = (a' * a) * a''$.
  - Sappiamo che $a' * a = u$: $a' = u * a''$.
  - Poiché u è neutro: $a' = a''$.
  - Quindi l'inverso, se esiste, è unico.
- **Notazione:** L'inverso di a, se esiste, si denota spesso a^{-1} (notazione moltiplicativa) o $-a$ (notazione additiva).
- **Gruppo degli Elementi Invertibili $U(S)$ (Pag 16):**
  - L'insieme di tutti gli elementi invertibili di un monoide $(S, *, u)$ si denota $U(S)$ (o S^*, o $S^\times$).
  - $U(S) = \{a \in S \mid \exists a' \in S : a * a' = a' * a = u\}$.

- L'elemento neutro u è sempre invertibile ($u * u = u$), quindi $u \in U(S)$, e $U(S)$ è **sempre non vuoto**.
- **Teorema (Pag 24):** $(U(S), *)$ è un **gruppo**. In particolare, $U(S)$ è **chiuso** rispetto all'operazione $*$.
  - **Dimostrazione Chiusura:** Siano $a, b \in U(S)$. Dobbiamo dimostrare che $a * b \in U(S)$. Esistono $a', b' \in S$ tali che $a * a' = a' * a = u$ e $b * b' = b' * b = u$. Cerchiamo l'inverso di $(a * b)$. Proviamo con $(b' * a')$.
    - $(a * b) * (b' * a') = a * (b * b') * a'$ (associatività) $= a * u * a' = a * a' = u$.
    - $(b' * a') * (a * b) = b' * (a' * a) * b$ (associatività) $= b' * u * b = b' * b = u$.
    - Abbiamo trovato l'inverso di $a * b$, che è $b' * a'$. Quindi $a * b \in U(S)$.
  - L'operazione è associativa perché lo è in S. $u \in U(S)$ è l'elemento neutro. Ogni elemento in $U(S)$ ha un inverso per definizione. Quindi $(U(S), *)$ è un gruppo.
- **Inversa della Composizione (Pag 25):** Se f, g sono funzioni invertibili (biettive) e la composizione $f \circ g$ è definita, allora anche $f \circ g$ è invertibile e vale:

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}$$

  - **Spiegazione:** Per annullare "prima g poi f", devi annullare "prima f (con f^{-1}) poi g (con g^{-1})". L'ordine si inverte. Questa regola vale in generale per gli inversi in $U(S)$: $(a * b)' = b' * a'$.

Elemento Invertibile (Simmetrico) Unicità dell'Inverso Gruppo degli Elementi Invertibili Inverso di una Composizione

3.5 Esempi di U(S) (Pag 17-18)

- $(\mathbb{N}, +, 0)$: $U(\mathbb{N}, +) = \{0\}$. (Solo 0 ha un opposto in $\mathbb{N}$).
- $(\mathbb{N}, \cdot, 1)$: $U(\mathbb{N}, \cdot) = \{1\}$. (Solo 1 ha un reciproco in $\mathbb{N}$).
- $(\mathbb{Z}, +, 0)$: $U(\mathbb{Z}, +) = \mathbb{Z}$. (Ogni intero a ha opposto $-a \in \mathbb{Z}$).
- $(\mathbb{Z}, \cdot, 1)$: $U(\mathbb{Z}, \cdot) = \{1, -1\}$. (Solo 1 e -1 hanno reciproco intero).
- $(\mathbb{Q}, \cdot, 1)$: $U(\mathbb{Q}, \cdot) = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.
- $(\mathbb{R}, \cdot, 1)$: $U(\mathbb{R}, \cdot) = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$.
- $(\mathbb{Q}, +, 0)$: $U(\mathbb{Q}, +) = \mathbb{Q}$.
- $(\mathbb{R}, +, 0)$: $U(\mathbb{R}, +) = \mathbb{R}$.
- $(\mathbb{R}^2, \cdot)$ con $(a, b) \cdot (c, d) = (ac, bd)$ e $u = (1, 1)$:
  $U(\mathbb{R}^2, \cdot) = \{(a, b) \in \mathbb{R}^2 \mid a \neq 0 \wedge b \neq 0\} = \mathbb{R}^* \times \mathbb{R}^*$.
- $(S = \mathbb{R} \times \{0\}, \cdot)$ con $u = (1, 0)$:
  $U(S) = \{(a, 0) \in S \mid a \neq 0\} = \mathbb{R}^* \times \{0\}$.
- $(A^A, \circ, id_A)$: $U(A^A) = \{f \in A^A \mid f \text{ è biettiva}\}$. (Chiamato Gruppo delle Permutazioni o Simmetrico S_A).
- $(M_n(\mathbb{R}), \cdot, I_n)$: $U(M_n(\mathbb{R})) = GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$. (Gruppo Lineare Generale).
- $(P(S), \cap, S)$: $U(P(S), \cap) = \{S\}$. (Solo S ha inverso S perché $S \cap S = S$).
- $(P(S), \cup, \emptyset)$: $U(P(S), \cup) = \{\emptyset\}$. (Solo $\emptyset$ ha inverso $\emptyset$ perché $\emptyset \cup \emptyset = \emptyset$).
- $(P(S), \Delta, \emptyset)$: $A \Delta A' = \emptyset \iff A = A'$. Quindi l'inverso di A è A stesso. $U(P(S), \Delta) = P(S)$.
- **Esempio $(\mathbb{Z}, *)$ con $a * b = a + b + 2ab$ e $u = 0$ (Pag 19-20):**
  - Cerchiamo l'inverso a' di a. Vogliamo $a * a' = 0$.
  - $a + a' + 2aa' = 0$
  - $a'(1 + 2a) = -a$
  - $a' = \frac{-a}{1+2a}$
  - Questo a' deve essere un intero $\mathbb{Z}$. Quando succede?
    - Se $a = 0$, $a' = 0/1 = 0$. 0 è inverso di se stesso. $0 \in U(\mathbb{Z}, *)$.
    - Se $a = -1$, $a' = -(-1)/(1 + 2(-1)) = 1/(1 - 2) = 1/(-1) = -1$. -1 è inverso di se stesso. $-1 \in U(\mathbb{Z}, *)$.
    - Se $a = 1$, $a' = -1/(1 + 2) = -1/3 \notin \mathbb{Z}$.
    - Se $a = -2$, $a' = -(-2)/(1 - 4) = 2/(-3) \notin \mathbb{Z}$.
    - Sembra che a' sia intero solo se $1 + 2a$ divide $-a$. Questo accade solo per $a = 0$ e $a = -1$.
  - Quindi $U(\mathbb{Z}, *) = \{0, -1\}$.

---

4. Sottostrutture Stabili (Parti Chiuse)

- **Definizione (Pag 21):** Sia $(S, *)$ una struttura con un'operazione binaria interna. Un sottoinsieme non vuoto $H \subseteq S$ si dice **stabile** (o **parte chiusa**) rispetto a $*$ se:

$$\forall h, k \in H, \quad h * k \in H$$

  - **Spiegazione:** Se prendi due elementi qualsiasi dentro H e applichi l'operazione $*$, il risultato deve rimanere dentro H.
- **Esempi (Pag 22-23):**
  - $S = \{0, 1, \ldots, 9\}$. $(P(S), \cap)$. $H = \{X \in P(S) \mid 1 \in X \wedge 5 \in X\}$.
    - H è stabile per $\cap$? Siano $X, Y \in H$. Allora $1, 5 \in X$ e $1, 5 \in Y$. Ne segue che $1, 5 \in X \cap Y$. Quindi $X \cap Y \in H$. **SÌ**.
    - H è stabile per $\cup$? Siano $X, Y \in H$. Allora $1, 5 \in X$ e $1, 5 \in Y$. Ne segue che $1, 5 \in X \cup Y$. Quindi $X \cup Y \in H$. **SÌ**.

    - H è stabile per Δ? $X \Delta Y = (X \cup Y) \setminus (X \cap Y)$. Se $X = \{1,5\}$ e $Y = \{1,5,2\}$, entrambi in H. $X \Delta Y = \{1,2,5\} \setminus \{1,5\} = \{2\}$. Ma $\{2\} \notin H$. **NO**.
  - $(\mathbb{Z}, +)$. $D = \{2n+1 \mid n \in \mathbb{Z}\}$ (interi dispari).
    - D è stabile per $+$? Siano $a = 2n+1, b = 2m+1 \in D$. $a+b = (2n+1)+(2m+1) = 2n+2m+2 = 2(n+m+1)$. Questo è un numero pari. Non appartiene a D. **NO**.
  - $(A^A, \circ)$. $C = \{f \in A^A \mid f \text{ è costante}\}$.
    - C è stabile per $\circ$? Siano $f, g \in C$. $f(x) = c_1$, $g(x) = c_2$ per ogni x.
    - $(f \circ g)(x) = f(g(x)) = f(c_2) = c_1$. La funzione composta è la funzione costante uguale a c_1. Quindi $f \circ g \in C$. **SÌ**.
  - $(\mathbb{R}^2, \cdot)$ con $(a,b) \cdot (c,d) = (ac, bd)$. $S = \mathbb{R} \times \{0\} = \{(a,0) \mid a \in \mathbb{R}\}$.
    - S è stabile? Siano $(a,0), (b,0) \in S$. $(a,0) \cdot (b,0) = (a \cdot b, 0 \cdot 0) = (ab, 0)$. Poiché $ab \in \mathbb{R}$, il risultato $(ab,0)$ è ancora in S. **SÌ**.
  - $(\mathbb{R}^2, \cdot)$. $T = \{(a,-1) \mid a \in \mathbb{R}\}$.
    - T è stabile? Siano $(a,-1), (b,-1) \in T$. $(a,-1) \cdot (b,-1) = (a \cdot b, (-1) \cdot (-1)) = (ab, 1)$. Poiché la seconda componente è 1 (e non -1), il risultato $(ab,1)$ **non** appartiene a T. **NO**.
- **Proprietà (Pag 24):** Se $(S, *)$ è un semigruppo (o monoide) e $H \subseteq S$ è una parte stabile, allora $(H, *)$ è anch'esso un semigruppo. Se S è monoide con neutro u, $(H, *)$ è un monoide solo se $u \in H$. L'elemento neutro di H sarà lo stesso u.

Parte Stabile (Sottoinsieme Chiuso)

---

5. Gruppi

La struttura algebrica fondamentale.

- **Definizione (Pag 26):** Una struttura $(G, *)$ è un **gruppo** se:
  1. $*$ è **associativa** (quindi $(G, *)$ è un semigruppo).
  2. Esiste l'**elemento neutro** $u \in G$ (quindi $(G, *, u)$ è un monoide).
  3. **Ogni elemento** $a \in G$ è **invertibile** (ammette simmetrico) in G. (Cioè, $U(G) = G$).
- **Gruppo Abeliano (Commutativo) (Pag 27):** Un gruppo $(G, *)$ si dice **abeliano** se l'operazione $*$ è **commutativa**.
- **Esempi di Gruppi (Pag 26-27):**
  - $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ (Abeliani)
  - $(\mathbb{R}^n, +)$ (Abeliano)
  - $(M_{m,n}(\mathbb{R}), +)$ (Abeliano)
  - $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ (Abeliani)
  - $(P(S), \Delta)$ (Abeliano, neutro $\emptyset$, inverso di A è A stesso).
  - $(B(A) = \{f : A \to A \mid f \text{ biettiva}\}, \circ)$ (Gruppo Simmetrico S_A, non abeliano se $|A| \geq 3$).
  - $(GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}, \cdot)$ (Gruppo Lineare Generale, non abeliano se $n \geq 2$).
- **Esempi di Monoidi che NON sono Gruppi:**
  - $(\mathbb{N}, +, 0)$ (mancano inversi tranne per 0)
  - $(\mathbb{Z}, \cdot, 1)$ (mancano inversi tranne per 1, -1)
  - $(P(S), \cap, S)$ (mancano inversi tranne per S)
  - $(P(S), \cup, \emptyset)$ (mancano inversi tranne per $\emptyset$)
  - $(M_n(\mathbb{R}), \cdot, I_n)$ (le matrici non invertibili non hanno inverso)

Gruppo (matematica) Gruppo Abeliano

Riepilogo Veloce Lezione 6

- Abbiamo visto che l'esponenziazione non è associativa.
- Abbiamo definito e praticato il **prodotto tra matrici**, notando che è associativo ma non commutativo, e che $(M_n(\mathbb{R}), \cdot, I_n)$ è un monoide.
- Abbiamo definito i **monoidi commutativi**.
- Abbiamo definito l'**elemento invertibile (simmetrico)** in un monoide e dimostrato la sua **unicità**.
- Abbiamo introdotto il **gruppo degli elementi invertibili** $U(S)$ di un monoide S, dimostrando che è chiuso e forma un gruppo.
- Abbiamo visto la regola per l'**inversa della composizione**: $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.
- Abbiamo definito una **parte stabile (chiusa)** $H \subseteq S$.
- Abbiamo finalmente definito la struttura di **Gruppo** (associatività, neutro, inverso per tutti gli elementi) e di **Gruppo Abeliano** (gruppo con operazione commutativa).
- Abbiamo visto numerosi esempi di gruppi e monoidi.

Prossimi Passi

- Assicurati di aver ben compreso la definizione di Gruppo e le sue proprietà costitutive.
- Rivedi gli esempi di gruppi e monoidi, cercando di capire perché alcuni lo sono e altri no.
- Il prossimo passo sarà esplorare le proprietà fondamentali dei gruppi e introdurre i sottogruppi.

Lezione 7: Gruppi (Recap), Anelli, Caratteristica, Cancellabilità e Divisori dello Zero

Data: 01/04/2025 (come da note)
Argomenti: Definizione di Gruppo (recap), Esempi (Abeliani/Non Abeliani), Matrici (notazione, inversa 2x2), Verifica proprietà strutture algebriche, Definizione di Anello, Esempi di Anelli (P(S), Matrici), Anello Commutativo, Anello Unitario, Caratteristica di un Anello, Elementi Cancellabili, Divisori dello Zero.

#tag/algebraic-structures #tag/groups #tag/abelian-groups #tag/rings #tag/matrices #tag/cancellable-element #tag/zero-divisor #tag/characteristic #tag/algebra-avanzata

---

1. Gruppi: Definizione ed Esempi (Recap)

- **Definizione (Pag 1):** Una struttura $(G, *)$ è un **Gruppo** se:
  1. $*$ è **associativa** (Semigruppo)
  2. Esiste l'**elemento neutro** $u \in G$ (Monoide)
  3. **Ogni elemento** $a \in G$ è **invertibile** (o simmetrizzabile) in G (cioè $U(G) = G$).
- **Esempi (Pag 1, 5):**
  - **Gruppi Abeliani (Commutativi):**
    - $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$
    - $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ (dove $X^* = X \setminus \{0\}$)
    - $(\{1, -1\}, \cdot)$
    - $(\mathbb{R}^n, +)$ (somma vettoriale)
    - $(M_{m,n}(\mathbb{R}), +)$ (somma matriciale)
    - $(P(S), \Delta)$ (differenza simmetrica)
  - **Gruppi NON Abeliani (Non Commutativi):**
    - $(B(A) = \{f : A \to A \mid f \text{ biettiva}\}, \circ)$ (Gruppo Simmetrico S_A, se $|A| \geq 3$)
    - $(GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}, \cdot)$ (Gruppo Lineare Generale, se $n \geq 2$)

Gruppo (matematica) Gruppo Abeliano

---

2. Matrici: Notazione e Inversa 2x2

- **Notazione (Pag 2):** Una matrice $A = (a_{ij})_{\substack{i=1..m \\ j=1..n}}$ può essere vista come:
  - Un insieme di vettori colonna: $A = (C^1 | C^2 | \dots | C^n)$ dove $C^j \in \mathbb{R}^m$.
  - Un insieme di vettori riga: $A = \begin{pmatrix} R_1 \\ \vdots \\ R_m \end{pmatrix}$ dove $R_i \in \mathbb{R}^n$.
- **Matrice Diagonale:** Una matrice quadrata D è diagonale se $d_{ij} = 0$ per ogni $i \neq j$.
- **Matrice Identità I_n:** Matrice diagonale con $a_{ii} = 1$ per ogni i.
- **Matrice Nulla O:** Matrice con tutti gli elementi uguali a 0.
- **Inversa di una Matrice 2x2 (Pag 3):**
  Sia $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ una matrice 2×2.
  - Il **determinante** di A è $\det(A) = |A| = ad - bc$.
  - Se $\det(A) \neq 0$, allora A è invertibile e la sua inversa è:

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

  - **Spiegazione:** Si scambiano gli elementi sulla diagonale principale (a, d), si cambiano i segni degli elementi sull'altra diagonale $(-b, -c)$, e si divide tutto per il determinante.
- **Esempio (Pag 4):**

$$A = \begin{pmatrix} 2 & 2 \\ 5 & 3 \end{pmatrix}$$

- $\det(A) = (2)(3) - (2)(5) = 6 - 10 = -4$. Poiché $\det(A) \neq 0$, A è invertibile.
- $A^{-1} = \frac{1}{-4}\begin{pmatrix} 3 & -2 \\ -5 & 2 \end{pmatrix} = \begin{pmatrix} -3/4 & 1/2 \\ 5/4 & -1/2 \end{pmatrix}$.
- **Verifica:**
  - $A^{-1} \cdot A = \begin{pmatrix} -3/4 & 1/2 \\ 5/4 & -1/2 \end{pmatrix}\begin{pmatrix} 2 & 2 \\ 5 & 3 \end{pmatrix} = \begin{pmatrix} (-6/4+5/2) & (-6/4+3/2) \\ (10/4-5/2) & (10/4-3/2) \end{pmatrix} = \begin{pmatrix} (-3/2+5/2) & (-3/2+3/2) \\ (5/2-5/2) & (5/2-3/2) \end{pmatrix} = \begin{pmatrix} 2/2 & 0 \\ 0 & 2/2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} =$.
  - $A \cdot A^{-1} = \begin{pmatrix} 2 & 2 \\ 5 & 3 \end{pmatrix}\begin{pmatrix} -3/4 & 1/2 \\ 5/4 & -1/2 \end{pmatrix} = \begin{pmatrix} (-6/4+10/4) & (2/2-2/2) \\ (-15/4+15/4) & (5/2-3/2) \end{pmatrix} = \begin{pmatrix} 4/4 & 0 \\ 0 & 2/2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$. OK.

Determinante Matrice Invertibile

---

3. Esempi di Strutture Algebriche: Verifica Proprietà

- **Esempio 1:** $(\mathbb{Q}, *)$ **con** $a * b = a + b - 3ab$ **(Pag 6-9):**
  1. **Associatività?**
     - $a * (b * c) = a * (b + c - 3bc) = a + (b + c - 3bc) - 3a(b + c - 3bc) = a + b + c - 3bc - 3ab - 3ac + 9abc$.
     - $(a * b) * c = (a + b - 3ab) * c = (a + b - 3ab) + c - 3(a + b - 3ab)c = a + b - 3ab + c - 3ac - 3bc + 9abc$.
     - I risultati coincidono. **SÌ, è associativa.**
  2. **Commutatività?**
     - $a * b = a + b - 3ab$.
     - $b * a = b + a - 3ba$.
     - Poiché $+$ e $\cdot$ sono commutative in $\mathbb{Q}$. **SÌ, è commutativa.**
  3. **Elemento Neutro?** Cerchiamo $u \in \mathbb{Q}$ tale che $a * u = a$.
     - $a + u - 3au = a \implies u - 3au = 0 \implies u(1 - 3a) = 0$.
     - Questa deve valere per *ogni* $a \in \mathbb{Q}$. L'unico modo è che $u = 0$.
     - Verifica: $a * 0 = a + 0 - 3a(0) = a$. **SÌ,** $u = 0$ **è l'elemento neutro.**
     - Quindi $(\mathbb{Q}, *, 0)$ è un **monoide commutativo**.
  4. **Elementi Invertibili** $U(\mathbb{Q}, *)$**?** Cerchiamo a' tale che $a * a' = 0$.
     - $a + a' - 3aa' = 0 \implies a'(1 - 3a) = -a$.
     - $a' = \frac{-a}{1-3a}$.
     - Questo a' esiste ed è in $\mathbb{Q}$ se e solo se il denominatore $1 - 3a \neq 0$.
     - $1 - 3a \neq 0 \iff 3a \neq 1 \iff a \neq 1/3$.
     - Quindi, tutti gli elementi $a \in \mathbb{Q}$ tranne $a = 1/3$ sono invertibili.
     - $U(\mathbb{Q}, *) = \mathbb{Q} \setminus \{1/3\}$.
     - Esempio: L'inverso di $a = 5$ è $a' = \frac{-5}{1-3(5)} = \frac{-5}{1-15} = \frac{-5}{-14} = 5/14$.
  5. **È un gruppo? NO**, perché l'elemento $1/3$ non ha inverso.
- **Esempio 2:** $(\mathbb{R}^2, *)$ **con** $(a_1, a_2) * (b_1, b_2) = (3a_1b_1, a_2 + b_2 - 3a_2b_2)$ **(Pag 10-13):**
  1. **Associatività?**
     - $[(a_1, a_2) * (b_1, b_2)] * (c_1, c_2) = (3a_1b_1, a_2 + b_2 - 3a_2b_2) * (c_1, c_2) = (3(3a_1b_1)c_1, (a_2 + b_2 - 3a_2b_2) + c_2 - 3(a_2 + b_2 - 3a_2b_2)c_2) = (9a_1b_1$.
     - $(a_1, a_2) * [(b_1, b_2) * (c_1, c_2)] = (a_1, a_2) * (3b_1c_1, b_2 + c_2 - 3b_2c_2) = (3a_1(3b_1c_1), a_2 + (b_2 + c_2 - 3b_2c_2) - 3a_2(b_2 + c_2 - 3b_2c_2)) = (9a_1b_1c$.
     - I risultati coincidono. **SÌ, è associativa.**
  2. **Commutatività?**
     - $(a_1, a_2) * (b_1, b_2) = (3a_1b_1, a_2 + b_2 - 3a_2b_2)$.
     - $(b_1, b_2) * (a_1, a_2) = (3b_1a_1, b_2 + a_2 - 3b_2a_2)$.
     - Poiché $\cdot$ e $+$ sono commutative in $\mathbb{R}$. **SÌ, è commutativa.**
  3. **Elemento Neutro?** Cerchiamo $u = (u_1, u_2)$ tale che $(a_1, a_2) * (u_1, u_2) = (a_1, a_2)$.
     - $(3a_1u_1, a_2 + u_2 - 3a_2u_2) = (a_1, a_2)$.
     - Deve valere per ogni (a_1, a_2):
       - $3a_1u_1 = a_1 \implies 3u_1 = 1 \implies u_1 = 1/3$.
       - $a_2 + u_2 - 3a_2u_2 = a_2 \implies u_2 - 3a_2u_2 = 0 \implies u_2(1 - 3a_2) = 0$. Questo deve valere per ogni a_2, quindi $u_2 = 0$.
     - L'elemento neutro è $u = (1/3, 0)$. **SÌ, esiste.**
     - Quindi $(\mathbb{R}^2, *, (1/3, 0))$ è un **monoide commutativo**.
  4. **Elementi Invertibili** $U(\mathbb{R}^2, *)$**?** Cerchiamo $(\bar{a}_1, \bar{a}_2)$ tale che $(a_1, a_2) * (\bar{a}_1, \bar{a}_2) = (1/3, 0)$.
     - $(3a_1\bar{a}_1, a_2 + \bar{a}_2 - 3a_2\bar{a}_2) = (1/3, 0)$.
     - $3a_1\bar{a}_1 = 1/3 \implies \bar{a}_1 = \frac{1}{9a_1}$. Esiste se $a_1 \neq 0$.
     - $a_2 + \bar{a}_2 - 3a_2\bar{a}_2 = 0 \implies \bar{a}_2(1 - 3a_2) = -a_2 \implies \bar{a}_2 = \frac{-a_2}{1-3a_2}$. Esiste se $a_2 \neq 1/3$.
     - Quindi, (a_1, a_2) è invertibile se e solo se $a_1 \neq 0$ e $a_2 \neq 1/3$.

- $U(\mathbb{R}^2, *) = \{(a_1, a_2) \in \mathbb{R}^2 \mid a_1 \neq 0 \wedge a_2 \neq 1/3\}$.
- Esempio: L'inverso di $(5,7)$ è $(\bar{a}_1, \bar{a}_2)$ con $\bar{a}_1 = 1/(9 \cdot 5) = 1/45$ e $\bar{a}_2 = -7/(1 - 3 \cdot 7) = -7/(1 - 21) = -7/(-20) = 7/20$. Inverso: $(1/45, 7/20)$.

---

4. Anelli: La Struttura con Due Operazioni

Passiamo ora a strutture algebriche un po' più ricche, che hanno due operazioni che interagiscono tra loro. Pensa a come i numeri interi $\mathbb{Z}$ hanno sia la somma che il prodotto, e queste operazioni non vivono per conto loro, ma sono legate dalla proprietà distributiva.

- **Definizione Generale di Anello (Pag 19):** Una struttura $(A, +, \cdot)$ è un **Anello** se soddisfa queste tre condizioni fondamentali:
  1. **La "somma" è un Gruppo Abeliano:** L'operazione $+$ rende $(A, +)$ un gruppo abeliano. Questo significa che:
     - $+$ è **associativa**: $(a + b) + c = a + (b + c)$ per ogni $a, b, c \in A$.
     - $+$ è **commutativa**: $a + b = b + a$ per ogni $a, b \in A$.
     - Esiste un **elemento neutro** per $+$, che chiamiamo lo **zero** dell'anello, denotato 0_A, tale che $a + 0_A = 0_A + a = a$ per ogni $a \in A$.
     - Ogni elemento $a \in A$ ha un **inverso additivo** (o opposto), denotato $-a$, tale che $a + (-a) = (-a) + a = 0_A$.
  2. **Il "prodotto" è un Semigruppo:** L'operazione $\cdot$ rende $(A, \cdot)$ un semigruppo. Questo significa che:
     - $\cdot$ è **associativa**: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ per ogni $a, b, c \in A$.
  3. **Il Prodotto si Distribuisce sulla Somma:** Le due operazioni sono legate dalle proprietà distributive:
     - **Distributiva sinistra:** $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ per ogni $a, b, c \in A$.
     - **Distributiva destra:** $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ per ogni $a, b, c \in A$.
- **Esempi Comuni di Anelli (Pag 20):**
  - $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ con le usuali somma e prodotto.
  - $(\mathbb{R}^n, +, \cdot)$ dove $+$ è la somma vettoriale e $\cdot$ è il prodotto **componente per componente**.
  - $(M_n(\mathbb{R}), +, \cdot)$ con la somma e il prodotto righe per colonne tra matrici $n \times n$.
  - $(\mathbb{Z}^{\mathbb{Z}}, +, \cdot)$ (l'insieme delle funzioni da $\mathbb{Z}$ a $\mathbb{Z}$ con somma e prodotto definiti "punto per punto": $(f + g)(x) = f(x) + g(x)$ e $(f \cdot g)(x) = f(x) \cdot g(x)$).

Anello (matematica) Proprietà Distributiva

4.1 Anelli Booleani: Una Proprietà Speciale

Ora, esiste una classe speciale di anelli che ha un nome specifico: gli Anelli Booleani.

- **Definizione di Anello Booleano:** Un anello $(A, +, \cdot)$ si dice **Anello Booleano** se, oltre a soddisfare le tre proprietà della definizione generale di Anello, ha anche questa proprietà aggiuntiva:
  - **Idempotenza del Prodotto:** Per ogni elemento $a \in A$, vale $a \cdot a = a$.

Pensa all'idempotenza come a un'operazione che, se applicata due volte di seguito allo stesso elemento, non cambia il risultato rispetto ad applicarla una sola volta.

- **Esempio Fondamentale: L'Anello Booleano dei Sottoinsiemi $(P(S), \Delta, \cap)$ (Pag 20):**
  Consideriamo l'insieme delle parti $P(S)$ di un insieme S, con l'operazione di "somma" data dalla differenza simmetrica Δ e l'operazione di "prodotto" data dall'intersezione $\cap$.
  - **È un Anello?** Le tue note verificano in modo eccellente che $(P(S), \Delta, \cap)$ è un anello generale:
    - $(P(S), \Delta)$ è un gruppo abeliano (l'elemento neutro è l'insieme vuoto $\emptyset$, e ogni insieme è l'inverso di se stesso rispetto a Δ).
    - $(P(S), \cap)$ è un semigruppo (l'intersezione è associativa).
    - L'intersezione $\cap$ è distributiva rispetto alla differenza simmetrica Δ. Le note mostrano la verifica dettagliata di questa proprietà cruciale: $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$.
  - **È un Anello Booleano?** Per esserlo, deve soddisfare anche la proprietà di idempotenza per il prodotto $\cap$. Dobbiamo verificare se per ogni $A \in P(S)$, vale $A \cap A = A$.
    - Ebbene sì! Per la definizione stessa di intersezione, l'intersezione di un insieme con se stesso è sempre l'insieme stesso. $A \cap A = A$ vale per qualsiasi insieme A.
  - **Conclusione:** Poiché $(P(S), \Delta, \cap)$ è un anello e soddisfa la proprietà $A \cap A = A$ per ogni suo elemento A, è effettivamente un **Anello Booleano**.
- **Esempio di NON Anello (Pag 22):** $(P(S), \Delta, \cup)$.
  Come mostrano le note, questa struttura non è un anello perché l'unione $\cup$ non si distribuisce sulla differenza simmetrica Δ. Abbiamo visto il controesempio con insiemi specifici $\{a\}, \{b\}, \{c\}$. Quindi, non ha senso chiedersi se sia un Anello Booleano, perché non è nemmeno un Anello!

Anello Booleano Idempotenza

4.2 Tipi di Anelli Aggiuntivi

Oltre agli Anelli Booleani, ci sono altre proprietà che un anello può avere:

- **Anello Commutativo (Pag 24):** Un anello $(A, +, \cdot)$ è **commutativo** se l'operazione di prodotto $\cdot$ è commutativa, cioè $a \cdot b = b \cdot a$ per ogni $a, b \in A$.
  - Esempi: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\mathbb{R}^n$, $(P(S), \Delta, \cap)$ (l'intersezione è commutativa!), $(\mathbb{Z}^{\mathbb{Z}}, +, \cdot)$.
  - Non Esempio: $(M_n(\mathbb{R}), +, \cdot)$ per $n \geq 2$ (il prodotto tra matrici in generale non è commutativo).
- **Anello Unitario (con unità) (Pag 24):** Un anello $(A, +, \cdot)$ è **unitario** se il semigruppo $(A, \cdot)$ è un **monoide**, cioè se esiste un elemento neutro per il prodotto $\cdot$, che chiamiamo l'**unità** dell'anello, denotato 1_A, tale che $a \cdot 1_A = 1_A \cdot a = a$ per ogni $a \in A$.
  - Esempi: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (unità 1), $(M_n(\mathbb{R}), +, \cdot)$ (unità I_n, la matrice identità), $(P(S), \Delta, \cap)$ (l'unità è l'insieme S, perché $A \cap S = A$ per ogni $A \in P(S)$), $(\mathbb{Z}^{\mathbb{Z}}, +, \cdot)$ (l'unità è la funzione costante $f(x) = 1$).
- **Anello Commutativo Unitario:** Un anello che è sia commutativo che unitario. (Es. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, $(P(S), \Delta, \cap)$).

Anello Commutativo Anello Unitario

4.3 Caratteristica di un Anello Unitario (Pag 25)

Questa è una proprietà interessante che si definisce solo per anelli che hanno un'unità moltiplicativa.

Sia $(A, +, \cdot)$ un anello unitario con unità 1_A.

- Consideriamo i multipli additivi dell'unità: $n \cdot 1_A$ è la somma di 1_A con se stesso n volte (per $n > 0$). Ad esempio, $2 \cdot 1_A = 1_A + 1_A$. Definiamo $0 \cdot 1_A = 0_A$ e $(-n) \cdot 1_A = -(n \cdot 1_A)$.
- La **caratteristica** dell'anello A, denotata $char(A)$, è definita come:
  - $char(A) = 0$ se $n \cdot 1_A \neq 0_A$ per ogni intero positivo $n \geq 1$. In altre parole, non importa quante volte sommi l'unità a se stessa, non otterrai mai lo zero dell'anello (a meno che non la sommi 0 volte).
  - $char(A) = m$ se m è il **più piccolo intero positivo** tale che $m \cdot 1_A = 0_A$. Qui, sommando l'unità a se stessa m volte ottieni lo zero dell'anello, e m è il primo numero positivo per cui succede.
- **Esempi di Caratteristica (Pag 26):**
  - $char(\mathbb{Z}) = 0$, $char(\mathbb{Q}) = 0$, $char(\mathbb{R}) = 0$, $char(\mathbb{C}) = 0$. (Perché in questi anelli, $n \cdot 1 = n$, e n è diverso da 0 per ogni $n \geq 1$).
  - $char(P(S), \Delta, \cap) = 2$. L'unità è S. Il neutro additivo (zero dell'anello) è $\emptyset$.
    - $1 \cdot S = S$. Se S non è vuoto, $S \neq \emptyset$.
    - $2 \cdot S = S \Delta S$. Ricordi la differenza simmetrica di un insieme con se stesso? $S \Delta S = (S \setminus S) \cup (S \setminus S) = \emptyset \cup \emptyset = \emptyset$.
    - Quindi, $2 \cdot S = \emptyset$. Il più piccolo intero positivo m tale che $m \cdot S = \emptyset$ è $m = 2$. La caratteristica è 2.

Caratteristica (algebra)

---

5. Elementi Cancellabili e Divisori dello Zero

Proprietà degli elementi rispetto a un'operazione.

5.1 Elementi Cancellabili (Pag 27-28)

Sia $(S, *)$ una struttura con operazione binaria. Un elemento $a \in S$ è:

- **Cancellabile a sinistra** se: $\forall b, c \in S, \quad a * b = a * c \implies b = c$.
- **Cancellabile a destra** se: $\forall b, c \in S, \quad b * a = c * a \implies b = c$.
- **Cancellabile** (bilatero) se è cancellabile sia a sinistra sia a destra.
- **Esempi:**
  - $(P(S), \cap)$: $A = \{a\}, B = \{b\}, C = \{c\}$. $A \cap B = \emptyset$, $A \cap C = \emptyset$. Ma $B \neq C$. Quindi $A = \{a\}$ non è cancellabile a sinistra (e per commutatività, neanche a destra). In generale, in $(P(S), \cap)$ solo S è cancellabile.
  - $(\mathbb{Z}, \cdot)$: Gli elementi cancellabili sono tutti gli interi **diversi da 0**. Se $a \neq 0$ e $ab = ac$, allora $a(b - c) = 0$, che implica $b - c = 0$, cioè $b = c$. Se $a = 0$, $0 \cdot b = 0 \cdot c$ (cioè $0 = 0$) non implica $b = c$.
- **Relazione con Invertibilità (Pag 29):** In un monoide $(S, *, u)$:
  - Se $a \in S$ è **invertibile**, allora a è **cancellabile** (sia a sinistra che a destra).
  - **Dimostrazione (cancellabile a sinistra):** Supponiamo $a * b = a * c$. Poiché a è invertibile, esiste a'. Moltiplichiamo a sinistra per a':
    - $a' * (a * b) = a' * (a * c)$
    - $(a' * a) * b = (a' * a) * c$ (Associatività)
    - $u * b = u * c$
    - $b = c$. OK. (Dimostrazione analoga per destra).

- **Il viceversa NON vale in generale:** Un elemento può essere cancellabile senza essere invertibile.
  - Esempio: In $(\mathbb{Z}, \cdot)$, l'elemento 2 è cancellabile ($2b = 2c \implies b = c$), ma non è invertibile (il suo inverso $1/2$ non è in $\mathbb{Z}$).

Elemento Cancellabile

5.2 Divisori dello Zero (Pag 30-31)

Concetto specifico degli anelli $(A, +, \cdot)$.

- **Definizione:** Un elemento $a \in A$, con $a \neq 0_A$, si dice **divisore dello zero** se esiste un elemento $b \in A$, con $b \neq 0_A$, tale che $a \cdot b = 0_A$ oppure $b \cdot a = 0_A$.
  - Se $a \cdot b = 0_A$ con $a, b \neq 0_A$, a è un divisore dello zero a sinistra, b è un divisore dello zero a destra.
  - Se l'anello è commutativo, la distinzione sx/dx non serve.
- **Relazione con Cancellabilità (Pag 31):** In un anello $(A, +, \cdot)$:
  - Un elemento $a \neq 0_A$ è un **divisore dello zero** $\iff$ a **non è cancellabile** rispetto al prodotto $\cdot$.
  - **Dimostrazione ($\implies$):** Se a è divisore dello zero, esiste $b \neq 0_A$ tale che $a \cdot b = 0_A$. Ma sappiamo anche che $a \cdot 0_A = 0_A$. Quindi $a \cdot b = a \cdot 0_A$. Se a fosse cancellabile (a sinistra), dovremmo concludere $b = 0_A$, ma avevamo $b \neq 0_A$. Assurdo. Quindi a non può essere cancellabile. (Dimostrazione simile se $b \cdot a = 0_A$).
  - **Dimostrazione ($\impliedby$):** Se $a \neq 0_A$ non è cancellabile (diciamo a sinistra), allora esistono $b, c \in A$ con $b \neq c$ tali che $a \cdot b = a \cdot c$. Questo implica $a \cdot b - a \cdot c = 0_A$, e per distributività $a \cdot (b - c) = 0_A$. Poiché $b \neq c$, l'elemento $d = b - c$ è diverso da 0_A. Abbiamo trovato $d \neq 0_A$ tale che $a \cdot d = 0_A$. Quindi a è un divisore dello zero (a sinistra).
- **Esempio $(P(S), \Delta, \cap)$ (Pag 32):**
  - L'elemento neutro per Δ è $\emptyset$. L'elemento neutro per $\cap$ è S.
  - Cerchiamo $A \neq \emptyset$ che sia divisore dello zero. Cioè esiste $B \neq \emptyset$ tale che $A \cap B = \emptyset$.
  - Questo è possibile se A non è l'insieme S. Se $A \neq S$ e $A \neq \emptyset$, possiamo prendere $B = S \setminus A$. Poiché $A \neq S$, $B \neq \emptyset$. Poiché $A \neq \emptyset$, $B \neq S$. E $A \cap B = A \cap (S \setminus A) = \emptyset$.
  - Quindi, in $(P(S), \Delta, \cap)$, i divisori dello zero sono **tutti i sottoinsiemi propri non vuoti** di S. Gli unici elementi non divisori dello zero sono $\emptyset$ (per definizione) e S (l'unità moltiplicativa).

Divisore dello zero

Riepilogo Veloce Lezione 7

- Abbiamo rivisto la definizione di **Gruppo** e classificato esempi comuni.
- Abbiamo visto come calcolare l'**inversa di una matrice 2x2**.
- Abbiamo analizzato in dettaglio due **strutture algebriche** verificando associatività, commutatività, neutro e invertibili.
- Abbiamo introdotto la **struttura di Anello** $(A, +, \cdot)$ (gruppo abeliano per $+$, semigruppo per $\cdot$, distributività).
- Abbiamo visto esempi di anelli, inclusi l'**Anello Booleano** $(P(S), \Delta, \cap)$.
- Abbiamo definito **Anello Commutativo** e **Anello Unitario**.
- Abbiamo definito la **Caratteristica** di un anello unitario.
- Abbiamo definito gli **elementi cancellabili** e visto che invertibile $\implies$ cancellabile.
- Abbiamo definito i **divisori dello zero** in un anello e visto che $a \neq 0$ è divisore dello zero $\iff$ a non è cancellabile (rispetto a $\cdot$).

Prossimi Passi

- Assicurati di aver compreso la definizione di Anello e le sue proprietà.
- Rifletti sulla differenza tra cancellabilità e invertibilità.
- Il prossimo passo potrebbe essere l'introduzione di Domini di Integrità e Campi, che sono anelli con proprietà aggiuntive legate ai divisori dello zero e agli inversi moltiplicativi.

Lezione 8: Cancellabilità, Anelli, Domini, Campi, Spazi Vettoriali, Permutazioni

Data: 04/04/2025 (come da note)
Argomenti: Elementi cancellabili (recap, esempi), Anelli (recap, notazione multipli/potenze, proprietà dello zero), Divisori dello zero (recap, esempi), Domini di Integrità, Campi (Corpi), Spazi Vettoriali, Omomorfismi (introduzione), Gruppi di Permutazioni (S_n), Esercizi.

#tag/algebraic-structures #tag/rings #tag/integral-domains #tag/fields #tag/vector-spaces #tag/homomorphisms #tag/permutations #tag/symmetric-group #tag/cancellable-element #tag/zero-divisor #tag/algebra-avanzata

---

1. Elementi Cancellabili (Recap e Approfondimenti)

Ricordiamo le definizioni da Lezione 7:
Sia $(S, *)$ una struttura con operazione binaria. Un elemento $a \in S$ è:

- **Cancellabile a sinistra** se: $\forall b, c \in S, \quad a * b = a * c \implies b = c$.
- **Cancellabile a destra** se: $\forall b, c \in S, \quad b * a = c * a \implies b = c$.
- **Cancellabile** (bilatero) se è cancellabile sia a sinistra sia a destra.
- **Esempio $(\mathbb{R}^2, \cdot)$ con $(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, x_2 y_2)$ (Pag 1):**
  - L'elemento $(1, 0)$ è cancellabile?
  - Proviamo a destra: $(x_1, x_2) * (1, 0) = (x_1 \cdot 1, x_2 \cdot 0) = (x_1, 0)$.
  - Consideriamo $(2, 1) * (1, 0) = (2, 0)$.
  - Consideriamo $(2, 2) * (1, 0) = (2, 0)$.
  - Abbiamo $(2, 1) * (1, 0) = (2, 2) * (1, 0)$, ma $(2, 1) \neq (2, 2)$.
  - Quindi $(1, 0)$ **non è cancellabile a destra**. (E analogamente, $(0, 1)$ non è cancellabile a sinistra).
- **Esempio $(\mathbb{Z}, *)$ con $x * y = x|y|$ (Pag 2-5):**
  - **Associatività:**
    - $a * (b * c) = a * (b|c|) = a|b|c|| = a \cdot |b| \cdot |c|$ (poiché $|b| \geq 0$, $|b|c|| = |b||c|$).
    - $(a * b) * c = (a|b|) * c = (a|b|)|c| = a \cdot |b| \cdot |c|$.
    - **SÌ, è associativa.** Quindi $(\mathbb{Z}, *)$ è un semigruppo.
  - **Commutatività?**
    - $1 * (-1) = 1|-1| = 1 \cdot 1 = 1$.
    - $(-1) * 1 = (-1)|1| = (-1) \cdot 1 = -1$.
    - Poiché $1 \neq -1$. **NO, non è commutativa.**
  - **Elemento Neutro?**
    - Neutro a destra u: $a * u = a \implies a|u| = a$. Questo vale per ogni a se $|u| = 1$, cioè $u = 1$ o $u = -1$.
    - Neutro a sinistra w: $w * a = a \implies w|a| = a$. Se $a = 1$, $w|1| = 1 \implies w = 1$. Se $a = -1$, $w|-1| = -1 \implies w = -1$. Non esiste un w unico che funzioni per tutti gli a.
    - **Conclusione:** Esistono elementi neutri a destra (1 e -1), ma non esiste un elemento neutro (né a sinistra né bilatero). Non è un monoide.
  - **Elementi Cancellabili?**
    - A destra: $b * a = c * a \implies b|a| = c|a|$. Se $a \neq 0$, allora $|a| \neq 0$, possiamo dividere per $|a|$ (in $\mathbb{Q}$, ma dato che b, c sono interi, l'uguaglianza vale anche in $\mathbb{Z}$) ottenendo $b = c$. Quindi **ogni $a \neq 0$ è cancellabile a destra**.
    - A sinistra: $a * b = a * c \implies a|b| = a|c|$. Se $a \neq 0$, possiamo dividere per a, ottenendo $|b| = |c|$. Questo **non** implica $b = c$. Esempio: $a = 1$, $b = 1$, $c = -1$. $1 * 1 = 1|1| = 1$. $1 * (-1) = 1|-1| = 1$. Quindi $1 * 1 = 1 * (-1)$ ma $1 \neq -1$. **Solo $a = 0$ non è cancellabile a sinistra, ma gli $a \neq 0$ non garantiscono la cancellabilità.** Nessun elemento è cancellabile a sinistra (tranne forse casi banali da verificare).
- **Relazione Invertibile $\implies$ Cancellabile (Recap, Pag 5-6):**
  - In un monoide $(S, *, u)$, se a è invertibile (simmetrizzabile), allora a è cancellabile.
  - **Dimostrazione (Pag 6):** Se $a * b = a * c$, moltiplichiamo a sinistra per l'inverso a':
    $a' * (a * b) = a' * (a * c) \implies (a' * a) * b = (a' * a) * c \implies u * b = u * c \implies b = c$. (Analogo per destra).
  - **Viceversa NON vale (Pag 7):** In $(\mathbb{Z}, \cdot)$, ogni $a \neq 0$ è cancellabile, ma gli unici invertibili sono $1, -1$.

---

2. Anelli: Proprietà e Divisori dello Zero

- **Definizione Anello (Recap, Pag 7):** $(A, +, \cdot)$ è un anello se:
  1. $(A, +)$ è Gruppo Abeliano (associativa, commutativa, neutro 0_A, opposto $-a$).
  2. $(A, \cdot)$ è Semigruppo (associativa).
  3. Proprietà Distributive (sx e dx).
- **Notazione Multipli e Potenze (Pag 8):** In un anello A:
  - $n \cdot a = a + \cdots + a$ (n volte) per $n \in \mathbb{N}, n > 0$.
  - $0 \cdot a = 0_A$.
  - $(-n) \cdot a = -(n \cdot a)$.
  - Se l'anello è unitario (con unità 1_A):
    - $a^n = a \cdot \cdots \cdot a$ (n volte) per $n \in \mathbb{N}, n > 0$.
    - $a^0 = 1_A$ (per $a \neq 0_A$, a volte anche per $a = 0_A$ a seconda delle convenzioni).
- **Proprietà dello Zero (Pag 11):** In ogni anello A:

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

  - **Dimostrazione:** $a \cdot 0_A = a \cdot (0_A + 0_A) = a \cdot 0_A + a \cdot 0_A$ (distributività). Poiché $(A, +)$ è un gruppo, ogni elemento è cancellabile rispetto a $+$. Cancellando $a \cdot 0_A$ da entrambi i lati, otteniamo $0_A = a \cdot 0_A$. (Dimostrazione analoga per

$0_A \cdot a$).

- **Divisori dello Zero (Recap, Pag 9-10):**
  - $a \in A, a \neq 0_A$ è **divisore dello zero** se $\exists b \in A, b \neq 0_A$ tale che $a \cdot b = 0_A$ o $b \cdot a = 0_A$.
  - Equivalenza: $a \neq 0_A$ è divisore dello zero $\iff$ a non è cancellabile rispetto a $\cdot$.
  - **Esempio $(\mathbb{Z}^2, +, \cdot)$ con prodotto componente per componente (Pag 9):**
    - $0_{\mathbb{Z}^2} = (0,0)$.
    - Sia $a = (0,1) \neq (0,0)$. Sia $b = (1,0) \neq (0,0)$.
    - $a \cdot b = (0,1) \cdot (1,0) = (0 \cdot 1, 1 \cdot 0) = (0,0) = 0_{\mathbb{Z}^2}$.
    - Quindi $(0,1)$ e $(1,0)$ sono divisori dello zero.
  - **Esempio Matrici (Pag 12):** In $(M_2(\mathbb{R}), +, \cdot)$:
    - $$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq O$$
    ,
    $$B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq O$$
    .
    - $$A \cdot B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = O$$
    .
    - Quindi A e B sono divisori dello zero. (In generale, le matrici quadrate con determinante nullo sono divisori dello zero, tranne la matrice nulla stessa).

Anello (matematica) Divisore dello zero

---

3. Esercizi Proposti (come da note e suggerimento)

Esercizio 1 (Pag 13 - Verifica Associatività)

Verificare se vale o meno l'associatività per le seguenti operazioni su $\mathbb{Z}$:

1. $a * b = a + |b|$
2. $a \perp b = |a| + |b|$
3. $a \circ b = |a + b|$
4. $a \star b = -|a \cdot b|$

Esercizio 2 (Pag 14 - Divisori Zero in $\mathbb{Z}^{\mathbb{Z}}$)

Determinare gli eventuali divisori dello zero nell'anello $(\mathbb{Z}^{\mathbb{Z}}, +, \cdot)$, dove $+$ e $\cdot$ sono definiti puntualmente: $(f+g)(x) = f(x) + g(x)$ e $(f \cdot g)(x) = f(x)g(x)$. L'elemento neutro additivo è la funzione costante $cost_0(x) = 0$.
Suggerimento: Una funzione $f \neq cost_0$ è divisore dello zero se esiste $g \neq cost_0$ tale che $f \cdot g = cost_0$. Cosa significa $f(x)g(x) = 0$ per ogni x?

Esercizio 3 (Pag 15 - Stabilità Funzioni Costanti)

Sia $T = \{f \in \mathbb{Z}^{\mathbb{Z}} \mid f \text{ è costante}\}$. Verificare che T è stabile (chiuso) rispetto a $+$ e $\cdot$ in $\mathbb{Z}^{\mathbb{Z}}$. È un sottoanello?

Esercizio 4 (Pag 15 - Studio Struttura $\mathbb{Z}$)

Studiare la struttura $(\mathbb{Z}, *)$ dove $a * b = a + b + 4ab$.

- Verificare associatività e commutatività.
- Cercare l'eventuale elemento neutro.
- Determinare gli eventuali elementi invertibili (simmetrici).
- È un monoide? È un gruppo?

Esercizio 5 (Pag 16-18 - Studio Struttura $\mathbb{Q}^2$)

Studiare la struttura $(\mathbb{Q}^2, *)$ dove $(x_1, x_2) * (y_1, y_2) = (x_1 y_1 + x_2 y_2, 3 x_2 y_2)$.

- Verificare se vale la proprietà associativa.
- Verificare se è commutativa.
- Cercare l'eventuale elemento neutro.
- (Se è un monoide) Determinare gli eventuali elementi invertibili.
- È un semigruppo? Monoide? Gruppo?
- Considerare la stabilità del sottoinsieme $T = \mathbb{Q} \times \{0\}$.

Esercizio 6 (Pag 19-20 - Studio Struttura $\mathbb{Q}^3$ e Anello)

Studiare la struttura $(\mathbb{Q}^3, *)$ dove $(x_1, x_2, x_3) * (y_1, y_2, y_3) = (x_1y_1, x_2y_1 + x_3y_2, x_3y_3)$.

- Verificare se è associativa.
- Verificare se è commutativa.
- Cercare l'eventuale elemento neutro.
- (Se è un monoide) Determinare gli eventuali elementi invertibili.
- È un semigruppo? Monoide? Gruppo?

Verifica Anello (Suggerimento Leonardo): Sia $+$ la somma componente per componente in $\mathbb{Q}^3$. Verificare se $(\mathbb{Q}^3, +, *)$ è un anello.

- Verificare che $(\mathbb{Q}^3, +)$ sia gruppo abeliano (è standard).
- Verificare che $(\mathbb{Q}^3, *)$ sia semigruppo (associatività verificata sopra).
- Verificare le **proprietà distributive**:
  - $X * (Y + Z) = (X * Y) + (X * Z)$?
  - $(Y + Z) * X = (Y * X) + (Z * X)$?
    (dove $X = (x_1, x_2, x_3)$, $Y = (y_1, y_2, y_3)$, $Z = (z_1, z_2, z_3)$).

Esercizio 7 (Pag 21 - Stabilità Sottoinsiemi $\mathbb{Z}$)

Nella struttura $(\mathbb{Z}, *)$ con $a * b = a|b|$, verificare quali dei seguenti sottoinsiemi sono stabili:

- $P = \{2n \mid n \in \mathbb{Z}\}$ (Pari)
- $D = \{2n + 1 \mid n \in \mathbb{Z}\}$ (Dispari)
- $S = \{n \in \mathbb{Z} \mid n < 0\}$ (Negativi)
- $L = \{n \in \mathbb{Z} \mid n > 0\}$ (Positivi)

Esercizio 8 (Pag 22 - Studio Strutture $\mathbb{Z}$)

Studiare le strutture $(\mathbb{Z}, \perp)$ con $a \perp b = 2ab - a - b$ e $(\mathbb{Z}, \circ)$ con $a \circ b = a + b + 2ab$.

- Verificare associatività, commutatività.
- Cercare elemento neutro.
- Determinare elementi invertibili.

---

4. Omomorfismi tra Strutture Algebriche

Una funzione che "preserva la struttura".

- **Definizione (Pag 22):** Siano $(S, *)$ e $(T, \perp)$ due strutture algebriche con operazioni binarie. Una funzione $f : S \to T$ si dice **omomorfismo** di $(S, *)$ in $(T, \perp)$ se:

$$\forall a, b \in S, \quad f(a * b) = f(a) \perp f(b)$$

  - **Spiegazione:** Applicare l'operazione in S e poi mappare il risultato in T tramite f dà lo stesso risultato che mappare prima a e b in T tramite f e poi applicare l'operazione di T.
- **Esempi (Pag 23-26):**
  - $f : (\mathbb{N}, +) \to (\mathbb{N}, \cdot)$ con $f(a) = 2^a$.
    - Verifichiamo $f(a + b) = f(a) \cdot f(b)$.
    - $f(a + b) = 2^{a+b}$.
    - $f(a) \cdot f(b) = 2^a \cdot 2^b = 2^{a+b}$.
    - **SÌ, è un omomorfismo.**
  - $f : (\mathbb{N}, +) \to (\mathbb{N}, +)$ con $f(a) = 2^a$.
    - Verifichiamo $f(a + b) = f(a) + f(b)$.
    - $f(a + b) = 2^{a+b}$.
    - $f(a) + f(b) = 2^a + 2^b$.
    - $2^{a+b} \neq 2^a + 2^b$ in generale (es. $a = 1, b = 1 \implies 2^2 = 4 \neq 2^1 + 2^1 = 4$. Funziona solo in questo caso? No. $a = 1, b = 2 \implies 2^3 = 8 \neq 2^1 + 2^2 = 2 + 4 = 6$).
    - **NO, non è un omomorfismo.**
  - $f : (\mathbb{Q}^2, \cdot) \to (M_{2,2}(\mathbb{Q}), \cdot)$ con $f(x_1, x_2) = \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}$.
    - Operazione in $\mathbb{Q}^2$: $(x_1, x_2) \cdot (y_1, y_2) = (x_1y_1, x_2y_2)$.
    - Operazione in $M_{2,2}(\mathbb{Q})$: Prodotto righe per colonne.
    - Verifichiamo $f((x_1, x_2) \cdot (y_1, y_2)) = f(x_1, x_2) \cdot f(y_1, y_2)$.
    - $f((x_1y_1, x_2y_2)) = \begin{pmatrix} x_1y_1 & 0 \\ 0 & x_2y_2 \end{pmatrix}$.

- $f(x_1, x_2) \cdot f(y_1, y_2) = \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix} \cdot \begin{pmatrix} y_1 & 0 \\ 0 & y_2 \end{pmatrix} = \begin{pmatrix} (x_1y_1 + 0) & (0+0) \\ (0+0) & (0 + x_2y_2) \end{pmatrix} = \begin{pmatrix} x_1y_1 & 0 \\ 0 & x_2y_2 \end{pmatrix}$.
- **SÌ, è un omomorfismo.**

- $g : (\mathbb{Q}^2, \cdot) \to (M_{2,2}(\mathbb{Q}), \cdot)$ con $g(x_1, x_2) = \begin{pmatrix} x_1 & x_2 \\ 0 & 0 \end{pmatrix}$.
  - Verifichiamo $g((x_1, x_2) \cdot (y_1, y_2)) = g(x_1, x_2) \cdot g(y_1, y_2)$.
  - $g((x_1y_1, x_2y_2)) = \begin{pmatrix} x_1y_1 & x_2y_2 \\ 0 & 0 \end{pmatrix}$.
  - $g(x_1, x_2) \cdot g(y_1, y_2) = \begin{pmatrix} x_1 & x_2 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} y_1 & y_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} (x_1y_1 + 0) & (x_1y_2 + 0) \\ (0+0) & (0+0) \end{pmatrix} = \begin{pmatrix} x_1y_1 & x_1y_2 \\ 0 & 0 \end{pmatrix}$.
  - Le matrici risultato non sono uguali in generale (se $x_2y_2 \neq x_1y_2$).
  - **NO, non è un omomorfismo.**
- $g : (\mathbb{Q}^2, +) \to (M_{2,2}(\mathbb{Q}), +)$ con $g(x_1, x_2) = \begin{pmatrix} x_1 & x_2 \\ 0 & 0 \end{pmatrix}$.
  - Verifichiamo $g((x_1, x_2) + (y_1, y_2)) = g(x_1, x_2) + g(y_1, y_2)$.
  - $g((x_1 + y_1, x_2 + y_2)) = \begin{pmatrix} x_1 + y_1 & x_2 + y_2 \\ 0 & 0 \end{pmatrix}$.
  - $g(x_1, x_2) + g(y_1, y_2) = \begin{pmatrix} x_1 & x_2 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} y_1 & y_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x_1 + y_1 & x_2 + y_2 \\ 0 & 0 \end{pmatrix}$.
  - **SÌ, è un omomorfismo** (tra strutture additive).

Omomorfismo

---

5. Domini di Integrità e Campi

Anelli con proprietà aggiuntive desiderabili.

- **Dominio di Integrità (Pag 27):** Un anello $(A, +, \cdot)$ è un Dominio di Integrità se soddisfa:
  1. A è **commutativo**.
  2. A è **unitario** con $1_A \neq 0_A$.
  3. A è **privo di divisori dello zero** (diversi da 0_A).
     - Equivalente a: $\forall a, b \in A, a \cdot b = 0_A \implies (a = 0_A \vee b = 0_A)$.
     - Equivalente a: Ogni elemento $a \neq 0_A$ è cancellabile rispetto a $\cdot$.
- **Esempi:** $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sono domini di integrità.
- **Controesempio $(P(S), \Delta, \cap)$ (Pag 28):**
  - È commutativo e unitario (unità S).
  - Ma se $|S| \geq 2$, ha divisori dello zero (tutti i sottoinsiemi propri non vuoti).
  - Quindi **non** è un dominio di integrità (a meno che $|S| = 1$).

Dominio di integrità

- **Campo (Corpo Commutativo) (Pag 29):** Un anello $(K, +, \cdot)$ è un Campo (in italiano spesso si usa "Campo" per indicare un corpo commutativo) se:
  1. K è un **anello commutativo unitario** con $1_K \neq 0_K$.
  2. **Ogni elemento non nullo ha un inverso moltiplicativo:** $(K^*, \cdot)$ è un gruppo abeliano, dove $K^* = K \setminus \{0_K\}$.
- **Definizione alternativa (Corpo):** Un anello $(K, +, \cdot)$ è un Corpo se $(K^*, \cdot)$ è un gruppo. Se $\cdot$ è anche commutativa, è un Campo.
- **Relazione:** Un Campo è sempre un Dominio di Integrità. (Se $a \cdot b = 0_K$ e $a \neq 0_K$, allora a ha inverso a^{-1}. Moltiplicando per a^{-1} si ottiene $a^{-1}ab = a^{-1}0_K \implies 1_K b = 0_K \implies b = 0_K$. Quindi non ci sono divisori dello zero).
- **Esempi di Campi:** $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$.
- **Controesempio:** $(\mathbb{Z}, +, \cdot)$ è un dominio di integrità ma non un campo (mancano gli inversi moltiplicativi per elementi diversi da 1, -1).

Campo (matematica) Corpo (matematica)

- **Teorema di Wedderburn (Pag 33):** Ogni corpo finito è un campo (cioè il prodotto è automaticamente commutativo).

---

6. Spazi Vettoriali (Cenno)

Struttura fondamentale dell'algebra lineare.

- **Definizione (Pag 29-30):** Sia K un campo. Un **K-spazio vettoriale** (o spazio vettoriale su K) è una struttura $(V, +, \cdot_{ext})$ dove:

1. $(V, +)$ è un **Gruppo Abeliano** (gli elementi di V sono chiamati vettori, $+$ è la somma vettoriale, 0_V è il vettore nullo).
2. $\cdot_{ext} : K \times V \to V$ è un'**operazione esterna** (prodotto per scalare) che associa a uno scalare $\alpha \in K$ e un vettore $v \in V$ un vettore $\alpha \cdot_{ext} v \in V$.
3. Valgono le seguenti **proprietà di compatibilità** $(\forall \alpha, \beta \in K, \forall u, v \in V)$:
   - i) $\alpha \cdot_{ext} (\beta \cdot_{ext} v) = (\alpha \cdot_K \beta) \cdot_{ext} v$ (Associatività mista)
   - ii) $(\alpha +_K \beta) \cdot_{ext} v = (\alpha \cdot_{ext} v) +_V (\beta \cdot_{ext} v)$ (Distributività rispetto somma scalari)
   - iii) $\alpha \cdot_{ext} (u +_V v) = (\alpha \cdot_{ext} u) +_V (\alpha \cdot_{ext} v)$ (Distributività rispetto somma vettori)
   - iv) $1_K \cdot_{ext} v = v$ (Elemento neutro scalare)

- **Esempi (Pag 31):**
  - $K^n = \{(x_1, \dots, x_n) \mid x_i \in K\}$ con somma vettoriale e prodotto per scalare componente per componente.
  - $M_{m,n}(K)$ (matrici $m \times n$ a coefficienti in K) con somma matriciale e prodotto per scalare.

Spazio vettoriale

---

7. Gruppi di Permutazioni (S_n)

Un esempio importante di gruppo non abeliano.

- Sia S un insieme finito con $|S| = n$. Spesso si prende $S = \{1, 2, \dots, n\}$.
- $B(S) = \{f : S \to S \mid f \text{ è biettiva}\}$ è l'insieme delle **permutazioni** di S.
- $(B(S), \circ)$ è un gruppo, chiamato **Gruppo Simmetrico** su n elementi, denotato S_n.
- La cardinalità di S_n è $|S_n| = n! = n \cdot (n-1) \cdot \dots \cdot 1$.
- **Notazione Ciclica (Pag 34-36):**
  - Una permutazione può essere rappresentata elencando come mappa gli elementi:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}$$

  - Un **ciclo** $(c_1 c_2 \dots c_k)$ rappresenta la permutazione σ tale che $\sigma(c_1) = c_2, \sigma(c_2) = c_3, \dots, \sigma(c_{k-1}) = c_k, \sigma(c_k) = c_1$, e $\sigma(x) = x$ per gli elementi x non nel ciclo.
  - **Teorema (Decomposizione in Cicli Disgiunti, Pag 35):** Ogni permutazione $\sigma \in S_n$ si può scrivere in modo unico (a meno dell'ordine dei cicli) come prodotto (composizione) di cicli disgiunti.
  - **Esempio:**

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 7 & 1 & 5 & 6 & 3 & 9 & 8 \end{pmatrix}$$

    - $1 \to 2 \to 4 \to 1$. Ciclo: (124).
    - $3 \to 7 \to 3$. Ciclo: (37).
    - $5 \to 5$. (Ciclo di lunghezza 1, spesso omesso).
    - $6 \to 6$. (Ciclo di lunghezza 1, spesso omesso).
    - $8 \to 9 \to 8$. Ciclo: (89).
    - Decomposizione: $\sigma = (124)(37)(89)$.
  - **Inversa di un Ciclo (Pag 36):** L'inversa del ciclo $(c_1 c_2 \dots c_k)$ si ottiene leggendo gli elementi al contrario: $(c_1 c_k c_{k-1} \dots c_2)$.
    - Esempio: $(1743)^{-1} = (1347)$.
  - **Inversa di un Prodotto di Cicli Disgiunti:** L'inversa del prodotto è il prodotto delle inverse (nello stesso ordine, perché cicli disgiunti commutano).
    - Esempio:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 1 & 3 & 2 & 6 & 4 \end{pmatrix} = (1743)(25)$$

    .
    - $\sigma^{-1} = (1743)^{-1}(25)^{-1} = (1347)(25)$.

Gruppo simmetrico Permutazione Notazione ciclica

Riepilogo Veloce Lezione 8

- Abbiamo rivisto la **cancellabilità** e la sua relazione (non equivalenza) con l'invertibilità.
- Abbiamo definito la notazione per **multipli additivi e potenze moltiplicative** in anelli.
- Abbiamo dimostrato che $a \cdot 0_A = 0_A$.

- Abbiamo rivisto i **divisori dello zero** e la loro equivalenza con la non-cancellabilità.
- Abbiamo introdotto i **Domini di Integrità** (anelli commutativi unitari privi di divisori dello zero).
- Abbiamo introdotto i **Campi** (anelli commutativi unitari dove ogni elemento non nullo è invertibile moltiplicativamente).
- Abbiamo definito gli **Spazi Vettoriali** su un campo K.
- Abbiamo definito gli **Omomorfismi** tra strutture algebriche.
- Abbiamo introdotto il **Gruppo Simmetrico** S_n (permutazioni), la notazione ciclica, la decomposizione in cicli disgiunti e il calcolo dell'inversa.
- Sono stati proposti numerosi **esercizi** per praticare questi concetti.

Prossimi Passi

- Prova a svolgere gli esercizi proposti, in particolare quelli sullo studio delle strutture e sulla verifica delle proprietà (anello, associatività, commutatività, neutro, inversi, divisori dello zero).
- Familiarizza con la notazione ciclica delle permutazioni.
- Il prossimo passo potrebbe essere approfondire le proprietà dei gruppi (sottogruppi, teorema di Lagrange) o degli anelli (ideali, anelli quoziente).

Lezione 9: Tavole di Cayley, Divisibilità in Anelli, Relazioni Binarie

Data: 10/04/2025 (come da note)
Argomenti: Tavole di Cayley, Cancellabilità (recap), Elementi Nilpotenti, Divisibilità in Anelli, Elementi Associati, MCD/MCM, Numeri Primi in Z, Relazioni Binarie (definizione, proprietà).

#tag/algebraic-structures #tag/cayley-tables #tag/cancellable-element #tag/zero-divisor #tag/nilpotent #tag/divisibility #tag/rings #tag/relations #tag/algebra-avanzata

---

1. Tavole di Cayley (Tabelle Moltiplicative)

- **Definizione (Pag 2):** Per una struttura $(S, *)$ con un insieme finito $S = \{s_1, s_2, \ldots, s_n\}$, la **Tavola di Cayley** è una tabella quadrata dove l'elemento alla riga i e colonna j è il risultato dell'operazione $s_i * s_j$.
	s_1	s_2	...	s_j	...	s_n
s_1	...	...	...	...	...	...
s_2	...	...	...	...	...	...
...	...	...	...	...	...	...
s_i	...	...	...	$s_i * s_j$	...	...
...	...	...	...	...	...	...
s_n	...	...	...	...	...	...
- **Utilità:**
  - Visualizza l'intera struttura dell'operazione.
  - **Commutatività:** L'operazione è commutativa se e solo se la tavola è **simmetrica** rispetto alla diagonale principale (cioè $s_i * s_j = s_j * s_i$).
  - **Elemento Neutro:** Se esiste, ci sarà una riga e una colonna identiche agli indici della tabella.
  - **Inversi:** Si possono cercare gli inversi trovando l'elemento neutro nella tabella.
  - **Cancellabilità:** Un elemento a è cancellabile a sinistra se nella riga corrispondente ad a non ci sono ripetizioni. È cancellabile a destra se nella colonna corrispondente ad a non ci sono ripetizioni.
- **Esempio $(P(S), \cap)$ con $S = \{a, b\}$ (Pag 3):**
  - $P(S) = \{\emptyset, A = \{a\}, B = \{b\}, S = \{a, b\}\}$.
  - **Tavola di Cayley per $\cap$:**

∩	∅	A	B	S
∅	∅	∅	∅	∅
A	∅	A	∅	A
B	∅	∅	B	B
S	∅	A	B	S

  - **Osservazioni:**
    - Commutativa (tabella simmetrica).
    - Elemento Neutro: S (riga/colonna di S sono uguali agli indici).
    - Cancellabilità:
      - Riga ∅: tutti ∅ (non cancellabile a sx).
      - Riga A: ∅, A, ∅, A (ripetizioni, non cancellabile a sx).

        - Riga B: $\emptyset$, $\emptyset$, B, B (ripetizioni, non cancellabile a sx).
        - Riga S: $\emptyset$, A, B, S (nessuna ripetizione, S è cancellabile a sx).
        - Per simmetria, solo S è cancellabile (anche a dx).
    - Divisori dello zero: $A \cap B = \emptyset$. A, B sono divisori dello zero.
- **Esempio $(P(S), \Delta)$ con $S = \{a, b\}$ (Pag 4):**
    - **Tavola di Cayley per Δ:** (Ricorda $X \Delta Y = (X \cup Y) \setminus (X \cap Y)$)

Δ	$\emptyset$	A	B	S
$\emptyset$	$\emptyset$	A	B	S
A	A	$\emptyset$	S	B
B	B	S	$\emptyset$	A
S	S	B	A	$\emptyset$

    - **Osservazioni:**
        - Commutativa (tabella simmetrica).
        - Elemento Neutro: $\emptyset$.
        - Inversi: Ogni elemento è inverso di se stesso ($X \Delta X = \emptyset$).
        - Cancellabilità: Ogni riga/colonna è una permutazione degli elementi $\{\emptyset, A, B, S\}$. Non ci sono ripetizioni. **Tutti gli elementi sono cancellabili**.
        - È un **Gruppo Abeliano**.

Tavola di Cayley

---

2. Cancellabilità e Strutture Finite

- **Proprietà (Pag 5):** In una struttura finita $(S, *)$, un elemento $a \in S$ è **cancellabile a destra** se e solo se la funzione "moltiplicazione a destra per a", $f_a : S \to S$ definita da $f_a(x) = x * a$, è **iniettiva**.
    - **Dimostrazione:** a è cancellabile a destra $\iff (\forall x, y \in S, x * a = y * a \implies x = y) \iff (\forall x, y \in S, f_a(x) = f_a(y) \implies x = y) \iff f_a$ è iniettiva.
- **Corollario (Pag 5):** In una struttura finita $(S, *)$, se a è cancellabile (a dx o sx), allora la funzione $f_a(x) = x * a$ (o $g_a(x) = a * x$) è **biettiva**.
    - **Dimostrazione:** Una funzione $f : S \to S$ da un insieme finito a se stesso è iniettiva se e solo se è suriettiva, se e solo se è biettiva. Poiché f_a è iniettiva (se a è cancellabile), allora è anche biettiva.

---

3. Elementi Nilpotenti e Divisori

Sia $(A, +, \cdot)$ un anello.

- **Elemento Nilpotente (Pag 7):** Un elemento $a \in A$ si dice **nilpotente** se esiste un intero $n \geq 1$ tale che $a^n = 0_A$ (dove $a^n = a \cdot a \cdot \dots \cdot a$, n volte).
    - L'elemento 0_A è sempre nilpotente ($0_A^1 = 0_A$).
    - **Esempio $(M_2(\mathbb{Q}), +, \cdot)$ (Pag 8):** La matrice $N = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ è nilpotente?
        - $N^1 = N \neq O$.
        - $N^2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = O$.
        - Sì, N è nilpotente (con $n = 2$).
    - **Osservazione (Pag 8):** Se $a \neq 0_A$ è nilpotente (cioè $a^n = 0_A$ per $n \geq 1$), allora a è un **divisore dello zero**.
        - **Dimostrazione:** Sia n il più piccolo intero ≥ 1 tale che $a^n = 0_A$. Se $n = 1$, $a = 0_A$, caso escluso. Se $n > 1$, allora $a^{n-1} \neq 0_A$. Ma $a \cdot a^{n-1} = a^n = 0_A$. Abbiamo trovato $b = a^{n-1} \neq 0_A$ tale che $a \cdot b = 0_A$. Quindi a è divisore dello zero.
    - **Controesempio $(P(S), \Delta, \cap)$ (Pag 8):** L'elemento neutro additivo è $\emptyset$. $A^n = A \cap \dots \cap A = A$. Se $A \neq \emptyset$, $A^n = A \neq \emptyset$. Gli unici elementi nilpotenti sono $\emptyset$. Ma abbiamo visto che ci sono divisori dello zero (sottoinsiemi propri non vuoti).

Elemento Nilpotente

- **Relazione di Divisibilità (Pag 9, 13):** In un anello $(A, +, \cdot)$, diciamo che b **divide** a (o a è **multiplo** di b), e scriviamo $b \mid a$, se esiste un elemento $c \in A$ tale che $a = b \cdot c$.
    - L'insieme dei **divisori** di a è $div(a) = \{b \in A \mid b \mid a\}$.
    - L'insieme dei **multipli** di b è $mult(b) = \{a \in A \mid b \mid a\} = \{b \cdot c \mid c \in A\}$.
    - **Esempio $(\mathbb{Z}, +, \cdot)$ (Pag 9):** $div(4) = \{1, -1, 2, -2, 4, -4\}$.

- **Esempio $(P(S), \Delta, \cap)$ (Pag 9):** $A \mid B \iff B = A \cap C$ per qualche C. Questo significa $B \subseteq A$. Quindi $div(A) = \{X \in P(S) \mid A \subseteq X\}$.
  - $div(A) = \{S, A\}$? No, $div(A) = \{X | A \subseteq X\}$. Se $S = \{a, b\}$, $A = \{a\}$, $div(A) = \{\{a\}, \{a, b\} = S\}$.
  - $div(B) = \{B, S\}$. $div(S) = \{S\}$.
- **Divisori dell'Unità (Pag 10):** In un anello unitario $(A, +, \cdot, 1_A)$:
  - $div(1_A) = \{b \in A \mid \exists c : 1_A = b \cdot c\}$.
  - Questi sono esattamente gli elementi che hanno un inverso destro. Se l'anello è commutativo, sono gli elementi invertibili.
  - $div(1_A) = U(A)$ (il gruppo degli elementi invertibili).
  - **Esempio $(\mathbb{Z}, +, \cdot)$:** $div(1) = \{1, -1\} = U(\mathbb{Z})$.
- **Elementi Associati (Pag 11):** In un anello unitario commutativo A, due elementi $x, y \in A$ si dicono **associati** (notazione $x \sim y$) se esiste un elemento invertibile $u \in U(A)$ tale che $x = u \cdot y$.
  - Questa è una relazione di equivalenza.
  - Se $x = u \cdot y$, allora $y = u^{-1} \cdot x$, quindi anche $y \sim x$.
  - Se $x \sim y$, allora $div(x) = div(y)$.
  - **Esempio $(\mathbb{Z}, +, \cdot)$:** $U(\mathbb{Z}) = \{1, -1\}$. $x \sim y \iff x = 1 \cdot y$ o $x = -1 \cdot y$. Cioè $x = \pm y$. Gli elementi associati a a sono $\{a, -a\}$.
  - **Divisori Banali (Pag 12):** I divisori banali di a sono gli elementi associati ad a e gli elementi associati a 1_A (cioè gli invertibili $U(A)$).
  - **Divisori Propri (Pag 13):** Un divisore b di a è **proprio** se b non è associato ad a e b non è invertibile (non è associato a 1_A).
  - **Esempio $(\mathbb{Z}, +, \cdot)$:** $div(4) = \{1, -1, 2, -2, 4, -4\}$.
    - Associati a 4: $\{4, -4\}$.
    - Associati a 1 (invertibili): $\{1, -1\}$.
    - Divisori banali di 4: $\{1, -1, 4, -4\}$.
    - Divisori propri di 4: $\{2, -2\}$.

Divisibilità Elementi Associati

- **Proprietà Divisibilità (Pag 14):** Se $a \mid x$ e $a \mid y$, allora $\forall h, k \in A$, $a \mid (h \cdot x + k \cdot y)$.
  - **Dimostrazione:** $x = x_1 a$, $y = y_1 a$. $hx + ky = h(x_1 a) + k(y_1 a) = (hx_1 + ky_1)a$. Poiché $(hx_1 + ky_1) \in A$, abbiamo $a \mid (hx + ky)$.

---

4. Aritmetica in $\mathbb{Z}$ (Pag 15-19)

L'anello $(\mathbb{Z}, +, \cdot)$ è un **Dominio di Integrità** (commutativo, unitario, privo di divisori dello zero). $U(\mathbb{Z}) = \{1, -1\}$.

- **Divisori Banali di $a \in \mathbb{Z}$:** $\{1, -1, a, -a\}$.
- **Elementi Associati a $a \in \mathbb{Z}$:** $\{a, -a\}$. $(a \sim b \iff a = \pm b)$.
- **Proprietà:** $a \mid b$ e $b \mid a \iff a \sim b$ (cioè $a = \pm b$).
  - **Dimostrazione:** $b = b_1 a$, $a = a_1 b$. Sostituendo: $a = a_1(b_1 a) = (a_1 b_1)a$. Se $a \neq 0$, per cancellatività $1 = a_1 b_1$. Poiché siamo in $\mathbb{Z}$, gli unici elementi il cui prodotto è 1 sono $1 \cdot 1 = 1$ e $(-1)(-1) = 1$. Quindi $a_1, b_1 \in \{1, -1\} = U(\mathbb{Z})$. Perciò $a \sim b$. Se $a = 0$, allora $b = b_1 0 = 0$, quindi $a = b = 0$ e $a \sim b$.
- **Massimo Comun Divisore (MCD) (Pag 17):** $e \in \mathbb{Z}$ è un MCD di $a, b \in \mathbb{Z}$ se:
  1. $e \mid a$ e $e \mid b$ (è un divisore comune).
  2. $\forall x \in \mathbb{Z}$: se $x \mid a$ e $x \mid b$, allora $x \mid e$ (è il più grande tra i divisori comuni, nel senso della divisibilità).
  - Se e è un MCD, allora anche $-e$ (l'associato) è un MCD. L'insieme degli MCD di (a, b) è $\{e, -e\}$.
  - **Convenzione:** "il" MCD, denotato $\text{MCD}(a, b)$ o $\gcd(a, b)$, si intende quello **positivo**.
  - Esempio: $\text{MCD}(4, 6) = 2$. L'insieme degli MCD è $\{2, -2\}$.
- **Minimo Comune Multiplo (mcm) (Pag 18):** $m \in \mathbb{Z}$ è un mcm di $a, b \in \mathbb{Z}$ se:
  1. $a \mid m$ e $b \mid m$ (è un multiplo comune).
  2. $\forall x \in \mathbb{Z}$: se $a \mid x$ e $b \mid x$, allora $m \mid x$ (è il più piccolo tra i multipli comuni, nel senso della divisibilità).
  - Se m è un mcm, allora anche $-m$ è un mcm. L'insieme degli mcm di (a, b) è $\{m, -m\}$.
  - **Convenzione:** "il" mcm, denotato $\text{mcm}(a, b)$ o $\text{lcm}(a, b)$, si intende quello **positivo**.
  - Esempio: $\text{mcm}(4, 6) = 12$. L'insieme degli mcm è $\{12, -12\}$.
- **Numero Primo (Pag 19):** Un intero $p \in \mathbb{Z}$ è **primo** se:
  1. $p \notin U(\mathbb{Z})$ non è un elemento invertibile (cioè $p \neq 1, p \neq -1$).
  2. I suoi unici divisori sono quelli banali: $div(p) = \{1, -1, p, -p\}$.
  - **Proprietà Fondamentale (Lemma di Euclide):** Se p è primo e $p \mid (a \cdot b)$, allora $p \mid a$ oppure $p \mid b$.
  - Esempio: 6 non è primo. $6 \mid (3 \cdot 4) = 12$, ma $6 \nmid 3$ e $6 \nmid 4$.

5. Relazioni Binarie: Proprietà Fondamentali

Torniamo alle relazioni, ma ora definite su un singolo insieme A.

- **Relazione Binaria su A (Pag 20):** Una relazione $\mathcal{R}$ su A è un sottoinsieme del prodotto cartesiano $A \times A$. Formalmente $\mathcal{R} = (A \times A, G)$ dove $G \subseteq A \times A$ è il grafo. Scriviamo $a\mathcal{R}b \iff (a,b) \in G$.
- **Esempi Banali (Pag 21):**
  1. **Relazione Totale:** $G = A \times A$. $\forall a, b \in A, a\mathcal{R}b$.
  2. **Relazione di Identità (o Uguaglianza):** $G = Diag(A) = \{(a,a) \mid a \in A\}$. $a\mathcal{R}b \iff a = b$.
- **Proprietà delle Relazioni Binarie (Pag 22, 25):** Sia $\mathcal{R}$ una relazione su A.
  1. **Riflessiva:** $\forall x \in A, x\mathcal{R}x$. (Ogni elemento è in relazione con se stesso).
     - Equivalente a: $Diag(A) \subseteq G$.
  2. **Antiriflessiva (o Irriflessiva):** $\forall x \in A, \neg(x\mathcal{R}x)$. (Nessun elemento è in relazione con se stesso).
     - Equivalente a: $Diag(A) \cap G = \emptyset$.
  3. **Simmetrica:** $\forall x, y \in A, x\mathcal{R}y \implies y\mathcal{R}x$. (Se x è in relazione con y, allora y è in relazione con x).
  4. **Asimmetrica:** $\forall x, y \in A, x\mathcal{R}y \implies \neg(y\mathcal{R}x)$. (Se x è in relazione con y, allora y NON può essere in relazione con x).
     - Nota: Asimmetrica $\implies$ Antiriflessiva.
  5. **Antisimmetrica:** $\forall x, y \in A, (x\mathcal{R}y \land y\mathcal{R}x) \implies x = y$. (Gli unici "cicli di lunghezza 2" sono gli anelli su un elemento, cioè $x\mathcal{R}x$).
  6. **Transitiva:** $\forall x, y, z \in A, (x\mathcal{R}y \land y\mathcal{R}z) \implies x\mathcal{R}z$. (Se x è in relazione con y, e y con z, allora x è in relazione con z).
- **Esempi (Pag 23-28):**
  - Relazione Totale su $S = \{a, b\}$: $G = \{(a,a), (a,b), (b,a), (b,b)\}$. È Riflessiva, Simmetrica, Transitiva. Non Antiriflessiva, Non Asimmetrica, Non Antisimmetrica.
  - Relazione Identità su $S = \{a, b\}$: $G = \{(a,a), (b,b)\}$. È Riflessiva, Simmetrica, Antisimmetrica, Transitiva. Non Antiriflessiva, Non Asimmetrica.
  - $(\mathbb{Z}, \mathcal{R}_{||})$ con $a\mathcal{R}_{||}b \iff |a| = |b|$.
    - Riflessiva: $|a| = |a|$. Sì.
    - Simmetrica: $|a| = |b| \implies |b| = |a|$. Sì.
    - Transitiva: $|a| = |b| \land |b| = |c| \implies |a| = |c|$. Sì.
    - (È una relazione di equivalenza). Non Antiriflessiva, Non Asimmetrica, Non Antisimmetrica (es. $2\mathcal{R}_{||} - 2$ e $-2\mathcal{R}_{||}2$ ma $2 \neq -2$).
  - $(\mathbb{Z}, \mathcal{R}_{<})$ con $a\mathcal{R}_{<}b \iff |a| < |b|$.
    - Antiriflessiva: $|a| < |a|$ è falso. Sì.
    - Asimmetrica: $|a| < |b| \implies \neg(|b| < |a|)$. Sì.
    - Transitiva: $|a| < |b| \land |b| < |c| \implies |a| < |c|$. Sì.
    - (È una relazione d'ordine?). Non Riflessiva, Non Simmetrica, Non Antisimmetrica (non ci sono coppie $x\mathcal{R}y$ e $y\mathcal{R}x$).
  - $(\mathbb{Z}, \mathcal{R}^*)$ con $a\mathcal{R}^*b \iff a = |b|$.
    - Riflessiva? $a = |a|$ solo se $a \geq 0$. No.
    - Antiriflessiva? $1 = |1|$. No.
    - Simmetrica? $1\mathcal{R}^* - 1$ (perché $1 = |-1|$). Ma $-1\mathcal{R}^*1$ è falso (perché $-1 \neq |1|$). No.
    - Asimmetrica? No (vedi sopra).
    - Antisimmetrica? $a\mathcal{R}^*b \land b\mathcal{R}^*a \implies a = |b| \land b = |a|$. Se $a, b \geq 0$, $a = b$. Se $a = 1, b = -1$, $1 = |-1|$ e $-1 = |1|$ è falso. Se $a = -1, b = 1$, $-1 = |1|$ è falso. Sembra di sì? Verifichiamo: se $a = |b|$ e $b = |a|$, allora $|a| = ||a|| = |a|$, $|b| = ||b|| = |b|$. Se $a < 0$, $b = |a| > 0$. $a = |b| = b$. Contraddizione. Quindi a, b devono essere ≥ 0. In tal caso $a = b$ e $b = a$. Quindi $a = b$. **Sì, è antisimmetrica.**
    - Transitiva? $a\mathcal{R}^*b \land b\mathcal{R}^*c \implies a = |b| \land b = |c|$. Allora $a = ||c|| = |c|$. Quindi $a\mathcal{R}^*c$? No. Esempio: $a = 1, b = -1, c = 1$. $1\mathcal{R}^* - 1$ ($1 = |-1|$). $-1\mathcal{R}^*1$ (falso). Non si può applicare la transitività. Proviamo $a = 1, b = 1, c = -1$. $1\mathcal{R}^*1$ ($1 = |1|$). $1\mathcal{R}^* - 1$ ($1 = |-1|$). Dovrebbe seguire $1\mathcal{R}^* - 1$, che è vero. Proviamo $a = 2, b = -2, c = 2$. $2\mathcal{R}^* - 2$ ($2 = |-2|$). $-2\mathcal{R}^*2$ (falso). Sembra transitiva? No. $a = 2, b = 2, c = -2$. $2\mathcal{R}^*2$ ($2 = |2|$). $2\mathcal{R}^* - 2$ ($2 = |-2|$). Deve seguire $2\mathcal{R}^* - 2$, vero. Forse è transitiva.
  - $(\mathbb{Z}, \mathcal{R}_{\leq})$ con $a\mathcal{R}_{\leq}b \iff a \leq b$.
    - Riflessiva ($a \leq a$). Sì.
    - Antisimmetrica ($a \leq b \land b \leq a \implies a = b$). Sì.
    - Transitiva ($a \leq b \land b \leq c \implies a \leq c$). Sì.
    - (È una relazione d'ordine). Non Antiriflessiva, Non Simmetrica (a meno che $a = b$), Non Asimmetrica.
  - $(\mathbb{Z}, |)$ (divisibilità).

    - Riflessiva ($a \mid a$, $a = a \cdot 1$). Sì.
    - Antisimmetrica? $a \mid b \wedge b \mid a \implies a = \pm b$. Non è $a = b$. No.
    - Transitiva ($a \mid b \wedge b \mid c \implies a \mid c$). Sì.
- **Relazione Simmetrica e Asimmetrica (Pag 28):** Una relazione $\mathcal{R}$ è sia simmetrica sia asimmetrica se e solo se il suo grafo G è vuoto. (L'asimmetria implica $G \cap G^{-1} = \emptyset$, la simmetria $G = G^{-1}$, quindi $G = \emptyset$).
- **Relazione Simmetrica e Antisimmetrica (Pag 29):** Una relazione $\mathcal{R}$ è sia simmetrica sia antisimmetrica se e solo se il suo grafo G è contenuto nella diagonale ($G \subseteq Diag(A)$).
    - Esempio: La relazione di uguaglianza.

Relazione binaria Relazione riflessiva Relazione simmetrica Relazione transitiva Relazione antisimmetrica Relazione asimmetrica Relazione antiriflessiva

---

Riepilogo Veloce Lezione 9

- Le **Tavole di Cayley** aiutano a visualizzare operazioni su insiemi finiti e a verificarne le proprietà (commutatività, neutro, inversi, cancellabilità).
- In strutture finite, **cancellabilità** $\iff$ **iniettività** della mappa di moltiplicazione.
- Un elemento **nilpotente** $a \neq 0$ ($a^n = 0$) è sempre un **divisore dello zero**.
- Abbiamo definito la **divisibilità** in anelli, gli **elementi associati** ($x \sim y \iff x = uy, u \in U(A)$), i **divisori banali/propri**.
- In $\mathbb{Z}$, abbiamo definito **MCD**, **mcm** e **numeri primi**.
- Abbiamo introdotto le **relazioni binarie** su un insieme A e le loro proprietà fondamentali: riflessiva, antiriflessiva, simmetrica, asimmetrica, antisimmetrica, transitiva.

Prossimi Passi

- Rivedi le definizioni delle proprietà delle relazioni binarie. Prova a classificarne altre (es. "<", ">", "essere fratello di", "essere antenato di").
- Le combinazioni di queste proprietà daranno origine a strutture importanti: relazioni di equivalenza (riflessiva, simmetrica, transitiva) e relazioni d'ordine (riflessiva, antisimmetrica, transitiva).

Lezione 10: Principio di Induzione, Divisione Euclidea, Relazioni di Equivalenza

Data: 14/04/2025 (come da note)
Argomenti: Principio del Buon Ordinamento, Principio di Induzione (Forma I e II), Esempi di Induzione, Teorema della Divisione Euclidea, Identità di Bézout, Relazioni di Equivalenza, Relazioni d'Ordine, Esercizi.

#tag/induction #tag/well-ordering #tag/number-theory #tag/division-algorithm #tag/bezout-identity #tag/relations #tag/equivalence-relations #tag/order-relations #tag/algebra-avanzata

---

1. Principio del Buon Ordinamento e Principio di Induzione

1.1 Insiemi Ben Ordinati

- **Definizione (Pag 1):** Un insieme parzialmente ordinato $(S, \leq)$ si dice **ben ordinato** se ogni suo sottoinsieme **non vuoto** $X \subseteq S$ ammette un **elemento minimo**.
    - $\min X = a \iff (a \in X) \wedge (\forall x \in X, a \leq x)$.
- **Esempi:**
    - $(\mathbb{N}, \leq)$ **è ben ordinato**. Questo è il **Principio del Buon Ordinamento** per i naturali. È una proprietà fondamentale.
    - $(\mathbb{Z}, \leq)$ **non è ben ordinato**. Il sottoinsieme $\mathbb{Z}$ stesso non ha minimo. Il sottoinsieme degli interi negativi non ha minimo.
    - $(\mathbb{Q}^+, \leq)$ dove $\mathbb{Q}^+ = \{x \in \mathbb{Q} \mid x \geq 0\}$ **non è ben ordinato**.
        - Consideriamo $X = \{1/n \mid n \in \mathbb{N}^* = \{1, 2, 3, \dots\}\} = \{1, 1/2, 1/3, \dots\}$. Questo insieme non ha minimo (si avvicina a 0, ma 0 non appartiene a X e nessun elemento di X è il minimo).
        - Anche $\mathbb{Q}^+$ stesso ha minimo (0), ma non tutti i suoi sottoinsiemi non vuoti ce l'hanno.
    - Un insieme ben ordinato deve essere **totalmente ordinato** (Pag 3). Se $(S, \leq)$ è ben ordinato, allora per ogni $a, b \in S$, il sottoinsieme $\{a, b\}$ deve avere un minimo. Se $\min\{a, b\} = a$, allora $a \leq b$. Se $\min\{a, b\} = b$, allora $b \leq a$. Quindi a, b sono sempre confrontabili.
    - Tuttavia, essere totalmente ordinato non basta per essere ben ordinato (es. $\mathbb{Z}, \mathbb{Q}^+$).

Insieme ben ordinato Principio del Buon Ordinamento

1.2 Principio di Induzione (Derivato dal Buon Ordinamento)

Il Principio di Induzione è uno strumento potente per dimostrare proprietà $P(n)$ che valgono per tutti i numeri naturali n a partire da un certo punto. Si basa sul fatto che $(\mathbb{N}, \leq)$ è ben ordinato.

- Sia $P(n)$ una proprietà definita per $n \in \mathbb{N}$. Sia $X = \{n \in \mathbb{N} \mid P(n) \text{ è vera}\}$. Vogliamo dimostrare che X contiene tutti i naturali a partire da un certo $\bar{n}$ (spesso $\bar{n} = 0$ o $\bar{n} = 1$).
- **Principio di Induzione (Forma I - Standard) (Pag 5, 11):**
  Sia $P(n)$ una proprietà per $n \in \mathbb{N}$. Se valgono entrambe le seguenti condizioni:
  1. **Base dell'Induzione:** $P(\bar{n})$ è vera per un certo $\bar{n} \in \mathbb{N}$ (spesso $\bar{n} = 0$ o 1).
  2. **Passo Induttivo:** Per ogni $n \geq \bar{n}$, **se** $P(n)$ è vera (**ipotesi induttiva**), **allora** anche $P(n+1)$ è vera. ($\forall n \geq \bar{n}, P(n) \implies P(n+1)$).
     Allora: $P(n)$ è vera per ogni $n \geq \bar{n}$. (Cioè $X = \{n \in \mathbb{N} \mid n \geq \bar{n}\}$).
- **Principio di Induzione (Forma II - Forte) (Pag 11):**
  Sia $P(n)$ una proprietà per $n \in \mathbb{N}$. Se valgono entrambe le seguenti condizioni:
  1. **Base dell'Induzione:** $P(\bar{n})$ è vera per un certo $\bar{n} \in \mathbb{N}$.
  2. **Passo Induttivo Forte:** Per ogni $n > \bar{n}$, **se** $P(i)$ è vera per **tutti** gli i tali che $\bar{n} \leq i < n$ (**ipotesi induttiva forte**), **allora** anche $P(n)$ è vera. ($\forall n > \bar{n}, (\forall i, \bar{n} \leq i < n \implies P(i)) \implies P(n)$).
     Allora: $P(n)$ è vera per ogni $n \geq \bar{n}$.

> **Le due forme sono logicamente equivalenti. La Forma II sembra richiedere un'ipotesi più forte, ma permette di dimostrare il passo induttivo in casi in cui $P(n+1)$ dipende non solo da $P(n)$ ma anche da $P(k)$ per $k < n$.**

Principio di Induzione

Ecco una tabella che confronta le due forme, aiuti a visualizzare meglio la differenza:

Caratteristica	Principio di Induzione (Forma I - Standard)	Principio di Induzione (Forma II - Forte)
Obiettivo	Dimostrare che una proprietà $P(n)$ è vera per tutti gli $n \geq \bar{n}$.	Dimostrare che una proprietà $P(n)$ è vera per tutti gli $n \geq \bar{n}$.
1. Base dell'Induzione	Dimostrare che $P(\bar{n})$ è vera.	Dimostrare che $P(\bar{n})$ è vera (a volte servono più casi base, es. $P(\bar{n}+1)$).
2. Passo Induttivo	Dimostrare l'implicazione: $\forall n \geq \bar{n}, \quad P(n) \implies P(n+1)$	Dimostrare l'implicazione: $\forall n > \bar{n}, \quad (\forall i, \bar{n} \leq i < n \implies P(i)) \implies P(n)$
Ipotesi Induttiva	Si assume che $P(n)$ sia vera per **un singolo** valore n.	Si assume che $P(i)$ sia vera per **TUTTI** i valori i da $\bar{n}$ fino a $n-1$.
Tesi da Dimostrare	Si dimostra che $P(n+1)$ è vera.	Si dimostra che $P(n)$ è vera.
Analogia Domino	Se la tessera n cade, allora fa cadere la tessera $n+1$.	Se **tutte** le tessere da $\bar{n}$ a $n-1$ sono cadute, allora fanno cadere la tessera n.

Punti Chiave della Tabella:

- L'**obiettivo** è lo stesso per entrambe le forme.
- La **Base** è simile (dimostrare il primo/i primi casi).
- La grande differenza è nel **Passo Induttivo**:
  - **Forma I:** Assumi vero per $n \implies$ Dimostri vero per $n+1$. (Guardi solo l'ultimo passo).
  - **Forma II:** Assumi vero per *tutti* da $\bar{n}$ a $n-1 \implies$ Dimostri vero per n. (Guardi tutta la storia precedente).

1.3 Esempi di Dimostrazioni per Induzione

- **Esempio 1: Somma dei primi n interi (Pag 4, 6):**
  - $P(n) : 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. Vogliamo dimostrare per $n \geq 1$.
  - **Base ($\bar{n} = 1$):** $P(1) : 1 = \frac{1(1+1)}{2} = \frac{1 \cdot 2}{2} = 1$. Vera.
  - **Passo Induttivo (Forma I):** Assumiamo $P(n)$ vera per un $n \geq 1$ (Ipotesi Induttiva: $1 + \cdots + n = \frac{n(n+1)}{2}$). Dobbiamo dimostrare $P(n+1)$, cioè $1 + \cdots + n + (n+1) = \frac{(n+1)((n+1)+1)}{2} = \frac{(n+1)(n+2)}{2}$.
    - Partiamo dal lato sinistro di $P(n+1)$:

$$(1 + 2 + \cdots + n) + (n+1)$$

    - Usiamo l'ipotesi induttiva sul pezzo tra parentesi:

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

    - Mettiamo a denominatore comune:

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

- Raccogliamo $(n+1)$:

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

- Questo è esattamente il lato destro di $P(n+1)$. Abbiamo dimostrato $P(n) \implies P(n+1)$.

- **Conclusione:** Per il Principio di Induzione, $P(n)$ è vera per ogni $n \geq 1$.

- **Esempio 2: Cardinalità dell'Insieme delle Parti (Pag 7-10):**
  - $P(n)$: Se $|S| = n$, allora $|P(S)| = 2^n$. Vogliamo dimostrare per $n \geq 0$.
  - **Base ($\bar{n} = 0$):** $P(0)$: Se $|S| = 0$, allora $S = \emptyset$. $P(S) = \{\emptyset\}$, quindi $|P(S)| = 1$. Vogliamo verificare se $1 = 2^0$. Sì. $P(0)$ è vera.
  - **Passo Induttivo (Forma I):** Assumiamo $P(n)$ vera per un $n \geq 0$ (Ipotesi Induttiva: per ogni insieme T con $|T| = n$, vale $|P(T)| = 2^n$). Dobbiamo dimostrare $P(n+1)$: per ogni insieme S con $|S| = n+1$, vale $|P(S)| = 2^{n+1}$.
    - Sia S un insieme con $|S| = n+1$. Scriviamo $S = \{a_1, \ldots, a_n, a_{n+1}\}$.
    - Consideriamo l'insieme $T = S \setminus \{a_{n+1}\} = \{a_1, \ldots, a_n\}$. Allora $|T| = n$.
    - Per ipotesi induttiva, $|P(T)| = 2^n$.
    - Consideriamo i sottoinsiemi di S. Possiamo dividerli in due categorie:
      1. $\mathcal{B} = \{X \in P(S) \mid a_{n+1} \notin X\}$: Questi sono esattamente i sottoinsiemi di T. Quindi $\mathcal{B} = P(T)$, e $|\mathcal{B}| = |P(T)| = 2^n$.
      2. $\mathcal{A} = \{X \in P(S) \mid a_{n+1} \in X\}$: Ogni insieme X in $\mathcal{A}$ può essere scritto come $X = Y \cup \{a_{n+1}\}$ dove $Y = X \setminus \{a_{n+1}\}$. Notiamo che $Y \subseteq T$ (perché Y non contiene a_{n+1}). Quindi $Y \in P(T) = \mathcal{B}$.
    - Consideriamo la funzione $f : \mathcal{A} \to \mathcal{B}$ definita da $f(X) = X \setminus \{a_{n+1}\}$.
      - È ben definita: se $X \in \mathcal{A}$, $f(X)$ non contiene a_{n+1} ed è un sottoinsieme di T, quindi $f(X) \in \mathcal{B}$.
      - È iniettiva? Se $f(X) = f(Y)$, allora $X \setminus \{a_{n+1}\} = Y \setminus \{a_{n+1}\}$. Poiché sia X che Y contengono a_{n+1} (perché appartengono ad $\mathcal{A}$), aggiungere a_{n+1} ad entrambi i lati mantiene l'uguaglianza: $(X \setminus \{a_{n+1}\}) \cup \{a_{n+1}\} = (Y \setminus \{a_{n+1}\}) \cup \{a_{n+1}\}$, cioè $X = Y$. Sì.
      - È suriettiva? Per ogni $Y \in \mathcal{B}$ (cioè $Y \subseteq T$), consideriamo $X = Y \cup \{a_{n+1}\}$. Chiaramente $a_{n+1} \in X$, quindi $X \in \mathcal{A}$. Inoltre, $f(X) = (Y \cup \{a_{n+1}\}) \setminus \{a_{n+1}\} = Y$. Sì.
      - Quindi f è biettiva.
    - Poiché $f : \mathcal{A} \to \mathcal{B}$ è biettiva, $|\mathcal{A}| = |\mathcal{B}| = 2^n$.
    - L'insieme delle parti $P(S)$ è l'unione disgiunta di $\mathcal{A}$ e $\mathcal{B}$: $P(S) = \mathcal{A} \cup \mathcal{B}$ e $\mathcal{A} \cap \mathcal{B} = \emptyset$.
    - Quindi $|P(S)| = |\mathcal{A}| + |\mathcal{B}| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$.
    - Abbiamo dimostrato $P(n+1)$.
  - **Conclusione:** Per il Principio di Induzione, $P(n)$ è vera per ogni $n \geq 0$.

---

2. Teorema della Divisione Euclidea e Identità di Bézout

Torniamo all'aritmetica in $\mathbb{Z}$.

2.1 Teorema della Divisione Euclidea (Pag 14)

- **Enunciato:** Per ogni $m, n \in \mathbb{Z}$ con $n \neq 0$, esistono **unici** interi q (quoziente) e r (resto) tali che:

$$m = n \cdot q + r \quad \text{e} \quad 0 \leq r < |n|$$

- **Esempi (Pag 14-15):**
  - $m = 17, n = 5$: $17 = 5 \cdot 3 + 2$. $(q = 3, r = 2)$. $0 \leq 2 < |5| = 5$.
  - $m = 17, n = -5$: $17 = (-5) \cdot (-3) + 2$. $(q = -3, r = 2)$. $0 \leq 2 < |-5| = 5$.
  - $m = -17, n = 5$: $-17 = 5 \cdot (-4) + 3$. $(q = -4, r = 3)$. $0 \leq 3 < |5| = 5$. (Attenzione: non $-17 = 5 \cdot (-3) - 2$, perché il resto -2 non soddisfa $0 \leq r < 5$).
  - $m = -17, n = -5$: $-17 = (-5) \cdot 4 + 3$. $(q = 4, r = 3)$. $0 \leq 3 < |-5| = 5$.
  - $m = 5, n = 17$: $5 = 17 \cdot 0 + 5$. $(q = 0, r = 5)$. $0 \leq 5 < |17| = 17$.

- **Dimostrazione (Cenno per Esistenza, $m, n > 0$, Pag 16-18):**
  - Si usa l'induzione (forte) su m.
  - **Base:** Se $0 \leq m < n$. Allora $m = n \cdot 0 + m$. Scegliamo $q = 0, r = m$. Vale $0 \leq r < n$. OK.
  - **Passo Induttivo Forte:** Supponiamo che la tesi valga per tutti gli $\bar{m}$ con $0 \leq \bar{m} < m$ (per un n fissato). Dobbiamo dimostrare che vale per m (assumendo $m \geq n$).
    - Consideriamo $\bar{m} = m - n$. Poiché $m \geq n$, $\bar{m} \geq 0$. Poiché $n > 0$, $\bar{m} < m$.
    - Per ipotesi induttiva forte, esistono $\bar{q}, \bar{r}$ tali che $\bar{m} = n \cdot \bar{q} + \bar{r}$ con $0 \leq \bar{r} < n$.
    - Sostituiamo $\bar{m}$: $m - n = n \cdot \bar{q} + \bar{r}$.
    - Portiamo n a destra: $m = n \cdot \bar{q} + n + \bar{r} = n \cdot (\bar{q} + 1) + \bar{r}$.
    - Abbiamo trovato $q = \bar{q} + 1$ e $r = \bar{r}$. Poiché $0 \leq \bar{r} < n$, abbiamo $0 \leq r < n$.
    - La tesi vale anche per m.

- Per il principio di induzione, l'esistenza è dimostrata per $m, n \geq 0$. (Si estende poi ai casi negativi).
- **Dimostrazione (Unicità, Pag 19-20):**
  - Supponiamo che esistano due coppie (q_1, r_1) e (q_2, r_2) tali che:
    - $m = n \cdot q_1 + r_1$ con $0 \leq r_1 < |n|$
    - $m = n \cdot q_2 + r_2$ con $0 \leq r_2 < |n|$
  - Sottraendo le due equazioni: $0 = n(q_1 - q_2) + (r_1 - r_2)$.
  - Quindi $n(q_1 - q_2) = r_2 - r_1$.
  - Poiché $0 \leq r_1 < |n|$ e $0 \leq r_2 < |n|$, la loro differenza $r_2 - r_1$ soddisfa $-|n| < r_2 - r_1 < |n|$.
  - Ma $n(q_1 - q_2)$ è un multiplo di n. L'unico multiplo di n strettamente compreso tra $-|n|$ e $|n|$ è 0.
  - Quindi deve essere $r_2 - r_1 = 0$, cioè $r_1 = r_2$.
  - Sostituendo nell'equazione $n(q_1 - q_2) = r_2 - r_1$, otteniamo $n(q_1 - q_2) = 0$.
  - Poiché $n \neq 0$, deve essere $q_1 - q_2 = 0$, cioè $q_1 = q_2$.
  - La coppia (q, r) è unica.

Divisione Euclidea

2.2 Identità di Bézout (Pag 21)

- **Enunciato (Corollario del Teorema della Divisione / Algoritmo Euclideo):** Per ogni $a, b \in \mathbb{Z}$, se $d = \text{MCD}(a, b)$ (il MCD positivo), allora esistono interi $h, k \in \mathbb{Z}$ tali che:

$$d = a \cdot h + b \cdot k$$

  - **Spiegazione:** Il Massimo Comun Divisore di due interi può sempre essere espresso come una **combinazione lineare** intera degli stessi due interi.
  - Gli interi h, k non sono unici, ma possono essere trovati usando l'**Algoritmo Euclideo** delle divisioni successive (non visto in dettaglio qui).
- Anche l'associato $-d$ si può esprimere: $-d = a(-h) + b(-k)$.

Identità di Bézout Algoritmo di Euclide

---

3. Relazioni di Equivalenza e Ordine

Riprendiamo le proprietà delle relazioni binarie su un insieme S.

- **Proprietà (Pag 23, 27):**
  1. Riflessiva: $\forall x, x \mathcal{R} x$
  2. Antiriflessiva: $\forall x, \neg(x \mathcal{R} x)$
  3. Simmetrica: $x \mathcal{R} y \implies y \mathcal{R} x$
  4. Antisimmetrica: $(x \mathcal{R} y \wedge y \mathcal{R} x) \implies x = y$
  5. Transitiva: $(x \mathcal{R} y \wedge y \mathcal{R} z) \implies x \mathcal{R} z$
- **Relazione di Equivalenza (Pag 24):** Una relazione $\mathcal{R}$ su S è di equivalenza se è:
  - **Riflessiva (1)**
  - **Simmetrica (3)**
  - **Transitiva (5)**
  - Obiettivo: Partizionare l'insieme in classi di elementi "equivalenti".
- **Relazione d'Ordine (Pag 24):** Una relazione $\mathcal{R}$ su S è d'ordine (parziale) se è:
  - **Riflessiva (1)**
  - **Antisimmetrica (4)**
  - **Transitiva (5)**
  - Se è anche **totalmente definita** ($\forall x, y$, $x \mathcal{R} y$ o $y \mathcal{R} x$), si parla di **ordine totale**.
  - Obiettivo: Stabilire un ordinamento (parziale o totale) tra gli elementi.
- **Esempi di Relazioni di Equivalenza (Pag 25-28):**
  1. **Relazione Totale ($G = S \times S$):** Riflessiva, Simmetrica, Transitiva. **SÌ**. (Tutti gli elementi sono equivalenti tra loro, un'unica classe di equivalenza S).
  2. **Relazione di Identità ($G = Diag(A)$):** Riflessiva, Simmetrica, Transitiva. **SÌ**. (Ogni elemento è equivalente solo a se stesso, classi di equivalenza sono i singleton $\{a\}$).
  3. **$(\mathbb{Z}, \mathcal{R}_{||})$ con $a \mathcal{R}_{||} b \iff |a| = |b|$:** Riflessiva, Simmetrica, Transitiva. **SÌ**. (Classi di equivalenza: $\{0\}, \{1, -1\}, \{2, -2\}, \ldots$).
  4. **Costruzione di $\mathbb{Q}$ (Pag 26-28):** Sia $S = \mathbb{Z} \times \mathbb{Z}^* = \{(a, b) \mid a, b \in \mathbb{Z}, b \neq 0\}$. Definiamo $\mathcal{R}$ su S come:

$$(a, b) \mathcal{R} (c, d) \iff a \cdot d = b \cdot c$$

     (Questa rappresenta l'uguaglianza delle frazioni $a/b = c/d$).

- **Riflessiva?** $(a,b)\mathcal{R}(a,b) \iff a\cdot b = b\cdot a$. Vero per commutatività in $\mathbb{Z}$. **SÌ**.
- **Simmetrica?** $(a,b)\mathcal{R}(c,d) \implies a\cdot d = b\cdot c$. Vogliamo $(c,d)\mathcal{R}(a,b)$, cioè $c\cdot b = d\cdot a$. Per commutatività, $b\cdot c = c\cdot b$ e $a\cdot d = d\cdot a$. Quindi $a\cdot d = b\cdot c \implies d\cdot a = c\cdot b$. **SÌ**.
- **Transitiva?** $(a,b)\mathcal{R}(c,d) \wedge (c,d)\mathcal{R}(e,f)$. Significa $ad = bc$ e $cf = de$. Vogliamo $(a,b)\mathcal{R}(e,f)$, cioè $af = be$.
  - Da $ad = bc$, moltiplichiamo per f: $adf = bcf$.
  - Da $cf = de$, sostituiamo cf: $adf = b(de)$.
  - $adf = bde$. Poiché $d \in \mathbb{Z}^*$, $d \neq 0$. Possiamo cancellare d (perché $\mathbb{Z}$ è dominio): $af = be$. **SÌ**.
- **Conclusione:** $\mathcal{R}$ è una relazione di equivalenza su $\mathbb{Z}\times\mathbb{Z}^*$. Le classi di equivalenza $[(a,b)]$ rappresentano i numeri razionali.

Relazione di equivalenza Relazione d'ordine Costruzione dei numeri razionali

---

4. Esercizi Proposti (Pag 29)

Verificare se le seguenti sono relazioni di equivalenza sui rispettivi insiemi. Ricorda che per essere di equivalenza, una relazione deve essere **Riflessiva**, **Simmetrica** e **Transitiva**.

Esercizio 1: Relazione su P(S)

Sia $S = \{a,b,c,d\}$ e sia $K = \{b,c\}$.
Si consideri la relazione $\mathcal{R}_1$ su $P(S)$ definita da:

$$X\mathcal{R}_1 Y \iff X\cap K = Y\cap K$$

Verificare se $\mathcal{R}_1$ è una relazione di equivalenza.

Esercizio 2: Relazione su P(S)

Sia $S = \{a,b,c,d\}$ e sia $K = \{b,c\}$.
Si consideri la relazione $\mathcal{R}_2$ su $P(S)$ definita da:

$$X\mathcal{R}_2 Y \iff X\cup K = Y\cup K$$

Verificare se $\mathcal{R}_2$ è una relazione di equivalenza.

Esercizio 3: Relazione su P(S)

Sia $S = \{a,b,c,d\}$ e sia $K = \{b,c\}$.
Si consideri la relazione $\mathcal{R}_3$ su $P(S)$ definita da:

$$X\mathcal{R}_3 Y \iff X\setminus K = Y\setminus K$$

Verificare se $\mathcal{R}_3$ è una relazione di equivalenza.

Esercizio 4: Relazione su $\mathbb{Z}\times\mathbb{Z}$

Si consideri la relazione $\mathcal{R}_4$ su $\mathbb{Z}\times\mathbb{Z}$ definita da:

$$(a,b)\mathcal{R}_4(c,d) \iff a+c = b+d$$

Verificare se $\mathcal{R}_4$ è una relazione di equivalenza.

Riepilogo Veloce Lezione 10

- Il **Principio del Buon Ordinamento** di $\mathbb{N}$ garantisce che ogni sottoinsieme non vuoto ha minimo.
- Il **Principio di Induzione** (Forma I e II) è una tecnica di dimostrazione basata sul buon ordinamento.
- Il **Teorema della Divisione Euclidea** garantisce esistenza e unicità di quoziente e resto r con $0 \leq r < |n|$.
- L'**Identità di Bézout** afferma che $\mathrm{MCD}(a,b)$ è combinazione lineare intera di a e b.
- Una **Relazione di Equivalenza** è Riflessiva, Simmetrica, Transitiva.
- Una **Relazione d'Ordine** è Riflessiva, Antisimmetrica, Transitiva.
- La relazione $ad = bc$ su $\mathbb{Z}\times\mathbb{Z}^*$ è di equivalenza e definisce i razionali.

Prossimi Passi

- Prova a svolgere gli esercizi sulle relazioni di equivalenza.
- Il passo successivo naturale è studiare le **classi di equivalenza** e l'**insieme quoziente** associati a una relazione di equivalenza, e vedere come le partizioni sono collegate.
- Approfondire le **relazioni d'ordine** (parziale, totale, massimi, minimi, maggioranti, minoranti).

Lezione 11: Divisione Euclidea, Bézout, FTA, Relazioni di Equivalenza

Data: 15/04/2025 (come da note)
Argomenti: Divisione Euclidea, Algoritmo Euclideo, MCD, Identità di Bézout, Algoritmo Esteso Euclideo, Teorema Fondamentale Aritmetica, Relazioni di Equivalenza, Classi di Equivalenza, Insieme Quoziente.

#tag/number-theory #tag/euclidean-algorithm #tag/bezout #tag/fta #tag/equivalence-relation #tag/equivalence-class #tag/quotient-set #tag/algebra-avanzata #tag/teorema #tag/definizione #tag/esempio

---

1. Aritmetica in $\mathbb{Z}$: MCD e Identità di Bézout

Approfondiamo le proprietà dei numeri interi $\mathbb{Z}$.

1.1 Teorema della Divisione Euclidea (Richiamo)

Questo teorema è la base per l'algoritmo di Euclide.

Teorema della Divisione Euclidea

Dati due interi $a, b \in \mathbb{Z}$, con $b \neq 0$, esistono **unici** due interi q (quoziente) e r (resto) tali che:

$$a = b \cdot q + r$$

con la condizione che $0 \leq r < |b|$ (il resto è non negativo e strettamente minore del valore assoluto del divisore).

- r è anche denotato come $r = \text{rest}(a, b)$.

Teorema Divisione Euclidea

1.2 Algoritmo di Euclide per il MCD

Questo algoritmo permette di calcolare il Massimo Comun Divisore (MCD) tra due interi a, b (non entrambi nulli) tramite divisioni successive.

Idea: Sfrutta la proprietà che $\text{MCD}(a, b) = \text{MCD}(b, r)$, dove r è il resto della divisione di a per b. Si continua a sostituire la coppia (a, b) con (b, r) finché il resto non diventa 0. L'ultimo resto **non nullo** è il MCD.

Passaggi:

1. Siano $a, b \in \mathbb{Z}$ con $b \neq 0$. (Se $b = 0$, $\text{MCD}(a, 0) = |a|$). Assumiamo $|a| \geq |b|$.
2. Dividi a per b: $a = bq_1 + r_1$, con $0 \leq r_1 < |b|$.
3. Se $r_1 = 0$, allora $b \mid a$ e $\text{MCD}(a, b) = |b|$. **STOP**.
4. Se $r_1 \neq 0$, sostituisci (a, b) con (b, r_1) e ripeti dal passo 2:
   - Dividi b per r_1: $b = r_1 q_2 + r_2$, con $0 \leq r_2 < r_1$.
5. Se $r_2 = 0$, allora $\text{MCD}(a, b) = r_1$. **STOP**.
6. Se $r_2 \neq 0$, sostituisci (b, r_1) con (r_1, r_2) e ripeti:
   - Dividi r_1 per r_2: $r_1 = r_2 q_3 + r_3$, con $0 \leq r_3 < r_2$.
7. Continua così. Poiché i resti $r_1 > r_2 > r_3 > \cdots \geq 0$ sono interi e decrescono strettamente, l'algoritmo deve terminare con un resto nullo $r_{n+1} = 0$.
8. L'ultimo resto **non nullo**, r_n, è $\text{MCD}(a, b)$.

Algoritmo di Euclide Massimo Comun Divisore

1.3 Esempio: Calcolo MCD(375, 110) (da note)

Applichiamo l'algoritmo di Euclide:

1. $a = 375, b = 110$.
   $375 = 110 \cdot 3 + 45$ $(q_1 = 3, r_1 = 45)$
2. $a = 110, b = 45$. $(r_1 \neq 0)$
   $110 = 45 \cdot 2 + 20$ $(q_2 = 2, r_2 = 20)$
3. $a = 45, b = 20$. $(r_2 \neq 0)$
   $45 = 20 \cdot 2 + 5$ $(q_3 = 2, r_3 = 5)$
4. $a = 20, b = 5$. $(r_3 \neq 0)$
   $20 = 5 \cdot 4 + 0$ $(q_4 = 4, r_4 = 0)$
5. Il resto è 0. L'ultimo resto non nullo è $r_3 = 5$.

$\text{MCD}(375, 110) = 5$.

1.4 Teorema di Bézout (Identità)

Questo teorema fondamentale collega il MCD a una combinazione lineare degli interi originali.

Teorema di Bézout

Siano $a, b \in \mathbb{Z}$, non entrambi nulli. Allora esistono due interi $x, y \in \mathbb{Z}$ tali che:

$$ax + by = \text{MCD}(a, b)$$

Questi interi x, y sono detti **coefficienti di Bézout**.

- **Dimostrazione (Idea):** Si considera l'insieme $S = \{as + bt \mid s, t \in \mathbb{Z}, as + bt > 0\}$. Si dimostra che S non è vuoto e che il suo minimo elemento (che esiste per il principio del buon ordinamento) è proprio $d = \text{MCD}(a, b)$. Quindi esistono x, y tali che $ax + by = d$.

1. **Definizione dell'insieme S:**
   Consideriamo l'insieme S di tutte le combinazioni lineari positive di a e b:
   $$S = \{as + bt \mid s, t \in \mathbb{Z} \text{ e } as + bt > 0\}$$
2. **S è non vuoto:**
   Poiché a e b non sono entrambi nulli, supponiamo senza perdita di generalità che $a \neq 0$.
   - Se $a > 0$, allora scegliendo $s = 1, t = 0$, si ha $a \cdot 1 + b \cdot 0 = a > 0$. Quindi $a \in S$.
   - Se $a < 0$, allora scegliendo $s = -1, t = 0$, si ha $a \cdot (-1) + b \cdot 0 = -a > 0$. Quindi $-a \in S$.
     In entrambi i casi, S contiene almeno un elemento (nello specifico, $|a| \in S$ se $a \neq 0$, e $|b| \in S$ se $b \neq 0$).
     Pertanto, $S \neq \emptyset$.
3. **Esistenza di un elemento minimo in S:**
   S è un sottoinsieme non vuoto di $\mathbb{Z}^+$ (l'insieme degli interi positivi). Per il **Principio del Buon Ordinamento**, S deve contenere un elemento minimo. Sia d tale elemento minimo.
   Poiché $d \in S$, per la definizione di S, esistono $x, y \in \mathbb{Z}$ tali che:
   $$d = ax + by$$
4. **Dimostriamo che d divide a e d divide b:**
   - **d divide a:**
     Per il Teorema della Divisione Euclidea, esistono unici interi q (quoziente) e r (resto) tali che:
     $$a = dq + r$$
     con $0 \leq r < d$.
     Vogliamo dimostrare che $r = 0$.
     Sostituendo $d = ax + by$ nell'espressione del resto:
     $$r = a - dq = a - (ax + by)q = a - axq - byq = a(1 - xq) + b(-yq)$$
     Siano $s' = 1 - xq$ e $t' = -yq$. Allora $s', t' \in \mathbb{Z}$, e $r = as' + bt'$.
     Se $r > 0$, allora r sarebbe un elemento di S (poiché è una combinazione lineare positiva di a e b).
     Tuttavia, $r < d$, e d è l'elemento minimo di S. Questo è una contraddizione, poiché non può esistere un elemento in S che sia positivo e strettamente minore del minimo elemento di S.
     Pertanto, l'ipotesi $r > 0$ deve essere falsa. Poiché $0 \leq r$, ne consegue che $r = 0$.
     Se $r = 0$, allora $a = dq$, il che implica che $d \mid a$.
   - **d divide b:**
     Analogamente, applicando la Divisione Euclidea a b e d:
     $b = dq' + r'$, con $0 \leq r' < d$.
     Si ottiene $r' = b - dq' = b - (ax + by)q' = a(-xq') + b(1 - yq')$.
     Se $r' > 0$, allora $r' \in S$ e $r' < d$, il che contraddice la minimalità di d in S.
     Quindi $r' = 0$, il che implica $b = dq'$, e dunque $d \mid b$.

   Abbiamo così stabilito che d è un divisore comune di a e b.
5. **Dimostriamo che d è il *massimo* comun divisore:**
   Sia c un qualsiasi divisore comune di a e b. Allora $c \mid a$ e $c \mid b$.
   Questo significa che esistono interi k_1, k_2 tali che $a = ck_1$ e $b = ck_2$.
   Consideriamo l'espressione di d:
   $$d = ax + by$$
   Sostituendo le espressioni per a e b:
   $$d = (ck_1)x + (ck_2)y = c(k_1x + k_2y)$$
   Poiché k_1, x, k_2, y sono interi, anche $K = k_1x + k_2y$ è un intero.
   Quindi $d = cK$, il che significa che $c \mid d$.
   Se c è un divisore comune di a e b, allora c divide anche d.

Per convenzione, il MCD è positivo. Poiché $d \in S$, $d > 0$. Se c è un divisore comune positivo, allora $c \leq d$.
Questo dimostra che d è maggiore o uguale a ogni altro divisore comune di a e b.
Pertanto, $d = \text{MCD}(a, b)$.

6. **Conclusione:**
Abbiamo dimostrato che l'elemento minimo d dell'insieme S è uguale a $\text{MCD}(a, b)$.
Poiché $d = ax + by$ per alcuni $x, y \in \mathbb{Z}$ (dalla definizione di d come elemento di S), segue che:

$$\text{MCD}(a, b) = ax + by$$

Questo completa la dimostrazione dell'esistenza dei coefficienti di Bézout x e y.

Q.E.D. (Quod Erat Demonstrandum - Ciò Che Dovevasi Dimostrare)

Teorema di Bézout

1.5 Algoritmo Esteso di Euclide (Trovare x, y)

Questo metodo permette di trovare i coefficienti x, y dell'identità di Bézout risalendo i passaggi dell'algoritmo di Euclide.

Passaggi:

1. Esegui l'algoritmo di Euclide per trovare $d = \text{MCD}(a, b)$, tenendo traccia di tutte le divisioni.
2. Prendi l'equazione della penultima divisione, quella che ha dato d come resto. Esplicita d da questa equazione.
3. Prendi l'equazione della divisione precedente. Esplicita il resto di quella divisione.
4. Sostituisci il resto del passo 3 nell'espressione di d ottenuta al passo 2. Raccogli i termini contenenti a e b (o i resti precedenti).
5. Continua a risalire le equazioni dell'algoritmo di Euclide, sostituendo via via i resti precedenti e raccogliendo i termini, finché non ottieni un'espressione della forma $d = a \cdot x + b \cdot y$.

Algoritmo Esteso di Euclide

1.6 Esempio: Trovare x, y per MCD(375, 110) = 5 (da note)

Riprendiamo le divisioni dell'esempio 1.3:
(1) $375 = 110 \cdot 3 + 45$
(2) $110 = 45 \cdot 2 + 20$
(3) $45 = 20 \cdot 2 + 5$
(4) $20 = 5 \cdot 4 + 0$

Il MCD è 5. Partiamo dall'equazione (3) e isoliamo 5:
$5 = 45 - 20 \cdot 2$

Ora usiamo l'equazione (2) per sostituire 20. Da (2): $20 = 110 - 45 \cdot 2$.
$5 = 45 - (110 - 45 \cdot 2) \cdot 2$
$5 = 45 - 110 \cdot 2 + 45 \cdot 4$
$5 = 45 \cdot (1 + 4) - 110 \cdot 2$
$5 = 45 \cdot 5 - 110 \cdot 2$

Ora usiamo l'equazione (1) per sostituire 45. Da (1): $45 = 375 - 110 \cdot 3$.
$5 = (375 - 110 \cdot 3) \cdot 5 - 110 \cdot 2$
$5 = 375 \cdot 5 - 110 \cdot 15 - 110 \cdot 2$
$5 = 375 \cdot 5 - 110 \cdot (15 + 2)$
$5 = 375 \cdot 5 - 110 \cdot 17$
$5 = 375 \cdot (5) + 110 \cdot (-17)$

Abbiamo trovato l'identità di Bézout: $ax + by = d$ con $a = 375, b = 110, d = 5$.
I coefficienti sono $x = 5$ e $y = -17$.

$375 \cdot (5) + 110 \cdot (-17) = 5$.

1.7 Esempio Alternativo: MCD(100, 54) e Bézout (da lavagna)

1. $100 = 54 \cdot 1 + 46 \ \ (r_1 = 46)$
2. $54 = 46 \cdot 1 + 8 \ \ (r_2 = 8)$
3. $46 = 8 \cdot 5 + 6 \ \ (r_3 = 6)$
4. $8 = 6 \cdot 1 + 2 \ \ (r_4 = 2)$
5. $6 = 2 \cdot 3 + 0 \ \ (r_5 = 0)$

$\text{MCD}(100, 54) = 2$.

Troviamo x, y tali che $100x + 54y = 2$.
Partiamo da (4): $2 = 8 - 6 \cdot 1$
Sostituiamo 6 da (3): $6 = 46 - 8 \cdot 5$
$2 = 8 - (46 - 8 \cdot 5) \cdot 1 = 8 - 46 + 8 \cdot 5 = 8 \cdot 6 - 46 \cdot 1$
Sostituiamo 8 da (2): $8 = 54 - 46 \cdot 1$
$2 = (54 - 46 \cdot 1) \cdot 6 - 46 \cdot 1 = 54 \cdot 6 - 46 \cdot 6 - 46 \cdot 1 = 54 \cdot 6 - 46 \cdot 7$
Sostituiamo 46 da (1): $46 = 100 - 54 \cdot 1$
$2 = 54 \cdot 6 - (100 - 54 \cdot 1) \cdot 7 = 54 \cdot 6 - 100 \cdot 7 + 54 \cdot 7$
$2 = 54 \cdot (6 + 7) - 100 \cdot 7$
$2 = 54 \cdot 13 - 100 \cdot 7$
$2 = 100 \cdot (-7) + 54 \cdot (13)$

I coefficienti sono $x = -7$ e $y = 13$.

$100 \cdot (-7) + 54 \cdot (13) = 2$.

1.8 Conseguenze e Proprietà (da note/lavagna)

Siano $a, b \in \mathbb{Z}$.

1. $\text{MCD}(a, b)$ è definito a meno del segno (cioè, è l'insieme $\{d, -d\}$). Si prende convenzionalmente il positivo.
2. $\text{mcm}(a, b)$ è definito a meno del segno (cioè, è l'insieme $\{m, -m\}$). Si prende convenzionalmente il positivo.
3. $|a \cdot b| = \text{MCD}(a, b) \cdot \text{mcm}(a, b)$.
4. Se $d \mid a$ e $d \mid b$, allora $d \mid (ax + by)$ per ogni $x, y \in \mathbb{Z}$. In particolare $d \mid \text{MCD}(a, b)$.
5. a, b sono **coprimi** (o primi tra loro) $\iff \text{MCD}(a, b) = 1$.
   - Questo è equivalente a dire che esistono $x, y \in \mathbb{Z}$ tali che $ax + by = 1$.
6. **Lemma di Euclide:** Se p è un numero primo e $p \mid (a \cdot b)$, allora $p \mid a$ oppure $p \mid b$.
   - **Dimostrazione (Idea):** Se $p \nmid a$, allora $\text{MCD}(p, a) = 1$. Per Bézout, $\exists x, y : px + ay = 1$. Moltiplichiamo per b: $pxb + aby = b$. Poiché $p \mid pxb$ e $p \mid aby$ (dato che $p \mid ab$), allora p divide la loro somma, cioè $p \mid b$.
7. Se $\text{MCD}(a, p) = 1$ e p è primo, allora $p \nmid a$.

Cosa dice il Lemma di Euclide? (La "Regola d'Oro" dei Numeri Primi)

Immagina i numeri primi come gli "atomi indivisibili" dei numeri interi. Il Lemma di Euclide ci dice una cosa fondamentale sul loro comportamento quando incontrano un prodotto:

> Se un numero primo p divide il prodotto di due interi $a \cdot b$ (cioè $p \mid ab$),
> allora p deve dividere almeno uno dei due fattori: o p divide a (cioè $p \mid a$) oppure p divide b (cioè $p \mid b$).
> (Potrebbe anche dividerli entrambi, ma ne divide *almeno uno*).

Esempio Veloce:

- Sia $p = 5$ (un numero primo).
- Consideriamo il prodotto $a \cdot b = 6 \cdot 10 = 60$.
- 5 divide 60 (infatti $60 = 5 \cdot 12$).
- Il lemma ci dice che 5 deve dividere 6 OPPURE 5 deve dividere 10.
- 5 non divide 6.
- 5 divide 10 (infatti $10 = 5 \cdot 2$). Ecco! Il lemma è verificato.

La Dimostrazione: Usiamo Bézout come Arma Segreta!

Ecco come si dimostra formalmente, passo dopo passo. La strategia è considerare i due casi possibili per la relazione tra il primo p e il primo fattore a.

Ingredienti per la Dimostrazione:

1. p è un numero primo.
2. a, b sono numeri interi.
3. Sappiamo per ipotesi che $p \mid (a \cdot b)$. (Il nostro punto di partenza)
4. Vogliamo dimostrare che: $p \mid a$ oppure $p \mid b$. (Il nostro obiettivo)
5. **Strumento Chiave:** Il Teorema di Bézout.

La Dimostrazione:

Consideriamo il numero primo p e l'intero a. Ci sono solo due possibilità per la loro relazione in termini di divisibilità (dato che p è primo):

- **Caso 1: p divide a (cioè $p \mid a$)**
  Se p divide a, allora la conclusione del lemma ($p \mid a$ oppure $p \mid b$) è già soddisfatta! Non dobbiamo fare altro.

Missione compiuta per questo caso.
Esempio: Se $p = 3$ e $ab = 6 \cdot 5 = 30$. $3 \mid 30$. Qui $3 \mid 6$, quindi siamo a posto.

- **Caso 2: p non divide a (cioè $p \nmid a$)**
Questo è il caso più interessante e dove entra in gioco la potenza di Bézout.
Se p è un numero primo e p non divide a, qual è il loro Massimo Comun Divisore, $\text{MCD}(p, a)$?
I divisori (positivi) di un numero primo p sono solo 1 e p stesso.

  - Se p non divide a, allora p non può essere un divisore comune di p e a (diverso da 1, se a non è un multiplo di p).
  - L'unico altro divisore positivo di p è 1. E 1 divide qualsiasi intero, quindi 1 divide a.
  - Quindi, se $p \nmid a$, l'unico divisore comune positivo di p e a è 1.
  - Questo significa che $\text{MCD}(p, a) = 1$. Cioè, p e a sono **coprimi** (o primi tra loro).

  Ora che sappiamo che $\text{MCD}(p, a) = 1$, possiamo usare il **Teorema di Bézout**!
  Il Teorema di Bézout ci dice che esistono due interi x e y tali che:

  $$px + ay = \text{MCD}(p, a)$$

  Sostituendo $\text{MCD}(p, a) = 1$:

  $$px + ay = 1$$

  Questa equazione è la nostra "arma segreta". Ora, moltiplichiamo entrambi i membri di questa equazione per b:

  $$b \cdot (px + ay) = b \cdot 1$$
  $$pxb + aby = b$$

  Adesso analizziamo i termini a sinistra dell'uguale:

  1. **Termine pxb**: Questo termine contiene p come fattore. Quindi, p divide pxb (cioè $p \mid pxb$).
  2. **Termine aby**: Ricordi l'ipotesi iniziale del lemma? Ci è stato dato che $p \mid (a \cdot b)$. Se p divide ab, allora p divide anche qualsiasi multiplo di ab, quindi p divide $(ab)y$ (cioè $p \mid aby$).

  Abbiamo quindi che:

  - p divide il primo addendo (pxb).
  - p divide il secondo addendo (aby).

  Una proprietà fondamentale della divisibilità dice che se un numero (p) divide due altri numeri (nel nostro caso pxb e aby), allora divide anche la loro somma.
  Quindi, p deve dividere la somma $pxb + aby$.
  Ma abbiamo appena visto che $pxb + aby = b$.
  Dunque, concludiamo che $p \mid b$.

  Questo è esattamente ciò che volevamo dimostrare nel Caso 2! Se $p \nmid a$ (e $p \mid ab$), allora necessariamente $p \mid b$.

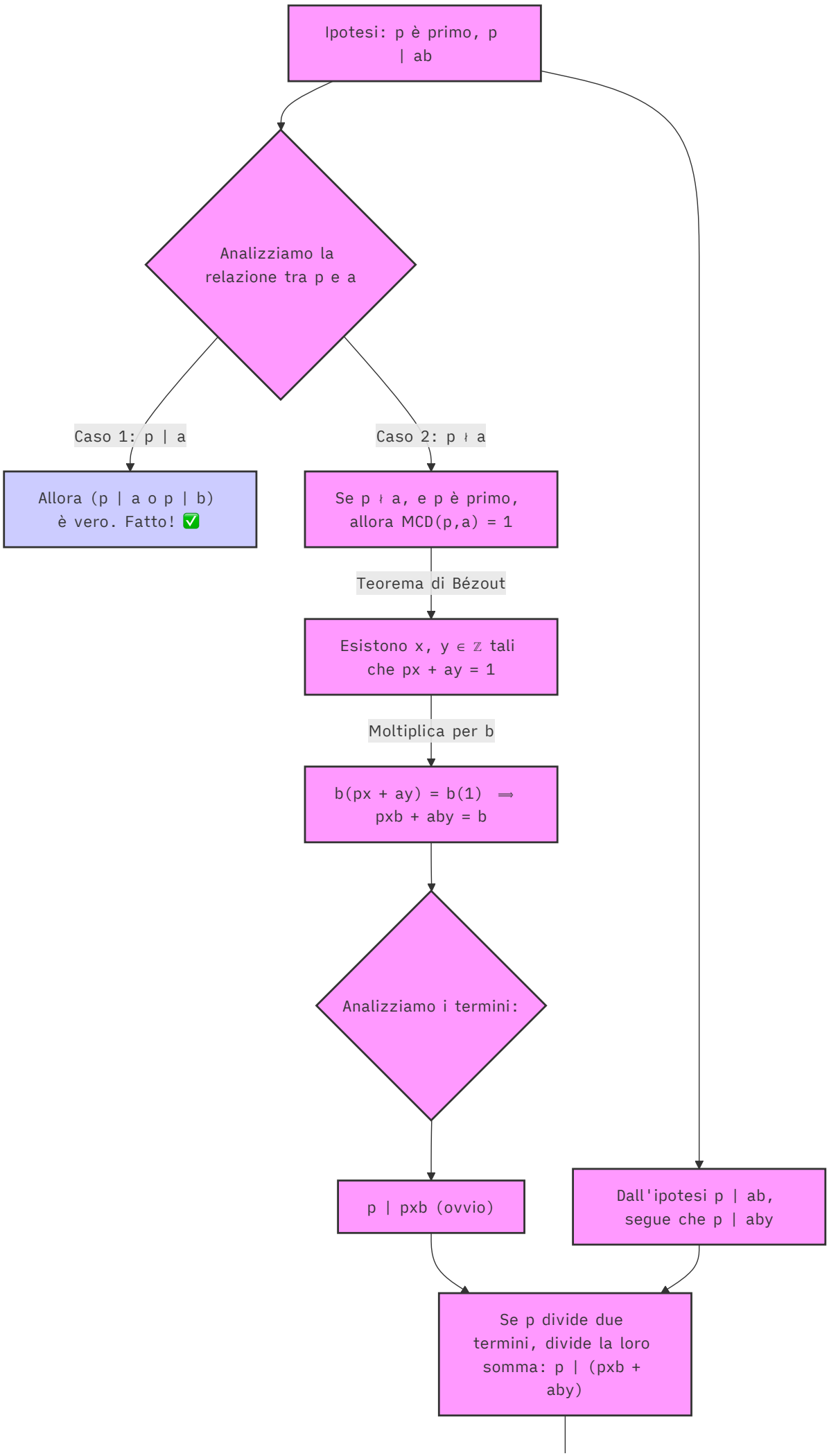
Conclusione della Dimostrazione:

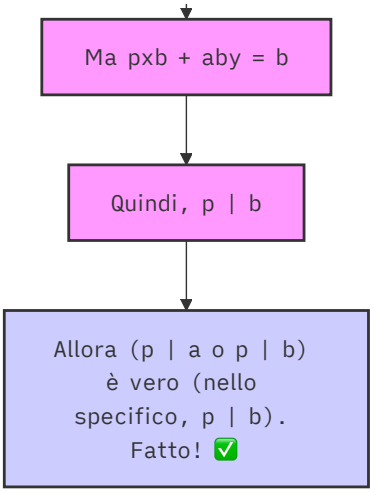
Abbiamo esaminato entrambi i casi possibili:

1. Se $p \mid a$, il lemma è vero.
2. Se $p \nmid a$, abbiamo dimostrato (usando Bézout e l'ipotesi $p \mid ab$) che allora $p \mid b$.

In ogni situazione, se $p \mid ab$, allora $p \mid a$ oppure $p \mid b$.
Il Lemma di Euclide è dimostrato!

Visualizziamo la Logica del Caso 2 (il più complesso):


Ipotesi: p è primo, p | ab
Analizziamo la relazione tra p e a
Caso 1: p | a
Caso 2: p ∤ a
Allora (p | a o p | b) è vero. Fatto! ✅
Se p ∤ a, e p è primo, allora MCD(p,a) = 1
Teorema di Bézout
Esistono x, y ∈ ℤ tali che px + ay = 1
Moltiplica per b
b(px + ay) = b(1) ⟹ pxb + aby = b
Analizziamo i termini:
p | pxb (ovvio)
Dall'ipotesi p | ab, segue che p | aby
Se p divide due termini, divide la loro somma: p | (pxb + aby)



Numeri Coprimi Lemma di Euclide

---

2. Teorema Fondamentale dell'Aritmetica (FTA)

Questo teorema afferma che ogni intero (diverso da 0, 1, -1) si scompone in modo unico in fattori primi.

Teorema Fondamentale dell'Aritmetica

Ogni intero $a \in \mathbb{Z} \setminus \{0, 1, -1\}$ si può scrivere come prodotto di numeri primi. Tale decomposizione è **unica** a meno dell'ordine dei fattori e della sostituzione di un fattore primo p_i con il suo associato $-p_i$.

$$a = (\pm 1) \cdot p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

dove $p_1, \ldots, p_k$ sono primi positivi distinti e $e_i \geq 1$.

- **Unicità (Osservazioni):** L'unicità significa che se abbiamo due scomposizioni in primi positivi $a = p_1 \ldots p_m = q_1 \ldots q_n$, allora $m = n$ e, riordinando opportunamente i q_j, si ha $p_i = q_i$ per ogni i.
- **Ruolo del Lemma di Euclide:** Il Lemma di Euclide è cruciale per dimostrare l'unicità della fattorizzazione.
- **Esempio:** $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3^1$. Le uniche altre scomposizioni (a meno dell'ordine) sono $(-2)(-2) \cdot 3$, $2 \cdot (-2) \cdot (-3)$, ecc., che usano primi associati.

Teorema Fondamentale dell'Aritmetica

---

3. Relazioni di Equivalenza

Un tipo speciale di relazione binaria che generalizza il concetto di "uguaglianza".

3.1 Definizione

Sia $\mathcal{R}$ una relazione binaria su un insieme non vuoto S (cioè $G \subseteq S \times S$). $\mathcal{R}$ è una **Relazione di Equivalenza** se è contemporaneamente:

1. **Riflessiva:** $\forall x \in S, x \mathcal{R} x$.
2. **Simmetrica:** $\forall x, y \in S, x \mathcal{R} y \implies y \mathcal{R} x$.
3. **Transitiva:** $\forall x, y, z \in S, (x \mathcal{R} y \land y \mathcal{R} z) \implies x \mathcal{R} z$.

Relazione di equivalenza

3.2 Classi di Equivalenza

Data una relazione di equivalenza $\mathcal{R}$ su S, per ogni elemento $a \in S$, la **classe di equivalenza** di a rispetto a $\mathcal{R}$ è l'insieme di tutti gli elementi di S che sono in relazione con a:

$$[a]_{\mathcal{R}} = \{x \in S \mid x \mathcal{R} a\}$$

(A volte si definisce come $\{x \in S \mid a \mathcal{R} x\}$, ma per la simmetria le due definizioni coincidono).

Classe di equivalenza

3.3 Proprietà delle Classi di Equivalenza

Sia $\mathcal{R}$ una relazione di equivalenza su S. Valgono le seguenti proprietà fondamentali:

1. **Non vuote:** Per ogni $a \in S$, $a \in [a]_{\mathcal{R}}$ (per riflessività), quindi $[a]_{\mathcal{R}} \neq \emptyset$.
2. **Uguaglianza o Disgiunzione:** Per ogni $a, b \in S$, si ha:

   $$a\mathcal{R}b \iff [a]_{\mathcal{R}} = [b]_{\mathcal{R}}$$

   Inoltre, due classi di equivalenza o sono **esattamente uguali** oppure sono **completamente disgiunte**:

   $$[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} \neq \emptyset \implies [a]_{\mathcal{R}} = [b]_{\mathcal{R}}$$

   Equivalentemente: Se $[a]_{\mathcal{R}} \neq [b]_{\mathcal{R}}$, allora $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} = \emptyset$.
3. **Unione:** L'unione di tutte le classi di equivalenza distinte restituisce l'insieme originale S.

   $$\bigcup_{a \in S} [a]_{\mathcal{R}} = S$$

Le classi di equivalenza formano una partizione dell'insieme S. Ogni elemento di S appartiene a una e una sola classe di equivalenza.

3.4 Insieme Quoziente

- L'**insieme quoziente** di S rispetto alla relazione di equivalenza $\mathcal{R}$, denotato $S/\mathcal{R}$, è l'insieme di **tutte** le classi di equivalenza distinte:

  $$S/\mathcal{R} = \{[a]_{\mathcal{R}} \mid a \in S\}$$

- Gli elementi dell'insieme quoziente sono *insiemi* (le classi di equivalenza).

Insieme quoziente

3.5 Teorema: Equivalenze e Partizioni

Esiste una corrispondenza biunivoca tra le relazioni di equivalenza su S e le partizioni di S.

1. Ogni relazione di equivalenza $\mathcal{R}$ su S **induce** una partizione di S (data dall'insieme quoziente $S/\mathcal{R}$).
2. Ogni partizione $\mathcal{F}$ di S **induce** una relazione di equivalenza $\mathcal{R}_{\mathcal{F}}$ su S, definita da:
   $a\mathcal{R}_{\mathcal{F}}b \iff a$ e b appartengono allo stesso blocco (elemento) $X \in \mathcal{F}$.

Relazioni di Equivalenza e Partizioni

3.6 Esempio: Classi di Equivalenza in P(S) (da lavagna)

Sia $S = \{a, b, c, d\}$. Consideriamo $P(S)$. Definiamo la relazione $\mathcal{R}$ su $P(S)$ come $X\mathcal{R}Y \iff X \cap \{b, c\} = Y \cap \{b, c\}$.

- È una relazione di equivalenza? (Verifica R, S, T è lasciata come esercizio implicito). Assumiamo di sì.
- Troviamo le classi di equivalenza. Due sottoinsiemi X, Y sono nella stessa classe se hanno la stessa intersezione con $\{b, c\}$. Le possibili intersezioni sono:
  - $\emptyset \cap \{b, c\} = \emptyset$
  - $\{b\} \cap \{b, c\} = \{b\}$
  - $\{c\} \cap \{b, c\} = \{c\}$
  - $\{b, c\} \cap \{b, c\} = \{b, c\}$
- Le classi sono determinate da queste 4 possibili intersezioni:
  - $[\emptyset]_{\mathcal{R}} = \{X \subseteq S \mid X \cap \{b, c\} = \emptyset\} = \{\emptyset, \{a\}, \{d\}, \{a, d\}\}$
  - $[\{b\}]_{\mathcal{R}} = \{X \subseteq S \mid X \cap \{b, c\} = \{b\}\} = \{\{b\}, \{a, b\}, \{b, d\}, \{a, b, d\}\}$
  - $[\{c\}]_{\mathcal{R}} = \{X \subseteq S \mid X \cap \{b, c\} = \{c\}\} = \{\{c\}, \{a, c\}, \{c, d\}, \{a, c, d\}\}$
  - $[\{b, c\}]_{\mathcal{R}} = \{X \subseteq S \mid X \cap \{b, c\} = \{b, c\}\} = \{\{b, c\}, \{a, b, c\}, \{b, c, d\}, \{a, b, c, d\} = S\}$
- L'insieme quoziente $P(S)/\mathcal{R}$ ha 4 elementi (queste 4 classi).

Riepilogo Veloce Lezione 11

- Abbiamo visto l'**Algoritmo di Euclide** per calcolare il MCD e l'**Algoritmo Esteso** per trovare i coefficienti dell'**Identità di Bézout** ($ax + by = d$).
- Abbiamo richiamato le **conseguenze** su coprimalità e il **Lemma di Euclide**.
- Abbiamo enunciato il **Teorema Fondamentale dell'Aritmetica** (fattorizzazione unica in primi).
- Abbiamo definito le **Relazioni di Equivalenza** (Riflessiva, Simmetrica, Transitiva).
- Abbiamo definito le **Classi di Equivalenza** $[a]_{\mathcal{R}}$ e visto che **partizionano** l'insieme.
- Abbiamo definito l'**Insieme Quoziente** $S/\mathcal{R}$ come l'insieme delle classi di equivalenza.
- Abbiamo enunciato la corrispondenza tra relazioni di equivalenza e partizioni.

Prossimi Passi

- Fai pratica con l'algoritmo esteso di Euclide per trovare i coefficienti di Bézout.
- Assicurati di aver compreso le proprietà R, S, T e come verificare se una relazione è di equivalenza.
- Cerca di capire bene cosa sono le classi di equivalenza e l'insieme quoziente, magari con esempi concreti (es. congruenza modulo n).

Lezione 12: Relazioni di Equivalenza, Partizioni e Congruenze

Data: 29/04/2025 (come da note)
Argomenti: Teorema Fondamentale (Relazioni di Equivalenza $\iff$ Partizioni), Insieme Quoziente, Relazione di Equivalenza indotta da una Funzione, Applicazione Quoziente, Congruenze, Congruenza Modulo m.

#tag/relations #tag/equivalence-relations #tag/partitions #tag/quotient-set #tag/functions #tag/congruence #tag/number-theory #tag/algebra-avanzata

---

1. Il Teorema Fondamentale sulle Relazioni di Equivalenza

Questo teorema stabilisce un legame profondo e fondamentale tra due concetti apparentemente distinti: le relazioni di equivalenza e le partizioni di un insieme.

- **Ricordiamo:**
  - Una **Relazione di Equivalenza** $\mathcal{R}$ su S è Riflessiva, Simmetrica e Transitiva.
  - Una **Partizione** $\mathcal{F}$ di S è una famiglia di sottoinsiemi non vuoti, disgiunti a due a due, la cui unione è S.
  - Data una relazione di equivalenza $\mathcal{R}$ su S, la **classe di equivalenza** di $a \in S$ è $[a]_{\mathcal{R}} = \{x \in S \mid x\mathcal{R}a\}$.
  - L'**insieme quoziente** $S/\mathcal{R}$ è l'insieme di tutte le classi di equivalenza: $S/\mathcal{R} = \{[a]_{\mathcal{R}} \mid a \in S\}$.
- **Proprietà delle Classi di Equivalenza (Pag 1):**
  1. $\forall a \in S, [a]_{\mathcal{R}} \neq \emptyset$ (perché $a\mathcal{R}a$ per riflessività, quindi $a \in [a]_{\mathcal{R}}$).
  2. $\forall a, b \in S$, o $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$ (se $a\mathcal{R}b$) oppure $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} = \emptyset$ (se $\neg(a\mathcal{R}b)$). Le classi o coincidono o sono disgiunte.
  3. $\bigcup_{a \in S} [a]_{\mathcal{R}} = S$ (ogni elemento $x \in S$ appartiene almeno alla classe $[x]_{\mathcal{R}}$).
- **Osservazione Chiave (Pag 1):** Le proprietà 1, 2, 3 delle classi di equivalenza sono esattamente le proprietà che definiscono una **partizione**! L'insieme quoziente $S/\mathcal{R}$ è una partizione di S.

Teorema Fondamentale sulle Relazioni di Equivalenza (Pag 2)

Sia S un insieme non vuoto ($S \neq \emptyset$). Esiste una **corrispondenza biunivoca** tra l'insieme di tutte le relazioni di equivalenza su S e l'insieme di tutte le partizioni di S.

i) **Da Relazione a Partizione:** Se $\mathcal{R}$ è una relazione di equivalenza su S, allora l'insieme quoziente $S/\mathcal{R} = \{[a]_{\mathcal{R}} \mid a \in S\}$ è una partizione di S.
ii) **Da Partizione a Relazione:** Viceversa, se $\mathcal{F}$ è una partizione di S, allora la relazione $\mathcal{R}_{\mathcal{F}}$ definita da:

$$x\mathcal{R}_{\mathcal{F}}y \iff \exists A \in \mathcal{F} \text{ tale che } x \in A \land y \in A$$

(cioè, x e y sono in relazione se e solo se appartengono allo stesso "pezzo" della partizione $\mathcal{F}$) è una relazione di equivalenza su S.

Inoltre, queste due costruzioni sono una l'inversa dell'altra: partendo da $\mathcal{R}$ e costruendo la partizione $S/\mathcal{R}$, la relazione indotta da questa partizione è proprio $\mathcal{R}$. Viceversa, partendo da $\mathcal{F}$ e costruendo $\mathcal{R}_{\mathcal{F}}$, le classi di equivalenza di $\mathcal{R}_{\mathcal{F}}$ sono esattamente gli insiemi della partizione $\mathcal{F}$.

- **Dimostrazione:**
  - **i) $\mathcal{R} \implies S/\mathcal{R}$ è partizione:** Già verificato osservando le proprietà delle classi di equivalenza (non vuote, disgiunte o coincidenti, unione fa S).
  - **ii) $\mathcal{F} \implies \mathcal{R}_{\mathcal{F}}$ è rel. equivalenza (Pag 3):**
    - **Riflessiva:** $\forall x \in S$. Poiché $\mathcal{F}$ è una partizione, $\bigcup_{A \in \mathcal{F}} A = S$. Quindi x deve appartenere a qualche $A \in \mathcal{F}$. Per definizione, $x\mathcal{R}_{\mathcal{F}}x$. **SÌ**.
    - **Simmetrica:** Supponiamo $x\mathcal{R}_{\mathcal{F}}y$. Allora $\exists A \in \mathcal{F}$ tale che $x \in A \land y \in A$. Ma allora $y \in A \land x \in A$, il che significa $y\mathcal{R}_{\mathcal{F}}x$. **SÌ**.
    - **Transitiva:** Supponiamo $x\mathcal{R}_{\mathcal{F}}y$ e $y\mathcal{R}_{\mathcal{F}}z$. Allora $\exists A \in \mathcal{F}$ tale che $x, y \in A$. E $\exists B \in \mathcal{F}$ tale che $y, z \in B$. Poiché $y \in A$ e $y \in B$, l'intersezione $A \cap B$ non è vuota (contiene almeno y). Ma i pezzi di una partizione sono disgiunti o coincidenti. Quindi, deve essere $A = B$. Ma allora $x \in A$ e $z \in A (= B)$. Per definizione, $x\mathcal{R}_{\mathcal{F}}z$. **SÌ**.
  - **Corrispondenza Inversa (Pag 4):** Dobbiamo verificare che $S/\mathcal{R}_{\mathcal{F}} = \mathcal{F}$.
    - Consideriamo una classe di equivalenza $[a]_{\mathcal{R}_{\mathcal{F}}} = \{x \in S \mid x\mathcal{R}_{\mathcal{F}}a\}$.
    - Per definizione di $\mathcal{R}_{\mathcal{F}}$, questo significa $\{x \in S \mid \exists A \in \mathcal{F} : x \in A \land a \in A\}$.
    - Poiché $\mathcal{F}$ è una partizione, esiste un unico $A_a \in \mathcal{F}$ tale che $a \in A_a$.
    - Quindi la condizione diventa $\{x \in S \mid x \in A_a\}$.

- Questo è esattamente l'insieme A_a.
- Quindi le classi di equivalenza $[a]_{\mathcal{R}_\mathcal{F}}$ sono proprio gli insiemi A_a della partizione originale $\mathcal{F}$.

Relazione di equivalenza Partizione di un insieme Insieme Quoziente Teorema Fondamentale Relazioni Equivalenza

- **Esempio 1 (Pag 5):** $S = \{0, 1, \dots, 20\}$. $\mathcal{F} = \{\{0\}, \{1, 10\}, \{2, 11, 20\}, \{3, 12\}, \{4, 13\}, \{5, 14\}, \{6, 15\}, \{7, 16\}, \{8, 17\}, \{9, 18\}, \{19\}\}$. (Sembra una partizione basata sulla somma delle cifre modulo qualcosa? O forse solo sulla somma delle cifre?).
  - La relazione $\mathcal{R}_\mathcal{F}$ associata è: $x \mathcal{R}_\mathcal{F} y \iff x, y$ appartengono allo stesso blocco di $\mathcal{F}$.
  - Esempio: $1 \mathcal{R}_\mathcal{F} 10$, $2 \mathcal{R}_\mathcal{F} 11$, $2 \mathcal{R}_\mathcal{F} 20$, $11 \mathcal{R}_\mathcal{F} 20$.
  - Le classi di equivalenza sono i blocchi stessi: $[0] = \{0\}$, $[1] = \{1, 10\}$, $[2] = \{2, 11, 20\}$, etc.
  - Se la relazione fosse $x \mathcal{R} y \iff \text{somma cifre}(x) = \text{somma cifre}(y)$:
    - `Somma(0)=0 -> {0}`
    - `Somma(1)=1, Somma(10)=1 -> {1, 10}`
    - `Somma(2)=2, Somma(11)=2, Somma(20)=2 -> {2, 11, 20}`
    - `...` corrisponde alla partizione data.
    - $[7] = \{7, 16\}$. $[1] = [10]$. $[2] = [11] = [20]$.
- **Esempio 2 (Pag 6):** $S = \{a, b, c, d, e\}$. $\mathcal{F} = \{\{a\}, \{b, d\}, \{c, e\}\}$.
  - Questa è una partizione.
  - La relazione $\mathcal{R}_\mathcal{F}$ associata ha le seguenti coppie (oltre a quelle riflessive): $(b, d), (d, b), (c, e), (e, c)$.
  - Le classi di equivalenza sono: $[a]_{\mathcal{R}_\mathcal{F}} = \{a\}$, $[b]_{\mathcal{R}_\mathcal{F}} = \{b, d\} = [d]_{\mathcal{R}_\mathcal{F}}$, $[c]_{\mathcal{R}_\mathcal{F}} = \{c, e\} = [e]_{\mathcal{R}_\mathcal{F}}$.
  - L'insieme quoziente è $S/\mathcal{R}_\mathcal{F} = \{\{a\}, \{b, d\}, \{c, e\}\} = \mathcal{F}$.

---

2. Relazione di Equivalenza Indotta da una Funzione

Ogni funzione definisce naturalmente una relazione di equivalenza sul suo dominio.

Teorema (Pag 8): Relazione di Equivalenza Indotta da una Funzione

Siano S, T insiemi non vuoti e $f : S \to T$ una funzione.
La relazione $\mathcal{R}_f$ su S definita da:

$$x \mathcal{R}_f y \iff f(x) = f(y)$$

è una **relazione di equivalenza** su S.

Dimostrazione (Pag 11):

1. **Riflessiva:** $\forall x \in S$. Poiché $f(x) = f(x)$, vale $x \mathcal{R}_f x$. **SÌ**.
2. **Simmetrica:** Supponiamo $x \mathcal{R}_f y$. Allora $f(x) = f(y)$. Ma allora $f(y) = f(x)$, il che significa $y \mathcal{R}_f x$. **SÌ**.
3. **Transitiva:** Supponiamo $x \mathcal{R}_f y$ e $y \mathcal{R}_f z$. Allora $f(x) = f(y)$ e $f(y) = f(z)$. Per transitività dell'uguaglianza in T, segue $f(x) = f(z)$. Quindi $x \mathcal{R}_f z$. **SÌ**.

- **Classi di Equivalenza per $\mathcal{R}_f$:**
  - $[a]_{\mathcal{R}_f} = \{x \in S \mid x \mathcal{R}_f a\} = \{x \in S \mid f(x) = f(a)\}$.
  - Questa classe è esattamente la **controimmagine** dell'elemento $f(a)$ (visto come singleton $\{f(a)\} \subseteq T$):

$$[a]_{\mathcal{R}_f} = \overleftarrow{f}(\{f(a)\})$$

- **Esempio 1 (Pag 9):** $f : \mathbb{Z} \to \mathbb{Z}$ con $f(x) = |x|$.
  - $x \mathcal{R}_f y \iff |x| = |y|$.
  - $[a]_{\mathcal{R}_f} = \{x \in \mathbb{Z} \mid |x| = |a|\} = \{a, -a\}$ (se $a \neq 0$).
  - $[0]_{\mathcal{R}_f} = \{0\}$.
  - L'insieme quoziente $\mathbb{Z}/\mathcal{R}_f = \{\{0\}, \{1, -1\}, \{2, -2\}, \dots\}$.
- **Esempio 2 (Pag 10):** $f : \{0, \dots, 20\} \to \mathbb{N}$ con $f(x) = \text{somma delle cifre di } x$.
  - $x \mathcal{R}_f y \iff \text{somma cifre}(x) = \text{somma cifre}(y)$.
  - Le classi di equivalenza sono i blocchi della partizione vista prima: $[0] = \{0\}$, $[1] = \{1, 10\}$, $[2] = \{2, 11, 20\}$, etc.

Relazione di equivalenza indotta da funzione

2.1 Applicazione Quoziente (Teorema di Fattorizzazione)

C'è un legame tra la funzione originale f e l'insieme quoziente $S/\mathcal{R}_f$.

- **Teorema (Pag 8, 12-13):** Sia $f : S \to T$ una funzione e $\mathcal{R}_f$ la relazione di equivalenza indotta ($x \mathcal{R}_f y \iff f(x) = f(y)$). Allora esiste un'unica funzione **iniettiva** $\bar{f}$ (detta **applicazione quoziente** o mappa indotta):

$$\bar{f} : S/\mathcal{R}_f \to T$$

definita da:

$$\bar{f}([a]_{\mathcal{R}_f}) = f(a)$$

tale che $f = \bar{f} \circ \pi$, dove $\pi : S \to S/\mathcal{R}_f$ è la **proiezione canonica** $\pi(a) = [a]_{\mathcal{R}_f}$.

- **Spiegazione:**
  - La mappa $\bar{f}$ prende un'intera classe di equivalenza $[a]$ e la manda nell'**unico** valore che la funzione f assume su tutti gli elementi di quella classe (cioè $f(a)$).
  - **Ben definita (Pag 12):** Dobbiamo assicurarci che la definizione di $\bar{f}$ non dipenda dal rappresentante scelto per la classe. Se $[a]_{\mathcal{R}_f} = [b]_{\mathcal{R}_f}$, dobbiamo verificare che $\bar{f}([a]_{\mathcal{R}_f}) = \bar{f}([b]_{\mathcal{R}_f})$.
    - $[a]_{\mathcal{R}_f} = [b]_{\mathcal{R}_f} \implies a\mathcal{R}_f b \implies f(a) = f(b)$.
    - Ma $\bar{f}([a]_{\mathcal{R}_f}) = f(a)$ e $\bar{f}([b]_{\mathcal{R}_f}) = f(b)$.
    - Poiché $f(a) = f(b)$, la definizione è coerente. $\bar{f}$ è ben definita.
  - **Iniettività di $\bar{f}$ (Pag 13):** Dobbiamo verificare che $\bar{f}([a]_{\mathcal{R}_f}) = \bar{f}([b]_{\mathcal{R}_f}) \implies [a]_{\mathcal{R}_f} = [b]_{\mathcal{R}_f}$.
    - $\bar{f}([a]_{\mathcal{R}_f}) = \bar{f}([b]_{\mathcal{R}_f}) \implies f(a) = f(b)$.
    - Per definizione di $\mathcal{R}_f$, $f(a) = f(b) \implies a\mathcal{R}_f b$.
    - Ma $a\mathcal{R}_f b \implies [a]_{\mathcal{R}_f} = [b]_{\mathcal{R}_f}$.
    - Quindi $\bar{f}$ è iniettiva.
  - **Fattorizzazione:** Il diagramma $S \xrightarrow{f} T$ può essere "fattorizzato" come $S \xrightarrow{\pi} S/\mathcal{R}_f \xrightarrow{\bar{f}} T$. Cioè, per andare da S a T con f, puoi prima "collassare" S nell'insieme quoziente $S/\mathcal{R}_f$ tramite π (mandando ogni elemento nella sua classe), e poi applicare la mappa iniettiva $\bar{f}$ per ottenere il valore in T.
- **Esempio $f(x) = |x|$ (Pag 9):**
  - $S = \mathbb{Z}$, $T = \mathbb{N} = \{0, 1, \dots\}$. $\mathcal{R}_f$ è $x\mathcal{R}_f y \iff |x| = |y|$.
  - $S/\mathcal{R}_f = \{[0], [1], [2], \dots\}$ dove $[0] = \{0\}$, $[a] = \{a, -a\}$ per $a > 0$.
  - $\bar{f} : S/\mathcal{R}_f \to \mathbb{N}$ è definita da $\bar{f}([a]) = f(a) = |a|$.
  - $\bar{f}([0]) = |0| = 0$.
  - $\bar{f}([1]) = |1| = 1$.
  - $\bar{f}([2]) = |2| = 2$. ...
  - Questa $\bar{f}$ è chiaramente iniettiva (e anche suriettiva su $\mathbb{N}$, quindi biettiva).
- **Esercizio (Pag 14):** $S = \{a, b, c\}$. $f : P(S) \to P(S)$ con $f(X) = X \cap \{a, b\}$.
  - Troviamo le classi di equivalenza $\mathcal{R}_f$. Due sottoinsiemi X, Y sono in relazione se $X \cap \{a, b\} = Y \cap \{a, b\}$.
  - $P(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, S\}$.
  - $f(\emptyset) = \emptyset \cap \{a, b\} = \emptyset$.
  - $f(\{c\}) = \{c\} \cap \{a, b\} = \emptyset$.
    - $[\emptyset]_{\mathcal{R}_f} = \{\emptyset, \{c\}\}$.
  - $f(\{a\}) = \{a\} \cap \{a, b\} = \{a\}$.
  - $f(\{a, c\}) = \{a, c\} \cap \{a, b\} = \{a\}$.
    - $[\{a\}]_{\mathcal{R}_f} = \{\{a\}, \{a, c\}\}$.
  - $f(\{b\}) = \{b\} \cap \{a, b\} = \{b\}$.
  - $f(\{b, c\}) = \{b, c\} \cap \{a, b\} = \{b\}$.
    - $[\{b\}]_{\mathcal{R}_f} = \{\{b\}, \{b, c\}\}$.
  - $f(\{a, b\}) = \{a, b\} \cap \{a, b\} = \{a, b\}$.
  - $f(S) = \{a, b, c\} \cap \{a, b\} = \{a, b\}$.
    - $[\{a, b\}]_{\mathcal{R}_f} = \{\{a, b\}, S\}$.
  - L'insieme quoziente $P(S)/\mathcal{R}_f$ ha 4 classi:
    - $C_1 = \{\emptyset, \{c\}\}$
    - $C_2 = \{\{a\}, \{a, c\}\}$
    - $C_3 = \{\{b\}, \{b, c\}\}$
    - $C_4 = \{\{a, b\}, S\}$
  - La mappa indotta $\bar{f} : P(S)/\mathcal{R}_f \to P(S)$ è:
    - $\bar{f}(C_1) = f(\emptyset) = \emptyset$.
    - $\bar{f}(C_2) = f(\{a\}) = \{a\}$.
    - $\bar{f}(C_3) = f(\{b\}) = \{b\}$.
    - $\bar{f}(C_4) = f(\{a, b\}) = \{a, b\}$.
    - Come previsto, $\bar{f}$ è iniettiva.

Teorema di Fattorizzazione (Insiemi) Proiezione Canonica

---

3. Congruenze

Relazioni di equivalenza "compatibili" con le operazioni algebriche.

- **Definizione (Pag 18):** Sia $(S, \perp)$ una struttura con un'operazione binaria $\perp$. Una relazione di equivalenza $\mathcal{R}$ su S si dice **congruenza** (o compatibile) rispetto a $\perp$ se:

$$\forall a, b, c, d \in S, \quad (a \mathcal{R} c \wedge b \mathcal{R} d) \implies (a \perp b) \mathcal{R} (c \perp d)$$

  - **Spiegazione:** Se a è equivalente a c, e b è equivalente a d, allora il risultato dell'operazione tra a e b deve essere equivalente al risultato dell'operazione tra c e d. L'equivalenza "rispetta" l'operazione.
- **Operazione Quoziente (Pag 20):** Se $\mathcal{R}$ è una congruenza su $(S, \perp)$, allora è possibile definire un'operazione $\perp_{\mathcal{R}}$ sull'insieme quoziente $S/\mathcal{R}$ in modo **ben definito**:

$$[a]_{\mathcal{R}} \perp_{\mathcal{R}} [b]_{\mathcal{R}} = [a \perp b]_{\mathcal{R}}$$

  - **Ben definita (Pag 21):** Se scegliamo altri rappresentanti $[a]_{\mathcal{R}} = [c]_{\mathcal{R}}$ (cioè $a \mathcal{R} c$) e $[b]_{\mathcal{R}} = [d]_{\mathcal{R}}$ (cioè $b \mathcal{R} d$), il risultato non deve cambiare: $[a \perp b]_{\mathcal{R}}$ deve essere uguale a $[c \perp d]_{\mathcal{R}}$. Questo è garantito dalla definizione di congruenza: $a \mathcal{R} c \wedge b \mathcal{R} d \implies (a \perp b) \mathcal{R} (c \perp d)$, che significa proprio $[a \perp b]_{\mathcal{R}} = [c \perp d]_{\mathcal{R}}$.
- **Esempi (Pag 19, 22):** Sia $(\mathbb{Z}, +)$.
  - $\mathcal{R}_1$: $a \mathcal{R}_1 b \iff a, b$ entrambi positivi o entrambi negativi (o zero?). a, b hanno lo stesso segno (considerando 0 a parte?).
    - È una congruenza rispetto a $+$?
    - $-1 \mathcal{R}_1 -5$. $3 \mathcal{R}_1 2$.
    - Dovrebbe valere $(-1+3) \mathcal{R}_1 (-5+2)$, cioè $2 \mathcal{R}_1 -3$.
    - Ma 2 è positivo e -3 è negativo. Non sono in relazione $\mathcal{R}_1$.
    - Quindi $\mathcal{R}_1$ **non è una congruenza** rispetto a $+$.
  - $\mathcal{R}_2$: $a \mathcal{R}_2 b \iff a, b$ entrambi pari o entrambi dispari (stessa parità).
    - È una congruenza rispetto a $+$?
    - Supponiamo $a \mathcal{R}_2 c$ (stessa parità) e $b \mathcal{R}_2 d$ (stessa parità).
    - Dobbiamo verificare $(a+b) \mathcal{R}_2 (c+d)$ (cioè $a+b$ e $c+d$ hanno la stessa parità).
      - Se a,c pari e b,d pari: a+b pari, c+d pari. OK.
      - Se a,c pari e b,d dispari: a+b dispari, c+d dispari. OK.
      - Se a,c dispari e b,d pari: a+b dispari, c+d dispari. OK.
      - Se a,c dispari e b,d dispari: a+b pari, c+d pari. OK.
    - **SÌ, $\mathcal{R}_2$ è una congruenza** rispetto a $+$.
  - È una congruenza rispetto a $\cdot$?
    - Supponiamo $a \mathcal{R}_2 c$ e $b \mathcal{R}_2 d$. Dobbiamo verificare $(a \cdot b) \mathcal{R}_2 (c \cdot d)$.
      - Se a,c pari: ab pari, cd pari. OK.
      - Se a,c dispari e b,d pari: ab pari, cd pari. OK.
      - Se a,c dispari e b,d dispari: ab dispari, cd dispari. OK.
    - **SÌ, $\mathcal{R}_2$ è una congruenza** rispetto a $\cdot$.

Relazione di congruenza Operazione quoziente

3.1 Congruenza Modulo m in $\mathbb{Z}$ (Pag 23-26)

Un esempio fondamentale di congruenza.

- Sia $m \in \mathbb{Z}$ un intero fissato. Definiamo la relazione $a \equiv b \pmod{m}$ (si legge "a congruo b modulo m") come:

$$a \equiv b \pmod{m} \iff m \mid (a-b)$$

  (cioè, m divide la differenza tra a e b; equivalente a $a - b = m \cdot h$ per qualche $h \in \mathbb{Z}$).
- **Teorema:** La congruenza modulo m è una **relazione di equivalenza** su $\mathbb{Z}$.
  - **Dimostrazione (Pag 23-24):**
    1. **Riflessiva:** $\forall a \in \mathbb{Z}$. $a - a = 0$. Poiché $m \mid 0$ (perché $0 = m \cdot 0$), vale $a \equiv a \pmod{m}$. **SÌ**.
    2. **Simmetrica:** Supponiamo $a \equiv b \pmod{m}$. Allora $m \mid (a-b)$. Questo significa $a - b = mh$. Allora $b - a = -(a-b) = m(-h)$. Poiché $-h \in \mathbb{Z}$, $m \mid (b-a)$. Quindi $b \equiv a \pmod{m}$. **SÌ**.
    3. **Transitiva:** Supponiamo $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$. Allora $m \mid (a-b)$ e $m \mid (b-c)$. Cioè $a - b = mh$ e $b - c = mk$ per $h, k \in \mathbb{Z}$. Sommiamo le due equazioni: $(a-b) + (b-c) = mh + mk$. $a - c = m(h+k)$. Poiché $h + k \in \mathbb{Z}$, $m \mid (a-c)$. Quindi $a \equiv c \pmod{m}$. **SÌ**.
- **Casi Speciali (Pag 25):**
  - Se $m = 0$: $a \equiv b \pmod{0} \iff 0 \mid (a-b)$. L'unico multiplo di 0 è 0 stesso. Quindi $a - b = 0 \iff a = b$. La congruenza modulo 0 è la **relazione di uguaglianza**.
  - Se $m = 1$: $a \equiv b \pmod{1} \iff 1 \mid (a-b)$. Poiché 1 divide qualsiasi intero, questo è sempre vero. La congruenza modulo 1 è la **relazione totale**.
  - $a \equiv b \pmod{m} \iff a \equiv b \pmod{-m}$. (Perché $m \mid (a-b) \iff -m \mid (a-b)$). Possiamo quindi considerare solo $m \geq 0$.

Legame con il Resto della Divisione Euclidea (per $m \geq 2$) (Pagine 26-27)

Prima di enunciare il teorema, ricordiamo brevemente la **Divisione Euclidea**:
Per ogni intero a (dividendo) e ogni intero $m \geq 1$ (divisore), esistono **unici** interi q (quoziente) e r (resto) tali che:

$$a = m \cdot q + r$$

e

$$0 \leq r < m$$

Il valore r è denotato come $\text{rest}(a, m)$.

Equivalenza tra Congruenza Modulo m e Uguaglianza dei Resti (Pag 26)

Siano $a, b \in \mathbb{Z}$ e $m \in \mathbb{Z}$ con $m \geq 2$. Allora:

$$a \equiv b \pmod{m} \iff \text{rest}(a, m) = \text{rest}(b, m)$$

In altre parole, due interi sono congrui modulo m se e solo se hanno lo stesso resto nella divisione euclidea per m.

Dimostrazione:

- **Parte 1: ($\implies$) Dimostriamo che se $a \equiv b \pmod{m}$, allora $\text{rest}(a, m) = \text{rest}(b, m)$.**
  1. **Ipotesi:** $a \equiv b \pmod{m}$.
     Per definizione, questo significa che $m \mid (a - b)$, quindi esiste un intero h tale che $a - b = m \cdot h$.
  2. **Divisione Euclidea per a e b:**
     Sia $r_1 = \text{rest}(a, m)$ e $r_2 = \text{rest}(b, m)$.
     Allora possiamo scrivere $a = mq_1 + r_1$ e $b = mq_2 + r_2$, dove q_1, q_2 sono i rispettivi quozienti e $0 \leq r_1 < m$, $0 \leq r_2 < m$.
  3. **Sostituzione nell'ipotesi:**
     Sostituiamo le espressioni di a e b nell'equazione $a - b = mh$:
     $(mq_1 + r_1) - (mq_2 + r_2) = mh$
  4. **Riorganizzazione algebrica:**
     $mq_1 + r_1 - mq_2 - r_2 = mh$
     $m(q_1 - q_2) + (r_1 - r_2) = mh$
  5. **Isoliamo la differenza dei resti $(r_1 - r_2)$:**
     $r_1 - r_2 = mh - m(q_1 - q_2)$
     $r_1 - r_2 = m(h - q_1 + q_2)$.
     Poiché h, q_1, q_2 sono interi, anche $k = (h - q_1 + q_2)$ è un intero. Quindi, $r_1 - r_2 = mk$.
     Questo mostra che $m \mid (r_1 - r_2)$ (cioè, $r_1 - r_2$ è un multiplo di m).
  6. **Consideriamo i limiti per la differenza $r_1 - r_2$:**
     Sappiamo che $0 \leq r_1 < m$ e $0 \leq r_2 < m$.
     Per trovare l'intervallo di $r_1 - r_2$:
     - Il valore massimo di r_1 è $m - 1$, il valore minimo di r_2 è 0. Quindi $r_1 - r_2 \leq (m - 1) - 0 = m - 1$.
     - Il valore minimo di r_1 è 0, il valore massimo di r_2 è $m - 1$. Quindi $r_1 - r_2 \geq 0 - (m - 1) = -(m - 1) = 1 - m$.
       Dunque, $-(m - 1) \leq r_1 - r_2 \leq m - 1$. Questo significa che $-m < r_1 - r_2 < m$.
  7. **Conclusione per la Parte 1:**
     Abbiamo stabilito che $r_1 - r_2$ è un multiplo di m e che $-m < r_1 - r_2 < m$.
     L'unico multiplo di m che si trova strettamente tra $-m$ e m è $0 \cdot m = 0$.
     Pertanto, deve essere $r_1 - r_2 = 0$, il che implica $r_1 = r_2$.
     Quindi, $\text{rest}(a, m) = \text{rest}(b, m)$.
- **Parte 2: ($\impliedby$) Dimostriamo che se $\text{rest}(a, m) = \text{rest}(b, m)$, allora $a \equiv b \pmod{m}$.**
  1. **Ipotesi:** $\text{rest}(a, m) = \text{rest}(b, m)$. Chiamiamo r questo resto comune, con $0 \leq r < m$.
  2. **Divisione Euclidea per a e b:**
     Possiamo scrivere $a = mq_1 + r$ per qualche intero q_1.
     E possiamo scrivere $b = mq_2 + r$ for qualche intero q_2.
  3. **Calcoliamo la differenza $a - b$:**
     $a - b = (mq_1 + r) - (mq_2 + r)$
     $a - b = mq_1 + r - mq_2 - r$
     $a - b = mq_1 - mq_2$
  4. **Mettiamo m in evidenza:**
     $a - b = m(q_1 - q_2)$.
  5. **Conclusione per la Parte 2:**
     Poiché q_1 e q_2 sono interi, la loro differenza $k = (q_1 - q_2)$ è anch'essa un intero.
     Quindi, $a - b = mk$, il che significa che $a - b$ è un multiplo di m.
     Per definizione di divisibilità, $m \mid (a - b)$.
     E per definizione di congruenza, $a \equiv b \pmod{m}$.

Avendo dimostrato entrambe le direzioni ($\implies$) e ($\impliedby$), il teorema è provato.

Implicazioni per le Classi di Equivalenza:
Questo teorema implica che le classi di equivalenza modulo m (per $m \geq 2$) sono determinate unicamente dal resto della divisione per m. Ci sono m resti possibili: $0, 1, \ldots, m-1$. Di conseguenza, ci sono esattamente m classi di equivalenza distinte modulo m, spesso denotate come $[0]_m, [1]_m, \ldots, [m-1]_m$. L'insieme di queste classi, $\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$, è l'insieme quoziente.

Congruenza Modulo m come Relazione di Congruenza

La relazione di congruenza modulo m non è solo una relazione di equivalenza, ma è anche una **congruenza** rispetto alle operazioni di addizione e moltiplicazione definite su $\mathbb{Z}$. Questo è un risultato cruciale.

Compatibilità della Congruenza Modulo m con Addizione e Moltiplicazione

Siano $a, b, c, d \in \mathbb{Z}$ e $m \in \mathbb{Z}$ con $m \neq 0$. Se

- $a \equiv c \pmod{m}$
- $b \equiv d \pmod{m}$

Allora valgono le seguenti proprietà:

1. **Compatibilità con l'Addizione:**
$$a + b \equiv c + d \pmod{m}$$
2. **Compatibilità con la Moltiplicazione:**
$$a \cdot b \equiv c \cdot d \pmod{m}$$

Dimostrazione:

1. **Dimostrazione della Compatibilità con l'Addizione:**
   - **Ipotesi:**
     - $a \equiv c \pmod{m} \implies m \mid (a-c) \implies a - c = k_1 m$ per qualche $k_1 \in \mathbb{Z}$.
     - $b \equiv d \pmod{m} \implies m \mid (b-d) \implies b - d = k_2 m$ per qualche $k_2 \in \mathbb{Z}$.
   - **Tesi:** Dobbiamo dimostrare che $a + b \equiv c + d \pmod{m}$, cioè che $m \mid ((a+b) - (c+d))$.
   - Consideriamo la differenza $(a+b) - (c+d)$:
     $(a+b) - (c+d) = a + b - c - d = (a-c) + (b-d)$.
   - Sostituiamo le espressioni dalle ipotesi:
     $(a-c) + (b-d) = k_1 m + k_2 m$.
   - Mettiamo m in evidenza:
     $k_1 m + k_2 m = m(k_1 + k_2)$.
   - Poiché $k_1, k_2 \in \mathbb{Z}$, anche $(k_1 + k_2) \in \mathbb{Z}$.
   - Quindi, $(a+b) - (c+d)$ è un multiplo di m.
   - Questo significa $m \mid ((a+b) - (c+d))$, e dunque $a + b \equiv c + d \pmod{m}$.
     La compatibilità con l'addizione è dimostrata.
2. **Dimostrazione della Compatibilità con la Moltiplicazione:**
   - **Ipotesi:** (Come sopra)
     - $a - c = k_1 m \implies a = c + k_1 m$.
     - $b - d = k_2 m \implies b = d + k_2 m$.
   - **Tesi:** Dobbiamo dimostrare che $a \cdot b \equiv c \cdot d \pmod{m}$, cioè che $m \mid (ab - cd)$.
   - Consideriamo la differenza $ab - cd$. Usiamo un trucco: aggiungere e sottrarre bc (o ad):
     $ab - cd = ab - bc + bc - cd$.
   - Raccogliamo:
     $ab - bc + bc - cd = b(a-c) + c(b-d)$.
   - Sostituiamo le espressioni dalle ipotesi:
     $b(k_1 m) + c(k_2 m)$.
   - Mettiamo m in evidenza:
     $m(bk_1 + ck_2)$.
   - Poiché $b, k_1, c, k_2 \in \mathbb{Z}$, anche $(bk_1 + ck_2) \in \mathbb{Z}$.
   - Quindi, $ab - cd$ è un multiplo di m.
   - Questo significa $m \mid (ab - cd)$, e dunque $a \cdot b \equiv c \cdot d \pmod{m}$.
     La compatibilità con la moltiplicazione è dimostrata.

Questa proprietà di essere una congruenza è ciò che permette di definire in modo **ben definito** le operazioni di somma e prodotto sull'insieme quoziente $\mathbb{Z}_m = \mathbb{Z}/\equiv_m$ (l'insieme delle classi di resto modulo m). Si definisce:

- $[a]_m + [b]_m = [a+b]_m$
- $[a]_m \cdot [b]_m = [a \cdot b]_m$

L'insieme $\mathbb{Z}_m$ con queste operazioni forma una nuova e fondamentale struttura algebrica (un anello commutativo unitario).

Congruenza (teoria dei numeri) Aritmetica modulare Anello Zn

Riepilogo Veloce Lezione 12

- Il **Teorema Fondamentale** stabilisce una corrispondenza 1:1 tra **relazioni di equivalenza** su S e **partizioni** di S. La partizione associata a $\mathcal{R}$ è l'insieme quoziente $S/\mathcal{R}$. La relazione associata a $\mathcal{F}$ è $x\mathcal{R}_{\mathcal{F}}y \iff x, y$ appartengono allo stesso blocco di $\mathcal{F}$.
- Ogni **funzione** $f: S \to T$ induce una relazione di equivalenza $\mathcal{R}_f$ su S ($x\mathcal{R}_f y \iff f(x) = f(y)$).
- Esiste una **mappa quoziente iniettiva** $\bar{f}: S/\mathcal{R}_f \to T$ tale che $\bar{f}([a]) = f(a)$.
- Una **congruenza** è una relazione di equivalenza compatibile con un'operazione algebrica.
- La **congruenza modulo m** ($a \equiv b \pmod m \iff m \mid (a-b)$) è una relazione di equivalenza su $\mathbb{Z}$.
- Per $m \geq 2$, $a \equiv b \pmod m \iff \text{rest}(a,m) = \text{rest}(b,m)$.

Prossimi Passi

- Assicurati di aver compreso il legame tra relazioni di equivalenza, classi di equivalenza e partizioni.
- Rifletti su come la relazione indotta da una funzione "raggruppa" gli elementi del dominio che hanno la stessa immagine.
- La congruenza modulo m è fondamentale. Il prossimo passo sarà studiare la struttura dell'insieme quoziente $\mathbb{Z}_m$ (l'anello delle classi di resto modulo m).

Lezione 13: Congruenze Modulo m e Anelli Quoziente Zn

Data: 06/05/2025 (come da note)
Argomenti: Congruenze in Z, Compatibilità con somma e prodotto, Anello Quoziente Zm, Classi di Resto, Tavole di Cayley per Zm, Campi Zm (quando m è primo), Caratteristica di Zm, Invertibili e Divisori dello Zero in Zm (legame con MCD), Elementi Nilpotenti in Zm, Equazioni Congruenziali, Algoritmo Euclideo Esteso, Esercizi.

#tag/number-theory #tag/congruences #tag/modular-arithmetic #tag/rings #tag/quotient-rings #tag/fields #tag/zero-divisor #tag/nilpotent #tag/euclidean-algorithm #tag/algebra-avanzata

---

1. Congruenze in $\mathbb{Z}$

Introduciamo una relazione fondamentale sull'insieme degli interi $\mathbb{Z}$.

- **Definizione:** Sia $m \in \mathbb{Z}$ un intero fissato (chiamato **modulo**). Dati $a, b \in \mathbb{Z}$, diciamo che a è **congruo** a b modulo m, e scriviamo $a \equiv b \pmod m$ (o $a \pmod m b$), se m divide la differenza $(a-b)$.

$$a \equiv b \pmod m \iff m \mid (a-b)$$

  - Questo significa che esiste un intero $k \in \mathbb{Z}$ tale che $a - b = m \cdot k$.
  - Nota: La relazione di congruenza modulo m è la stessa della congruenza modulo $-m$, quindi possiamo solitamente assumere $m \geq 0$.
- **Casi Particolari:**
  - **m = 0:** $a \equiv b \pmod 0 \iff 0 \mid (a-b)$. L'unico multiplo di 0 è 0 stesso. Quindi $a - b = 0 \iff a = b$. La congruenza modulo 0 è semplicemente l'**uguaglianza**.
  - **m = 1:** $a \equiv b \pmod 1 \iff 1 \mid (a-b)$. Poiché 1 divide qualsiasi intero, questa relazione è **sempre vera** per ogni $a, b \in \mathbb{Z}$. È la relazione totale.
- **Equivalenza con i Resti (per m $\geq$ 2):**
  Sia $m \geq 2$. Allora $a \equiv b \pmod m$ se e solo se a e b hanno lo **stesso resto** nella divisione euclidea per m.

$$a \equiv b \pmod m \iff \text{rest}(a,m) = \text{rest}(b,m)$$

  - **Dimostrazione (cenno):**
    - ($\implies$) Se $a \equiv b \pmod m$, allora $a - b = mk$. Siano $a = mq_a + r_a$ e $b = mq_b + r_b$ con $0 \leq r_a, r_b < m$. Allora $a - b = m(q_a - q_b) + (r_a - r_b)$. Poiché $a - b = mk$, abbiamo $mk = m(q_a - q_b) + (r_a - r_b)$, quindi $r_a - r_b = m(k - q_a + q_b)$. Dato che $0 \leq r_a, r_b < m$, si ha $-m < r_a - r_b < m$. L'unico multiplo di m in questo intervallo è 0. Quindi $r_a - r_b = 0$, cioè $r_a = r_b$.
    - ($\impliedby$) Se $r_a = r_b$, allora $a = mq_a + r_a$ e $b = mq_b + r_a$. $a - b = m(q_a - q_b)$. Quindi $m \mid (a-b)$, cioè $a \equiv b \pmod m$.

- **Proprietà:** Per un m fissato, la relazione $\equiv \pmod m$ è una **relazione di equivalenza** su $\mathbb{Z}$ (è riflessiva, simmetrica, transitiva).

Congruenza (teoria dei numeri) Divisione Euclidea Relazione di equivalenza

---

2. Compatibilità della Congruenza con le Operazioni

La relazione di congruenza si "comporta bene" rispetto alla somma e al prodotto in $\mathbb{Z}$.

- **Compatibilità con la Somma (Pag 2):**
  Se $a \equiv c \pmod m$ e $b \equiv d \pmod m$, allora $(a+b) \equiv (c+d) \pmod m$.
  - **Dimostrazione:**
    - $a \equiv c \pmod m \implies a - c = m \cdot h$ per qualche $h \in \mathbb{Z}$.
    - $b \equiv d \pmod m \implies b - d = m \cdot k$ per qualche $k \in \mathbb{Z}$.
    - Sommiamo le due equazioni: $(a-c) + (b-d) = mh + mk$.
    - Riorganizziamo: $(a+b) - (c+d) = m(h+k)$.
    - Poiché $h+k \in \mathbb{Z}$, questo significa $m \mid ((a+b) - (c+d))$.
    - Quindi, $(a+b) \equiv (c+d) \pmod m$.
- **Compatibilità con il Prodotto (Pag 3):**
  Se $a \equiv c \pmod m$ e $b \equiv d \pmod m$, allora $(a \cdot b) \equiv (c \cdot d) \pmod m$.
  - **Dimostrazione:**
    - $a = c + mh$
    - $b = d + mk$
    - Moltiplichiamo: $a \cdot b = (c+mh)(d+mk) = cd + cmk + mhd + m^2hk$.
    - $ab = cd + m(ck + hd + mhk)$.
    - $ab - cd = m(ck + hd + mhk)$.
    - Poiché $(ck + hd + mhk) \in \mathbb{Z}$, questo significa $m \mid (ab - cd)$.
    - Quindi, $ab \equiv cd \pmod m$.

> **La compatibilità della congruenza con somma e prodotto è ciò che permette di definire le operazioni sull'insieme quoziente $\mathbb{Z}_m$.**

---

3. L'Anello Quoziente $\mathbb{Z}_m$

L'insieme delle classi di equivalenza della congruenza modulo m.

- **Classe di Resto (o di Congruenza) (Pag 5):** Dato $a \in \mathbb{Z}$ e $m \geq 1$, la classe di resto di a modulo m è l'insieme di tutti gli interi congrui ad a modulo m:

$$[a]_m = \{b \in \mathbb{Z} \mid b \equiv a \pmod m\} = \{a + mk \mid k \in \mathbb{Z}\}$$

  - Proprietà: $[a]_m = [b]_m \iff a \equiv b \pmod m$.
  - Se $r_a = \text{rest}(a, m)$, allora $[a]_m = [r_a]_m$. Ogni classe ha un unico rappresentante nell'intervallo $\{0, 1, \ldots, m-1\}$.
- **Insieme Quoziente $\mathbb{Z}_m$ (Pag 4, 6):** L'insieme di tutte le classi di resto modulo m.

$$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \{[a]_m \mid a \in \mathbb{Z}\}$$

  - Poiché ogni classe è rappresentata univocamente da un resto r con $0 \leq r < m$, possiamo scrivere:

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

  - La cardinalità è $|\mathbb{Z}_m| = m$.
- **Operazioni in $\mathbb{Z}_m$ (Pag 4):** Grazie alla compatibilità, possiamo definire somma e prodotto tra classi usando i rappresentanti:
  - **Somma:** $[a]_m + [b]_m = [a+b]_m$
  - **Prodotto:** $[a]_m \cdot [b]_m = [a \cdot b]_m$
  - Queste operazioni sono **ben definite**, cioè il risultato non dipende dalla scelta dei rappresentanti a e b all'interno delle loro classi.
- **Struttura Algebrica (Pag 4):** $(\mathbb{Z}_m, +, \cdot)$ è un **Anello Commutativo Unitario**.
  - L'elemento neutro additivo è $[0]_m$. L'opposto di $[a]_m$ è $[-a]_m = [m-a]_m$.
  - L'elemento neutro moltiplicativo (unità) è $[1]_m$ (per $m \geq 2$).
  - Associatività, commutatività e distributività seguono dalle proprietà corrispondenti in $\mathbb{Z}$.
- **Esempi (Pag 8):**
  - $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$. $[0]_2$ sono i pari, $[1]_2$ sono i dispari.

- $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$. $[0]_3 = \{\dots, -3, 0, 3, 6, \dots\}$, $[1]_3 = \{\dots, -2, 1, 4, 7, \dots\}$, $[2]_3 = \{\dots, -1, 2, 5, 8, \dots\}$.

Aritmetica modulare Classe di resto Anello quoziente

---

4. Tavole di Cayley ed Esempi $\mathbb{Z}_m$

- **Esempio $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ (Pag 9):** (Usiamo $\bar{a}$ come notazione per $[a]_4$)
  - **Tavola Additiva (+):**

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

    - $(\mathbb{Z}_4, +)$ è un gruppo abeliano.
  - **Tavola Moltiplicativa ($\cdot$):**

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

    - $(\mathbb{Z}_4, \cdot)$ è un monoide commutativo (unità $\bar{1}$).
    - **Divisori dello Zero:** $\bar{2} \cdot \bar{2} = \bar{0}$. Poiché $\bar{2} \neq \bar{0}$, $\bar{2}$ è un divisore dello zero.
    - **Elementi Nilpotenti:** $\bar{2}^2 = \bar{0}$. $\bar{2}$ è nilpotente.
    - **Elementi Invertibili:** Solo $\bar{1}$ e $\bar{3}$ hanno inverso ($\bar{1}^{-1} = \bar{1}$, $\bar{3}^{-1} = \bar{3}$ perché $\bar{3} \cdot \bar{3} = \bar{9} = \bar{1}$). $U(\mathbb{Z}_4) = \{\bar{1}, \bar{3}\}$.
    - **Cancellabilità:** $\bar{2}$ non è cancellabile (es. $\bar{2} \cdot \bar{1} = \bar{2}$ e $\bar{2} \cdot \bar{3} = \bar{6} = \bar{2}$, ma $\bar{1} \neq \bar{3}$).
- **Esempio $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ (Pag 10):**
  - **Tavola Moltiplicativa ($\cdot$):**

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

  - **Osservazioni:**
    - Non ci sono divisori dello zero (a parte $\bar{0}$). Ogni riga/colonna non nulla contiene $\bar{0}$ solo nella prima posizione.
    - Tutti gli elementi non nulli $\{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ sono invertibili: $\bar{1}^{-1} = \bar{1}$, $\bar{2}^{-1} = \bar{3}$, $\bar{3}^{-1} = \bar{2}$, $\bar{4}^{-1} = \bar{4}$.
    - $U(\mathbb{Z}_5) = \mathbb{Z}_5 \setminus \{\bar{0}\}$.

---

5. Campi $\mathbb{Z}_m$ e Caratteristica

Teorema: $\mathbb{Z}_m$ è un Campo se e solo se m è Primo

- **Enunciato (Pag 11):** L'anello $(\mathbb{Z}_m, +, \cdot)$ è un **campo** se e solo se m è un numero **primo**.
- **Idea Chiave:** Questo risultato collega la struttura algebrica di $\mathbb{Z}_m$ (essere un campo, dove la divisione per elementi non nulli è sempre possibile) a una proprietà fondamentale del modulo m (essere primo).
- **Spiegazione (legata al Capitolo 6):** La dimostrazione completa si basa sulla caratterizzazione degli elementi invertibili in $\mathbb{Z}_m$. Un anello commutativo unitario è un campo se e solo se ogni suo elemento non nullo è invertibile. Come vedremo, un elemento $[a]_m$ (con $a \not\equiv 0 \pmod m$) è invertibile in $\mathbb{Z}_m$ se e solo se $\text{MCD}(a, m) = 1$.
  Quindi, $\mathbb{Z}_m$ è un campo
  $\iff$ ogni $[a]_m$ con $a \in \{1, 2, \dots, m-1\}$ è invertibile
  $\iff$ per ogni $a \in \{1, 2, \dots, m-1\}$, si ha $\text{MCD}(a, m) = 1$
  $\iff$ m non ha divisori propri (diversi da 1 e se stesso)
  $\iff$ m è un numero primo.
- **Esempi:** $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \mathbb{Z}_{11}, \dots$ sono campi. $\mathbb{Z}_4, \mathbb{Z}_6, \mathbb{Z}_8, \mathbb{Z}_9, \mathbb{Z}_{10}, \dots$ non sono campi.

Caratteristica di $\mathbb{Z}_m$

- **Definizione (Pag 11-12):** La **caratteristica** di un anello unitario R, indicata con $char(R)$, è il più piccolo intero positivo k tale che la somma di k copie dell'elemento neutro moltiplicativo 1_R sia uguale all'elemento neutro additivo 0_R. Se un tale k non esiste, la caratteristica è 0.
- **Proposizione:** Per ogni $m \geq 1$, la caratteristica dell'anello $\mathbb{Z}_m$ è m.

$$char(\mathbb{Z}_m) = m$$

- **Dimostrazione:**
  1. L'elemento neutro moltiplicativo (unità) in $\mathbb{Z}_m$ è $[1]_m$.
  2. L'elemento neutro additivo (zero) in $\mathbb{Z}_m$ è $[0]_m$.
  3. Dobbiamo trovare il più piccolo intero positivo k tale che:

$$\underbrace{[1]_m + [1]_m + \cdots + [1]_m}_{k \text{ volte}} = [0]_m$$

  4. Per la definizione di somma in $\mathbb{Z}_m$, il lato sinistro è uguale a $[1 + 1 + \cdots + 1]_m = [k]_m$.
  5. Quindi, cerchiamo il più piccolo intero positivo k tale che $[k]_m = [0]_m$.
  6. La condizione $[k]_m = [0]_m$ è equivalente a $k \equiv 0 \pmod{m}$.
  7. Questo significa che m deve dividere k.
  8. Il più piccolo intero *positivo* k che è divisibile per m è proprio m stesso (assumendo $m \geq 1$).
  9. Pertanto, $char(\mathbb{Z}_m) = m$.

Campo finito Caratteristica (algebra)

---

6. Invertibili e Divisori dello Zero in $\mathbb{Z}_m$

Sia $m \geq 2$. Consideriamo $\bar{a} \in \mathbb{Z}_m$ con $\bar{a} \neq \bar{0}$.

- **Proposizione (Pag 13):**
  1. $\bar{a}$ è un **divisore dello zero** in $\mathbb{Z}_m \iff \text{MCD}(a, m) > 1$.
  2. $\bar{a}$ è **invertibile** in $\mathbb{Z}_m \iff \text{MCD}(a, m) = 1$.
- **Dimostrazione 1 ($\Longleftarrow$):** Se $d = \text{MCD}(a, m) > 1$. Allora $a = d \cdot a_1$ e $m = d \cdot m_1$ con $1 \leq m_1 < m$. Consideriamo $\bar{b} = \bar{m_1}$. Poiché $m_1 < m$, $\bar{m_1} \neq \bar{0}$. Calcoliamo $\bar{a} \cdot \bar{b} = \bar{a} \cdot \bar{m_1} = \overline{a \cdot m_1} = \overline{(da_1)m_1} = \overline{a_1(dm_1)} = \overline{a_1 m} = \bar{0}$. Abbiamo trovato $\bar{b} \neq \bar{0}$ tale che $\bar{a}\bar{b} = \bar{0}$. Quindi $\bar{a}$ è divisore dello zero.
  - **Esempio (Pag 15):** $\bar{6} \in \mathbb{Z}_{15}$. $\text{MCD}(6, 15) = 3 > 1$. $m_1 = 15/3 = 5$. Allora $\bar{6} \cdot \bar{5} = \overline{30} = \bar{0}$ in $\mathbb{Z}_{15}$.
- **Dimostrazione 1 ($\Longrightarrow$):** Se $\bar{a}$ è divisore dello zero, esiste $\bar{b} \neq \bar{0}$ tale che $\bar{a}\bar{b} = \bar{0}$. Questo significa $ab \equiv 0 \pmod{m}$, cioè $m \mid ab$. Se fosse $\text{MCD}(a, m) = 1$, allora per una proprietà della divisibilità (generalizzazione Lemma Euclide), dovremmo avere $m \mid b$. Ma se $m \mid b$, allora $\bar{b} = \bar{0}$, che contraddice l'ipotesi $\bar{b} \neq \bar{0}$. Quindi deve essere $\text{MCD}(a, m) > 1$.
- **Dimostrazione 2 ($\Longleftarrow$):** Se $\text{MCD}(a, m) = 1$. Per il **Teorema di Bézout**, esistono interi h, k tali che $a \cdot h + m \cdot k = 1$. Considerando questa equazione modulo m: $ah + mk \equiv 1 \pmod{m}$. Poiché $mk \equiv 0 \pmod{m}$, otteniamo $ah \equiv 1 \pmod{m}$. Questo significa $\bar{a} \cdot \bar{h} = \bar{1}$ in $\mathbb{Z}_m$. Quindi $\bar{h}$ è l'inverso di $\bar{a}$. $\bar{a}$ è invertibile.
- **Dimostrazione 2 ($\Longrightarrow$):** Se $\bar{a}$ è invertibile, esiste $\bar{b}$ tale che $\bar{a}\bar{b} = \bar{1}$. Questo significa $ab \equiv 1 \pmod{m}$, cioè $ab - 1 = mk$ per qualche k. Riscrivendo: $ab - mk = 1$. Questa è un'identità di Bézout. Poiché esiste una combinazione lineare di a e m che dà 1, il loro massimo comun divisore deve essere 1. $\text{MCD}(a, m) = 1$.
- **Osservazione (Pag 13):** In $\mathbb{Z}_m$, ogni elemento $\bar{a} \neq \bar{0}$ o è invertibile (se $\text{MCD}(a, m) = 1$) o è un divisore dello zero (se $\text{MCD}(a, m) > 1$).
- **Esempio $\mathbb{Z}_{15}$ (Pag 19):**
  - Invertibili: $\text{MCD}(a, 15) = 1$. $a \in \{1, 2, 4, 7, 8, 11, 13, 14\}$. $U(\mathbb{Z}_{15}) = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \overline{11}, \overline{13}, \overline{14}\}$.
  - Divisori dello Zero: $\text{MCD}(a, 15) > 1$. $a \in \{3, 5, 6, 9, 10, 12\}$. Divisori: $\{\bar{3}, \bar{5}, \bar{6}, \bar{9}, \overline{10}, \overline{12}\}$.

Gruppo moltiplicativo degli interi modulo n Teorema di Bézout

---

7. Elementi Nilpotenti in $\mathbb{Z}_m$

- **Proposizione (Pag 20):** Sia $m = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ la fattorizzazione in primi distinti di m. Sia $a = p_1^{\beta_1} \cdots p_t^{\beta_t}$ con $1 \leq \beta_i$ per ogni i (cioè a è multiplo di ogni primo che divide m). Allora $\bar{a} \in \mathbb{Z}_m$ è **nilpotente**. (Senza dimostrazione qui).
- **Esempio $\mathbb{Z}_{40}$ (Pag 21):** $40 = 2^3 \cdot 5^1$. Gli elementi nilpotenti (oltre a $\bar{0}$) sono multipli di $2 \cdot 5 = 10$. Quindi $\overline{10}, \overline{20}, \overline{30}$. Verifichiamo $\overline{10}$: $\overline{10}^2 = \overline{100} = \overline{2 \cdot 40 + 20} = \overline{20}$. $\overline{10}^3 = \overline{10} \cdot \overline{20} = \overline{200} = \overline{5 \cdot 40 + 0} = \bar{0}$. Sì. Verifichiamo $\overline{20}$: $\overline{20}^2 = \overline{400} = \overline{10 \cdot 40 + 0} = \bar{0}$. Sì.
- **Esempio $\mathbb{Z}_{162}$ (Pag 21):** $162 = 2 \cdot 81 = 2^1 \cdot 3^4$. Gli elementi nilpotenti (oltre a $\bar{0}$) sono multipli di $2 \cdot 3 = 6$. Es. $\bar{6}, \overline{12}, \overline{18}, \ldots$

Elemento Nilpotente

---

8. Equazioni Congruenziali

Risolvere equazioni della forma $\bar{a} \cdot X = \bar{b}$ in $\mathbb{Z}_m$.

- Equivalente a: $ax \equiv b \pmod{m}$.
- **Teorema di Risolubilità** (Pag 24):** L'equazione congruenziale $ax \equiv b \pmod{m}$ ammette soluzione $x \in \mathbb{Z}$ se e solo se $d \mid b$, dove $d = \text{MCD}(a, m)$.
  - Se la soluzione esiste, ci sono esattamente d soluzioni distinte modulo m.
  - Se $d = 1$ (cioè $\bar{a}$ è invertibile in $\mathbb{Z}_m$), la soluzione è unica modulo m ed è data da $x \equiv a^{-1}b \pmod{m}$.
- **Esempio** $2x \equiv 5 \pmod{10}$ **(Pag 23):** $\text{MCD}(2, 10) = 2$. Poiché $2 \nmid 5$, non ci sono soluzioni.
- **Esempio** $2x \equiv 6 \pmod{8}$ **(Pag 23):** $\text{MCD}(2, 8) = 2$. Poiché $2 \mid 6$, ci sono soluzioni (esattamente 2). Dividendo tutto per $d = 2$: $x \equiv 3 \pmod{4}$. Le soluzioni sono $x \equiv 3 \pmod{8}$ e $x \equiv 3 + 4 = 7 \pmod{8}$. Soluzioni in $\mathbb{Z}_8$: $\{\bar{3}, \bar{7}\}$.
- **Esempio** $21x \equiv 10 \pmod{64}$ **(Pag 25):**
  1. Calcoliamo $d = \text{MCD}(21, 64)$.
     - $64 = 3 \cdot 21 + 1$.
     - $21 = 21 \cdot 1 + 0$.
     - $d = 1$.
  2. Poiché $d = 1$ divide $b = 10$, esiste una soluzione unica modulo 64.
  3. Dobbiamo trovare l'inverso di 21 modulo 64. Usiamo l'algoritmo esteso a ritroso:
     - $1 = 64 - 3 \cdot 21$.
     - Questa è già nella forma $ah + mk = 1$ con $a = 21, m = 64$. Abbiamo $h = -3, k = 1$.
     - L'inverso di $\overline{21}$ in $\mathbb{Z}_{64}$ è $\bar{h} = \overline{-3}$.
     - $\overline{-3} \equiv \overline{-3 + 64} = \overline{61}$. Quindi $\overline{21}^{-1} = \overline{61}$.
  4. La soluzione è $x \equiv a^{-1}b \pmod{m}$:
     - $x \equiv 61 \cdot 10 \pmod{64}$
     - $x \equiv 610 \pmod{64}$.
     - Dividiamo 610 per 64: $610 = 9 \cdot 64 + 34$. $(9 \times 64 = 576)$.
     - $x \equiv 34 \pmod{64}$.
  - Soluzione: $X = \overline{34}$ in $\mathbb{Z}_{64}$.

Equazione congruenziale lineare Algoritmo di Euclide Esteso

8.1 Esistenza e Numero delle Soluzioni

Guida Passo-Passo per Risolvere $ax \equiv b \pmod{m}$

1. **Identifica i Valori:**
   - Scrivi chiaramente i valori di a, b e m dalla tua equazione.
2. **Calcola il MCD:**
   - Calcola $d = \gcd(a, m)$ (il Massimo Comun Divisore tra a e m). Puoi usare l'Algoritmo di Euclide.
3. **Verifica l'Esistenza delle Soluzioni:**
   - **Se** d **non divide** b **(**$d \nmid b$**):** L'equazione **non ha soluzioni**. Fermati qui.
   - **Se** d **divide** b **(**$d \mid b$**):** L'equazione ha esattamente d **soluzioni distinte modulo** m. Procedi al passo successivo.
4. **Risolvi l'Equazione (se esistono soluzioni):**

   CASO A: $d = 1$ **(Soluzione Unica Modulo** m**)**

   - L'equazione è $ax \equiv b \pmod{m}$ con $\gcd(a, m) = 1$.
   - **Passo A1: Trova l'inverso di** a **modulo** m**.**
     - Usa l'Algoritmo di Euclide Esteso per trovare due interi s e t tali che $as + mt = 1$.
     - Da questa equazione, $as \equiv 1 \pmod{m}$. Quindi, l'inverso di a modulo m è $a^{-1} \equiv s \pmod{m}$.
     - Assicurati che s sia il rappresentante positivo più piccolo (tra 0 e $m - 1$). Se s è negativo, aggiungi m finché non diventa positivo. Se $s > m - 1$, prendi il resto $s \pmod{m}$.
   - **Passo A2: Calcola la soluzione.**
     - La soluzione unica è $x \equiv a^{-1} \cdot b \pmod{m}$.
   - **Passo A3: Riduci il risultato.**
     - Calcola il valore di $a^{-1} \cdot b$ e poi riducilo modulo m per ottenere la soluzione x_0 nell'intervallo $[0, m - 1]$.

   CASO B: $d > 1$ **(**d **Soluzioni Distinte Modulo** m**)**

   - L'equazione è $ax \equiv b \pmod{m}$ con $\gcd(a, m) = d > 1$ e $d \mid b$.
   - **Passo B1: Semplifica l'equazione.**
     - Dividi a, b e m per d:

- $a' = a/d$
- $b' = b/d$
- $m' = m/d$
- La nuova equazione (equivalente) è $a'x \equiv b' \pmod{m'}$.
- *Importante:* Ora, $\gcd(a', m') = 1$.

- **Passo B2: Risolvi l'equazione semplificata.**
  - Risolvi $a'x \equiv b' \pmod{m'}$ usando la procedura del **CASO A** (trova l'inverso di a' modulo m', moltiplica per b', riduci modulo m').
  - Chiama la soluzione di questa equazione semplificata x_0. Quindi $x_0 \equiv (a')^{-1}b' \pmod{m'}$. Assicurati che x_0 sia nell'intervallo $[0, m' - 1]$.
- **Passo B3: Trova tutte le d soluzioni modulo m.**
  - La prima soluzione (modulo m) è x_0.
  - Le altre $d - 1$ soluzioni si ottengono aggiungendo multipli di m' a x_0:
    $x_1 = x_0 + m'$
    $x_2 = x_0 + 2m'$
    ...
    $x_{d-1} = x_0 + (d-1)m'$
  - Tutte queste d soluzioni $(x_0, x_1, \ldots, x_{d-1})$ sono le soluzioni distinte modulo m dell'equazione originale.

5. **Verifica (Opzionale ma Consigliato):**
   - Sostituisci ciascuna delle soluzioni trovate nell'equazione originale $ax \equiv b \pmod{m}$ per assicurarti che la congruenza sia soddisfatta.

---

9. Esercizi Assegnati (Pag 26 e Foto)

Esercizio 1 (Pag 26)

Determinare gli elementi invertibili, i divisori dello zero e gli elementi nilpotenti di $\mathbb{Z}_{40}$.
Suggerimento: $40 = 2^3 \cdot 5$. Usare le proposizioni basate su $\text{MCD}(a, 40)$ e sulla fattorizzazione.

Esercizio 2 (Pag 26)

Determinare l'inverso di $\bar{25}$ in $\mathbb{Z}_{192}$.
Suggerimento: Calcolare $\text{MCD}(25, 192)$ con l'algoritmo di Euclide. Se è 1, usare l'algoritmo esteso a ritroso per trovare l'identità di Bézout $25h + 192k = 1$. L'inverso sarà $\bar{h}$.

Esercizio 3 (dalla Foto 1)

Calcolare l'inverso di $\bar{16}$ in $\mathbb{Z}_{125}$.
Suggerimento: Calcolare $\text{MCD}(16, 125)$ e usare l'algoritmo esteso.

Esercizio 4 (dalla Foto 1)

Calcolare l'inverso di $\bar{17}$ in $\mathbb{Z}_{42}$.
Suggerimento: Calcolare $\text{MCD}(17, 42)$ e usare l'algoritmo esteso.

Riepilogo Veloce Lezione 13

- Abbiamo definito la **congruenza modulo m** e visto la sua compatibilità con somma e prodotto.
- Abbiamo costruito l'**anello quoziente** $(\mathbb{Z}_m, +, \cdot)$ delle classi di resto.
- Abbiamo visto che $\mathbb{Z}_m$ è un **campo** $\iff$ m è primo.
- Abbiamo determinato la **caratteristica** di $\mathbb{Z}_m$.
- Abbiamo caratterizzato gli elementi **invertibili** $(\text{MCD}(a, m) = 1)$ e i **divisori dello zero** $(\text{MCD}(a, m) > 1)$ in $\mathbb{Z}_m$.
- Abbiamo introdotto gli elementi **nilpotenti** in $\mathbb{Z}_m$.
- Abbiamo studiato le **equazioni congruenziali** $ax \equiv b \pmod{m}$ e il teorema sulla loro risolubilità.

Prossimi Passi

- Fai pratica con l'algoritmo di Euclide esteso per trovare gli inversi in $\mathbb{Z}_m$.
- Risolvi gli esercizi assegnati su $\mathbb{Z}_{40}$ e $\mathbb{Z}_{192}$.
- Potremmo approfondire le proprietà degli omomorfismi di anelli o iniziare a studiare i sottogruppi e le loro proprietà.

Lezione 14: Anelli $\mathbb{Z}_m$, Criteri di Divisibilità, Equazioni Congruenziali

Data: 09/05/2025 (come da note).
Argomenti: Proprietà di $\mathbb{Z}_m$ (divisori dello zero, invertibili, nilpotenti, idempotenti), Criteri di divisibilità (via aritmetica modulare), Equazioni congruenziali lineari.

#tag/number-theory #tag/modular-arithmetic #tag/zn-rings #tag/congruences #tag/algebra-avanzata

---

1. Proprietà dell'Anello delle Classi di Resto $(\mathbb{Z}_m, +, \cdot)$

Ricordiamo che $(\mathbb{Z}_m, +, \cdot)$ è un **anello commutativo unitario**. L'unità è $\bar{1}$ (se $m > 1$).
Lo zero è $\bar{0}$.

- **1. Divisori dello Zero in $\mathbb{Z}_m$ (Pag 1):**
  - Un elemento $\bar{a} \in \mathbb{Z}_m$, con $\bar{a} \neq \bar{0}$, è un **divisore dello zero** se e solo se $\text{MCD}(a, m) \neq 1$.
  - **Spiegazione:** Se $d = \text{MCD}(a, m) \neq 1$, allora $a = d \cdot a'$ e $m = d \cdot m'$ con $m' < m$. Consideriamo $\bar{b} = \overline{m'}$. Poiché $m' < m$, $\overline{m'} \neq \bar{0}$.
    - $\bar{a} \cdot \overline{m'} = \overline{a \cdot m'} = \overline{(d \cdot a') \cdot m'} = \overline{a' \cdot (d \cdot m')} = \overline{a' \cdot m} = \bar{0}$.
    - Poiché $\bar{a} \neq \bar{0}$ e $\overline{m'} \neq \bar{0}$ ma il loro prodotto è $\bar{0}$, $\bar{a}$ è divisore dello zero.
  - Viceversa, se $\bar{a}$ è divisore dello zero, esiste $\bar{b} \neq \bar{0}$ tale che $\bar{a}\bar{b} = \bar{0}$, cioè $m \mid ab$. Se $\text{MCD}(a, m) = 1$, allora $m \mid b$, il che implica $\bar{b} = \bar{0}$, contraddizione. Quindi $\text{MCD}(a, m) \neq 1$.
- **2. Elementi Invertibili in $\mathbb{Z}_m$ (Pag 1):**
  - Un elemento $\bar{a} \in \mathbb{Z}_m$ è **invertibile** (o simmetrizzabile rispetto al prodotto) se e solo se $\text{MCD}(a, m) = 1$.
  - L'insieme degli elementi invertibili è $U(\mathbb{Z}_m) = \{\bar{a} \in \mathbb{Z}_m \mid \text{MCD}(a, m) = 1\}$.
  - $(U(\mathbb{Z}_m), \cdot)$ è un gruppo abeliano (gruppo moltiplicativo degli invertibili).
  - Il numero di elementi invertibili è $\phi(m)$ (Funzione toziente di Eulero).
- **Corollario: $\mathbb{Z}_p$ è un Campo (Pag 1):**
  - Se p è un numero **primo**, allora per ogni $\bar{a} \in \mathbb{Z}_p$ con $\bar{a} \neq \bar{0}$ (cioè $p \nmid a$), si ha $\text{MCD}(a, p) = 1$.
  - Quindi, tutti gli elementi non nulli di $\mathbb{Z}_p$ sono invertibili.
  - Poiché $(\mathbb{Z}_p, +, \cdot)$ è un anello commutativo unitario in cui ogni elemento non nullo è invertibile, **$\mathbb{Z}_p$ è un campo per ogni p primo.**
- **3. Elementi Nilpotenti in $\mathbb{Z}_m$ (Pag 1):**
  - Sia $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ la fattorizzazione in primi distinti di m.
  - Un elemento $\bar{a} \in \mathbb{Z}_m$ è **nilpotente** se e solo se a è un multiplo di $rad(m) = p_1 p_2 \dots p_k$ (il radicale di m).
  - Cioè, $\bar{a}$ è nilpotente $\iff p_i \mid a$ per ogni fattore primo p_i di m.
  - **Spiegazione:** Se $\bar{a}^N = \bar{0}$ per qualche $N \geq 1$, allora $m \mid a^N$. Questo implica che ogni fattore primo p_i di m deve dividere a^N, e quindi p_i deve dividere a. Viceversa, se ogni p_i divide a, allora $rad(m) \mid a$. Sia $N = \max(\alpha_i)$. Allora $(rad(m))^N$ sarà divisibile per m, e quindi a^N sarà divisibile per m, da cui $\bar{a}^N = \bar{0}$.
- **4. Elementi Idempotenti in $\mathbb{Z}_m$ (Pag 2):**
  - Un elemento $\bar{a} \in \mathbb{Z}_m$ è **idempotente** se $\bar{a}^2 = \bar{a}$.
  - Questo è equivalente a $a^2 \equiv a \pmod{m}$, cioè $m \mid (a^2 - a)$, ovvero $m \mid a(a-1)$.
  - Sempre $\bar{0}$ e $\bar{1}$ sono idempotenti.
  - **Esempio in $\mathbb{Z}_{10}$:**
    - $\bar{0}^2 = \bar{0}$.
    - $\bar{1}^2 = \bar{1}$.
    - $\bar{5}^2 = \overline{25} = \bar{5}$ (poiché $25 \equiv 5 \pmod{10}$).
    - $\bar{6}^2 = \overline{36} = \bar{6}$ (poiché $36 \equiv 6 \pmod{10}$).
    - Idempotenti in $\mathbb{Z}_{10}$: $\{\bar{0}, \bar{1}, \bar{5}, \bar{6}\}$.

Anello Zm Divisori dello zero in Zm Elementi invertibili in Zm Campo Zp Elemento nilpotente Elemento idempotente

---

2. Esercizi su $\mathbb{Z}_m$ (Pag 2-3)

Esercizio (Pag 2)

Determinare (se possibile) un $m \in \mathbb{N}, m > 1$ tale che $\mathbb{Z}_m$ soddisfi le seguenti condizioni:

- i) $\mathbb{Z}_m$ possiede esattamente 8 elementi invertibili e 6 divisori dello zero.
- ii) $\mathbb{Z}_m$ possiede esattamente 8 divisori dello zero e 6 elementi invertibili.

Suggerimenti:

- Il numero totale di elementi in $\mathbb{Z}_m$ è m.
- Gli elementi di $\mathbb{Z}_m$ sono o invertibili, o divisori dello zero, oppure $\bar{0}$ (che non è invertibile e, per definizione, non è divisore dello zero se $m > 1$).
- Numero invertibili = $\phi(m)$.

- Numero divisori dello zero = $m - \phi(m) - 1$ (per $m > 1$).

Per i):

- $\phi(m) = 8$.
- $m - \phi(m) - 1 = 6 \implies m - 8 - 1 = 6 \implies m - 9 = 6 \implies m = 15$.
- Verifichiamo $\phi(15)$: $15 = 3 \cdot 5$. $\phi(15) = \phi(3)\phi(5) = (3-1)(5-1) = 2 \cdot 4 = 8$. Corrisponde!
- Quindi $m = 15$ è una soluzione per (i).
- Divisori dello zero in $\mathbb{Z}_{15}$: elementi $\bar{a}$ tali che $\text{MCD}(a, 15) \neq 1$. I numeri coprimi con 15 (da 1 a 14) sono: 1, 2, 4, 7, 8, 11, 13, 14 (sono 8, come $\phi(15)$). I restanti (escluso 0) sono i divisori dello zero: 3, 5, 6, 9, 10, 12 (sono 6).

Per ii):

- Numero divisori dello zero = 8.
- Numero invertibili = $\phi(m) = 6$.
- $m - \phi(m) - 1 = 8 \implies m - 6 - 1 = 8 \implies m - 7 = 8 \implies m = 15$.
- Ma questo richiederebbe $\phi(15) = 6$, mentre sappiamo che $\phi(15) = 8$. C'è una contraddizione.
- Quindi **non è possibile** trovare un tale m per (ii).

- **Tabella per $\mathbb{Z}_{15}$ (Pag 3):**
  - **Divisori dello Zero:** $\bar{3}, \bar{5}, \bar{6}, \bar{9}, \overline{10}, \overline{12}$ (6 elementi)
  - **Elementi Invertibili:** $\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \overline{11}, \overline{13}, \overline{14}$ (8 elementi)

---

3. Criteri di Divisibilità (via Aritmetica Modulare)

Possiamo usare le congruenze per derivare i criteri di divisibilità. L'idea fondamentale è che un numero intero n è divisibile per un modulo m se e solo se il resto della divisione di n per m è 0. In termini di aritmetica modulare, questo si scrive come:

$$n \equiv 0 \pmod{m}$$

Consideriamo un numero intero positivo n scritto in base 10 con cifre $c_k, c_{k-1}, \ldots, c_1, c_0$. Questo significa che:

$$n = c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \cdots + c_1 \cdot 10^1 + c_0 \cdot 10^0$$

(Qui c_0 è la cifra delle unità, c_1 quella delle decine, c_2 quella delle centinaia, e così via. Il pedice i in c_i e 10^i indica la posizione della cifra, partendo da 0 per le unità).

Per verificare se n è divisibile per m, calcoliamo n modulo m. Usando le proprietà delle congruenze (la congruenza rispetta somma e prodotto), possiamo calcolare ogni termine separatamente:

$$n \equiv (c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \cdots + c_1 \cdot 10^1 + c_0 \cdot 10^0) \pmod{m}$$

$$n \equiv (c_k \cdot (10^k \pmod{m}) + c_{k-1} \cdot (10^{k-1} \pmod{m}) + \cdots + c_1 \cdot (10^1 \pmod{m}) + c_0 \cdot (10^0 \pmod{m})) \pmod{m}$$

Questa è la **formula generale** per calcolare il resto di un numero n modulo m basandosi sulle sue cifre.

Il Criterio Generale di Divisibilità:
Un numero n è divisibile per m se e solo se il risultato del calcolo:

$$(c_k \cdot (10^k \pmod{m}) + c_{k-1} \cdot (10^{k-1} \pmod{m}) + \cdots + c_1 \cdot (10^1 \pmod{m}) + c_0 \cdot (10^0 \pmod{m}))$$

è congruo a 0 modulo m.

I criteri di divisibilità "classici" (per 2, 3, 5, 9, 10, 11, ecc.) sono semplicemente questa formula generale applicata a specifici valori di m, sfruttando il pattern dei resti di $10^i \pmod{m}$.

Criteri Derivati dalla Formula Generale:

- **Divisibilità per $m = 2, 5, 10$:**
  - Osserviamo che $10 \equiv 0 \pmod{2}$, $10 \equiv 0 \pmod{5}$, $10 \equiv 0 \pmod{10}$.
  - Questo implica che per $m \in \{2, 5, 10\}$, $10^i \equiv 0 \pmod{m}$ per ogni $i \geq 1$.
  - La formula generale si semplifica notevolmente:

    $$n \equiv (c_k \cdot 0 + c_{k-1} \cdot 0 + \cdots + c_1 \cdot 0 + c_0 \cdot (10^0 \pmod{m})) \pmod{m}$$

    Poiché $10^0 = 1$ e $1 \equiv 1 \pmod{m}$ per $m > 1$:

    $$n \equiv (c_0 \cdot 1) \pmod{m} \implies n \equiv c_0 \pmod{m}$$

  - **Criterio:** n è divisibile per $m \in \{2, 5, 10\}$ se e solo se la sua ultima cifra c_0 è divisibile per m.
    - Per 2: c_0 è pari.
    - Per 5: c_0 è 0 o 5.
    - Per 10: c_0 è 0.

- **Divisibilità per $m = 4, 25, 100$:**
  - Osserviamo che $100 \equiv 0 \pmod 4$, $100 \equiv 0 \pmod{25}$, $100 \equiv 0 \pmod{100}$.
  - Questo implica che per $m \in \{4, 25, 100\}$, $10^i \equiv 0 \pmod m$ per ogni $i \geq 2$.
  - La formula generale diventa:

$$n \equiv (c_k \cdot 0 + \cdots + c_2 \cdot 0 + c_1 \cdot (10^1 \pmod m) + c_0 \cdot (10^0 \pmod m)) \pmod m$$
$$n \equiv (c_1 \cdot 10 + c_0 \cdot 1) \pmod m$$
$$n \equiv (10c_1 + c_0) \pmod m$$

  - **Criterio:** n è divisibile per $m \in \{4, 25, 100\}$ se e solo se il numero formato dalle sue ultime due cifre $(10c_1 + c_0)$ è divisibile per m.
    - Per 4: le ultime due cifre formano un numero divisibile per 4.
    - Per 25: le ultime due cifre formano un numero divisibile per 25 (00, 25, 50, 75).
    - Per 100: le ultime due cifre sono 00.
- **Divisibilità per $m = 3, 9$:**
  - Osserviamo che $10 \equiv 1 \pmod 3$ e $10 \equiv 1 \pmod 9$.
  - Questo implica che per $m \in \{3, 9\}$, $10^i \equiv 1^i \equiv 1 \pmod m$ per ogni $i \geq 0$.
  - La formula generale diventa:

$$n \equiv (c_k \cdot 1 + c_{k-1} \cdot 1 + \cdots + c_1 \cdot 1 + c_0 \cdot 1) \pmod m$$
$$n \equiv (c_k + c_{k-1} + \cdots + c_1 + c_0) \pmod m$$

  - **Criterio:** n è divisibile per $m \in \{3, 9\}$ se e solo se la somma delle sue cifre è divisibile per m.
- **Divisibilità per $m = 11$:**
  - Osserviamo che $10 \equiv -1 \pmod{11}$.
  - Questo implica che per $m = 11$, $10^i \equiv (-1)^i \pmod{11}$ per ogni $i \geq 0$.
  - La formula generale diventa:

$$n \equiv (c_k \cdot (-1)^k + c_{k-1} \cdot (-1)^{k-1} + \cdots + c_1 \cdot (-1)^1 + c_0 \cdot (-1)^0) \pmod{11}$$
$$n \equiv (c_0 - c_1 + c_2 - c_3 + \cdots + (-1)^k c_k) \pmod{11}$$

  - **Criterio:** n è divisibile per 11 se e solo se la somma a segni alterni delle sue cifre (partendo dalla cifra delle unità c_0 con segno positivo) è divisibile per 11.

Esempio Semplice: Verificare se 258 è divisibile per 3 (usando la formula generale)

Prendiamo il numero $n = 258$ e il modulo $m = 3$.

Passo 1: Identificare le cifre e le loro posizioni.
Il numero 258 ha 3 cifre:

- $c_0 = 8$ (posizione 0, unità)
- $c_1 = 5$ (posizione 1, decine)
- $c_2 = 2$ (posizione 2, centinaia)
  La posizione più alta è $k = 2$.

Passo 2: Scrivere il numero in forma polinomiale e impostare la congruenza modulo m.

$$n = 2 \cdot 10^2 + 5 \cdot 10^1 + 8 \cdot 10^0$$

Vogliamo calcolare $n \pmod 3$:

$$258 \equiv (2 \cdot 10^2 + 5 \cdot 10^1 + 8 \cdot 10^0) \pmod 3$$

Passo 3: Calcolare i resti delle potenze di 10 modulo m (cioè modulo 3).

- $10^0 \pmod 3$: $10^0 = 1$. $1 \equiv 1 \pmod 3$.
- $10^1 \pmod 3$: $10^1 = 10$. $10 = 3 \cdot 3 + 1$, quindi $10 \equiv 1 \pmod 3$.
- $10^2 \pmod 3$: $10^2 = 100$. $100 = 3 \cdot 33 + 1$, quindi $100 \equiv 1 \pmod 3$.
  In generale, per $m = 3$, $10^i \equiv 1 \pmod 3$ per ogni $i \geq 0$.

Passo 4: Sostituire i resti trovati nella formula generale.
Usiamo la formula: $n \equiv (c_k \cdot (10^k \pmod m) + \cdots + c_0 \cdot (10^0 \pmod m)) \pmod m$.
Nel nostro caso $(n = 258, m = 3,\ k = 2)$:

$$258 \equiv (c_2 \cdot (10^2 \pmod 3) + c_1 \cdot (10^1 \pmod 3) + c_0 \cdot (10^0 \pmod 3)) \pmod 3$$

Sostituiamo i valori delle cifre $(c_2 = 2, c_1 = 5, c_0 = 8)$ e i resti delle potenze di 10 (tutti 1):

$$258 \equiv (2 \cdot \mathbf{1} + 5 \cdot \mathbf{1} + 8 \cdot \mathbf{1}) \pmod 3$$

Passo 5: Eseguire i calcoli.

$$258 \equiv (2 + 5 + 8) \pmod 3$$

Sommiamo i numeri: $2 + 5 + 8 = 15$.

$$258 \equiv 15 \pmod 3$$

Passo 6: Verificare se il risultato finale è congruo a 0 modulo m.
Dobbiamo vedere se $15 \equiv 0 \pmod 3$.
$15 \div 3 = 5$ con resto 0.
Sì, $15 \equiv 0 \pmod 3$.

Passo 7: Concludere.
Poiché $258 \equiv 15 \pmod 3$ e $15 \equiv 0 \pmod 3$, per la proprietà transitiva della congruenza, $258 \equiv 0 \pmod 3$.
Questo significa che 258 è divisibile per 3.

Questo approccio formale mostra che il "trucco" della somma delle cifre per la divisibilità per 3 (o 9) non è magico, ma deriva direttamente dal fatto che le potenze di 10 hanno resto 1 quando divise per 3 (o 9).

Criteri di divisibilità Aritmetica modulare

---

4. Equazioni Congruenziali Lineari

Si tratta di equazioni della forma $ax \equiv b \pmod m$.
Cercare le soluzioni per x significa trovare le classi di resto $\bar{x} \in \mathbb{Z}_m$ tali che $[a]_m[x]_m = [b]_m$.

Esistenza e Numero di Soluzioni per $ax \equiv b \pmod m$

Sia data l'equazione congruenziale lineare:

$$ax \equiv b \pmod m$$

dove a, b sono interi e m è un intero positivo ($m > 1$). Sia $d = \text{MCD}(a, m)$.

Allora:

1. **Esistenza delle Soluzioni:** L'equazione $ax \equiv b \pmod m$ ammette soluzione se e solo se d divide b (scritto $d \mid b$).
2. **Numero delle Soluzioni:** Se $d \mid b$ (cioè se le soluzioni esistono), allora l'equazione ammette esattamente d soluzioni distinte modulo m.

In parole semplici:

Questo teorema ci dice due cose cruciali prima ancora di iniziare a risolvere l'equazione:

- **Prima cosa da controllare:** Calcola il Massimo Comun Divisore (MCD) tra il coefficiente della x (a) e il modulo (m). Chiamiamo questo MCD "d". Se questo d *non* divide il termine noto (b), allora non c'è nessuna soluzione. Puoi smettere subito!
- **Se invece d divide b:** Allora sai per certo che le soluzioni esistono. E non solo, sai anche *quante* ce ne sono: ce ne sono esattamente d soluzioni distinte se le consideriamo modulo m.

Questo teorema ti dice subito se vale la pena cercare soluzioni e quante te ne devi aspettare.

- **Procedimento Risolutivo (Pag 10-14):**
  1. Sia $d = \text{MCD}(a, m)$. Se $d \nmid b$, non ci sono soluzioni.
  2. Se $d \mid b$, dividiamo tutto per d:
     - $a = a_1 d$, $m = m_1 d$, $b = b_1 d$.
     - L'equazione $ax \equiv b \pmod m$ $(\star)$ è equivalente a $a_1 dx \equiv b_1 d \pmod{m_1 d}$.
     - Che si semplifica a $a_1 x \equiv b_1 \pmod{m_1}$ $(\star\star)$.
     - Importante: $\text{MCD}(a_1, m_1) = \text{MCD}(a/d, m/d) = \text{MCD}(a, m)/d = d/d = 1$.
  3. Ora dobbiamo risolvere $a_1 x \equiv b_1 \pmod{m_1}$, con $\text{MCD}(a_1, m_1) = 1$.
     - Questo significa che $\overline{a_1}$ è invertibile in $\mathbb{Z}_{m_1}$. Troviamo l'inverso $[\overline{a_1}]_{m_1}^{-1} = [\overline{c_1}]_{m_1}$.
     - Possiamo trovare c_1 risolvendo $a_1 x \equiv 1 \pmod{m_1}$ $(\star\star\star)$ usando l'algoritmo di Euclide esteso per l'identità di Bézout.
  4. Moltiplichiamo $(\star\star)$ per c_1: $c_1 a_1 x \equiv c_1 b_1 \pmod{m_1}$.
     - Poiché $c_1 a_1 \equiv 1 \pmod{m_1}$, otteniamo $1 \cdot x \equiv c_1 b_1 \pmod{m_1}$.
     - Quindi $x \equiv c_1 b_1 \pmod{m_1}$. Sia $c = c_1 b_1 \pmod{m_1}$.
     - La soluzione generale per $(\star\star)$ è $x = c + h \cdot m_1$ per $h \in \mathbb{Z}$.
  5. Le soluzioni distinte modulo m per l'equazione originale $(\star)$ sono:
     - $x_0 = c$
     - $x_1 = c + m_1$
     - $x_2 = c + 2m_1$

- ...
- $x_{d-1} = c + (d-1)m_1$
- Sono d soluzioni: $[c]_{m_1} = [c]_m \cup [c+m_1]_m \cup \cdots \cup [c+(d-1)m_1]_m$.

- **Esempio (Pag 11-12):** $10x \equiv 8 \pmod{14}$ $(\star)$
  1. $a = 10, b = 8, m = 14$. $d = \text{MCD}(10, 14) = 2$.
  2. $d = 2 \mid b = 8$. Ci sono $d = 2$ soluzioni.
  3. Dividiamo per $d = 2$: $5x \equiv 4 \pmod{7}$ $(\star\star)$. $(a_1 = 5, b_1 = 4, m_1 = 7)$. $\text{MCD}(5, 7) = 1$.
  4. Risolviamo $5x \equiv 1 \pmod{7}$ $(\star\star\star)$ per trovare l'inverso di 5 mod 7.
     - $7 = 5 \cdot 1 + 2$
     - $5 = 2 \cdot 2 + 1 \implies 1 = 5 - 2 \cdot 2$
     - $1 = 5 - 2 \cdot (7 - 5 \cdot 1) = 5 - 2 \cdot 7 + 2 \cdot 5 = 3 \cdot 5 - 2 \cdot 7$.
     - Quindi $3 \cdot 5 - 2 \cdot 7 = 1 \implies 3 \cdot 5 \equiv 1 \pmod{7}$. L'inverso di $\bar{5}$ è $\bar{3}$ in $\mathbb{Z}_7$. $c_1 = 3$.
  5. Moltiplichiamo $(\star\star)$ per $c_1 = 3$: $3 \cdot 5x \equiv 3 \cdot 4 \pmod{7} \implies x \equiv 12 \pmod{7} \implies x \equiv 5 \pmod{7}$.
     - $c = 5$. La soluzione generale di $(\star\star)$ è $x = 5 + h \cdot 7$.
  6. Le $d = 2$ soluzioni modulo $m = 14$ sono:
     - $x_0 = c = 5$. Sol: $\bar{5}_{14}$.
     - $x_1 = c + m_1 = 5 + 7 = 12$. Sol: $\overline{12}_{14}$.
     - Soluzioni: $[5]_{14}, [12]_{14}$.

Equazione congruenziale lineare Algoritmo di Euclide Esteso

---

5. Esercizi Proposti (Pag 15-21)

Esercizio 1 (Pag 15)

Risolvere $135x \equiv 10 \pmod{192}$.

- $d = \text{MCD}(135, 192)$. $192 = 135 \cdot 1 + 57$; $135 = 57 \cdot 2 + 21$; $57 = 21 \cdot 2 + 15$; $21 = 15 \cdot 1 + 6$; $15 = 6 \cdot 2 + 3$; $6 = 3 \cdot 2 + 0$. $d = 3$.
- $b = 10$. $d = 3 \nmid b = 10$. **Nessuna soluzione.**

Esercizio 2 (Pag 16-18)

Risolvere $135x \equiv 12 \pmod{192}$ $(\star)$.

- $a = 135, b = 12, m = 192$. $d = \text{MCD}(135, 192) = 3$.
- $d = 3 \mid b = 12$. Esistono $d = 3$ soluzioni.
- Dividiamo per $d = 3$: $45x \equiv 4 \pmod{64}$ $(\star\star)$. $(a_1 = 45, b_1 = 4, m_1 = 64)$. $\text{MCD}(45, 64) = 1$.
- Risolviamo $45x \equiv 1 \pmod{64}$ $(\star\star\star)$ per l'inverso di 45 mod 64.
  - $64 = 45 \cdot 1 + 19 \implies 19 = 64 - 45$
  - $45 = 19 \cdot 2 + 7 \implies 7 = 45 - 2 \cdot 19$
  - $19 = 7 \cdot 2 + 5 \implies 5 = 19 - 2 \cdot 7$
  - $7 = 5 \cdot 1 + 2 \implies 2 = 7 - 1 \cdot 5$
  - $5 = 2 \cdot 2 + 1 \implies 1 = 5 - 2 \cdot 2$
  - $1 = 5 - 2(7 - 5) = 3 \cdot 5 - 2 \cdot 7$
  - $1 = 3(19 - 2 \cdot 7) - 2 \cdot 7 = 3 \cdot 19 - 6 \cdot 7 - 2 \cdot 7 = 3 \cdot 19 - 8 \cdot 7$
  - $1 = 3 \cdot 19 - 8(45 - 2 \cdot 19) = 3 \cdot 19 - 8 \cdot 45 + 16 \cdot 19 = 19 \cdot 19 - 8 \cdot 45$
  - $1 = 19(64 - 45) - 8 \cdot 45 = 19 \cdot 64 - 19 \cdot 45 - 8 \cdot 45 = 19 \cdot 64 - 27 \cdot 45$.
  - Quindi $-27 \cdot 45 \equiv 1 \pmod{64}$. L'inverso $c_1 = -27 \equiv -27 + 64 \equiv 37 \pmod{64}$.
- Moltiplichiamo $(\star\star)$ per $c_1 = 37$: $x \equiv 37 \cdot 4 \pmod{64}$.
  - $37 \cdot 4 = 148$. $148 = 2 \cdot 64 + 20$. Quindi $148 \equiv 20 \pmod{64}$.
  - $c = 20$. Soluzione generale di $(\star\star)$: $x = 20 + h \cdot 64$.
- Le $d = 3$ soluzioni modulo $m = 192$ sono:
  - $x_0 = 20$.
  - $x_1 = 20 + 64 = 84$.
  - $x_2 = 20 + 2 \cdot 64 = 20 + 128 = 148$.
  - Soluzioni: $[20]_{192}, [84]_{192}, [148]_{192}$.

Esercizio 3 (Pag 19-20)

Risolvere $39x \equiv b \pmod{90}$ per $b \in \{10, 15, 17\}$.

- $a = 39, m = 90$. $d = \text{MCD}(39, 90)$. $90 = 39 \cdot 2 + 12$; $39 = 12 \cdot 3 + 3$; $12 = 3 \cdot 4 + 0$. $d = 3$.
- Caso $b = 10$: $d = 3 \nmid b = 10$. **Nessuna soluzione.**
- Caso $b = 17$: $d = 3 \nmid b = 17$. **Nessuna soluzione.**

- Caso $b=15$: $d=3 \mid b=15$. Esistono $d=3$ soluzioni.
  - Dividiamo $39x \equiv 15 \pmod{90}$ $(\star)$ per $d=3$: $13x \equiv 5 \pmod{30}$ $(\star\star)$. $(a_1=13, b_1=5, m_1=30)$.
  - Risolviamo $13x \equiv 1 \pmod{30}$ $(\star\star\star)$.
    - $30 = 13 \cdot 2 + 4 \implies 4 = 30 - 2 \cdot 13$
    - $13 = 4 \cdot 3 + 1 \implies 1 = 13 - 3 \cdot 4$
    - $1 = 13 - 3(30 - 2 \cdot 13) = 13 - 3 \cdot 30 + 6 \cdot 13 = 7 \cdot 13 - 3 \cdot 30$.
    - $7 \cdot 13 \equiv 1 \pmod{30}$. Inverso $c_1 = 7$.
  - Moltiplichiamo $(\star\star)$ per $c_1=7$: $x \equiv 7 \cdot 5 \pmod{30} \implies x \equiv 35 \pmod{30} \implies x \equiv 5 \pmod{30}$.
  - $c=5$. Soluzione generale di $(\star\star)$: $x = 5 + h \cdot 30$.
  - Le $d=3$ soluzioni modulo $m=90$ sono:
    - $x_0 = 5$.
    - $x_1 = 5 + 30 = 35$.
    - $x_2 = 5 + 2 \cdot 30 = 65$.
    - Soluzioni per $b=15$: $[5]_{90}, [35]_{90}, [65]_{90}$.

Esercizio 4 (Pag 21-23)

In $\mathbb{Z}_{100}$, con operazione $a * b = \overline{7}ab + \overline{25}(a+b)$, determinare gli $a \in \mathbb{Z}_{100}$ tali che $a * \bar{4} = \bar{4}$.

- $a * \bar{4} = \overline{7}a\bar{4} + \overline{25}(a + \bar{4}) = \overline{28}a + \overline{25}a + \overline{100} = \overline{53}a + \bar{0} = \overline{53}a$.
- Vogliamo $\overline{53}a = \bar{4}$, cioè $53a \equiv 4 \pmod{100}$ $(\star)$.
- $d = \text{MCD}(53, 100)$. $100 = 53 \cdot 1 + 47$; $53 = 47 \cdot 1 + 6$; $47 = 6 \cdot 7 + 5$; $6 = 5 \cdot 1 + 1$. $d = 1$.
- Poiché $d = 1 \mid b = 4$, esiste $d = 1$ soluzione.
- Risolviamo $53x \equiv 1 \pmod{100}$ $(\star\star\star)$.
  - $1 = 6 - 5 = 6 - (47 - 7 \cdot 6) = 8 \cdot 6 - 47$
  - $1 = 8(53 - 47) - 47 = 8 \cdot 53 - 8 \cdot 47 - 47 = 8 \cdot 53 - 9 \cdot 47$
  - $1 = 8 \cdot 53 - 9(100 - 53) = 8 \cdot 53 - 9 \cdot 100 + 9 \cdot 53 = 17 \cdot 53 - 9 \cdot 100$.
  - $17 \cdot 53 \equiv 1 \pmod{100}$. Inverso $c_1 = 17$.
- Moltiplichiamo $(\star)$ per $c_1 = 17$: $a \equiv 17 \cdot 4 \pmod{100} \implies a \equiv 68 \pmod{100}$.
- Soluzione: $a = \overline{68}$.

Esercizio 5 (Pag 24-26)

In $(\mathbb{Z}_{50}, *)$ con $a * b = \overline{3}ab$.

- Determinare l'elemento neutro u.
- Determinare $U(\mathbb{Z}_{50})$ rispetto a $*$.
- Determinare l'inverso di $\bar{8}$ e $\bar{9}$ (se esistono).

Elemento Neutro u:

- $a * u = a \implies \overline{3}au = a$. Questa deve valere per ogni $a \in \mathbb{Z}_{50}$.
- Se $a = \bar{1}$, $\overline{3}u = \bar{1} \implies 3u \equiv 1 \pmod{50}$.
- Risolviamo $3x \equiv 1 \pmod{50}$. $\text{MCD}(3, 50) = 1$.
  $50 = 3 \cdot 16 + 2 \implies 2 = 50 - 16 \cdot 3$.
  $3 = 2 \cdot 1 + 1 \implies 1 = 3 - 1 \cdot 2$.
  $1 = 3 - (50 - 16 \cdot 3) = 3 - 50 + 16 \cdot 3 = 17 \cdot 3 - 1 \cdot 50$.
  $17 \cdot 3 \equiv 1 \pmod{50}$. Quindi $x = \overline{17}$.
- L'elemento neutro è $u = \overline{17}$.

Elementi Invertibili $U(\mathbb{Z}_{50}, \cdot)$:

- $\bar{a}$ è invertibile se esiste $\bar{a}'$ tale che $\bar{a} * \bar{a}' = u = \overline{17}$.
- $\overline{3}aa' = \overline{17} \implies 3aa' \equiv 17 \pmod{50}$.
- Questa equazione ha soluzione per a' se $\text{MCD}(3a, 50) \mid 17$.
- Poiché 17 è primo, $\text{MCD}(3a, 50)$ deve essere 1.
- Affinché $\text{MCD}(3a, 50) = 1$, a non deve essere multiplo di 2 né di 5 (i fattori di 50), e $3a$ non deve essere multiplo di 2 né di 5. Dato che 3 non è mult. di 2 né 5, basta che a non sia mult. di 2 né 5.
- Quindi $\bar{a}$ è invertibile $\iff \text{MCD}(a, 50) = 1$. (Questi sono gli invertibili di $\mathbb{Z}_{50}$ rispetto al prodotto standard).
- $U(\mathbb{Z}_{50}, *) = U(\mathbb{Z}_{50}, \cdot) = \{\bar{a} \mid \text{MCD}(a, 50) = 1\}$.

Inverso di $\bar{8}$:

- $\text{MCD}(8, 50) = 2 \neq 1$. $\bar{8}$ non è invertibile rispetto al prodotto standard, quindi non sarà invertibile neanche qui. Non esiste.

Inverso di $\bar{9}$ (c):

- $\text{MCD}(9, 50) = 1$. Esiste. Vogliamo $\bar{9} * \bar{c} = \overline{17} \implies \overline{3 \cdot 9 \cdot c} = \overline{17} \implies \overline{27}c = \overline{17}$.
- $27c \equiv 17 \pmod{50}$. $d = \text{MCD}(27, 50) = 1$. Esiste soluzione unica.
- Risolviamo $27x \equiv 1 \pmod{50}$.
  $50 = 27 \cdot 1 + 23 \implies 23 = 50 - 27$

$27 = 23 \cdot 1 + 4 \implies 4 = 27 - 23$
$23 = 4 \cdot 5 + 3 \implies 3 = 23 - 5 \cdot 4$
$4 = 3 \cdot 1 + 1 \implies 1 = 4 - 1 \cdot 3$
$1 = 4 - (23 - 5 \cdot 4) = 6 \cdot 4 - 23$
$1 = 6(27 - 23) - 23 = 6 \cdot 27 - 6 \cdot 23 - 23 = 6 \cdot 27 - 7 \cdot 23$
$1 = 6 \cdot 27 - 7(50 - 27) = 6 \cdot 27 - 7 \cdot 50 + 7 \cdot 27 = 13 \cdot 27 - 7 \cdot 50$.
$13 \cdot 27 \equiv 1 \pmod{50}$. Inverso di $\overline{27}$ è $\overline{13}$.

- $c \equiv 13 \cdot 17 \pmod{50}$. $13 \cdot 17 = 221$.
  $221 = 4 \cdot 50 + 21$. $221 \equiv 21 \pmod{50}$.
- L'inverso di $\bar{9}$ è $\bar{c} = \overline{21}$.

Esercizio 6 (Pag 27-29)

In $\mathbb{Z}_{10}$ con l'operazione $a \oplus b = a + \bar{6}b$.

- È associativa? È commutativa?
- Determinare elementi neutri a destra e a sinistra.
- Considerare i sottoinsiemi $P = \{\overline{2k} \mid k \in \mathbb{Z}\}$ (pari) e $D = \{\overline{2k+1} \mid k \in \mathbb{Z}\}$ (dispari). $(P, \oplus)$ è stabile? È un gruppo? $(D, \oplus)$ è stabile?

Associatività:

- $a \oplus (b \oplus c) = a \oplus (b + \bar{6}c) = a + \bar{6}(b + \bar{6}c) = a + \bar{6}b + \overline{36}c = a + \bar{6}b + \bar{6}c$.
- $(a \oplus b) \oplus c = (a + \bar{6}b) \oplus c = (a + \bar{6}b) + \bar{6}c = a + \bar{6}b + \bar{6}c$.
- **SÌ, è associativa.**

Commutatività:

- $a \oplus b = a + \bar{6}b$.
- $b \oplus a = b + \bar{6}a$.
- Non sono uguali in generale. Es: $\bar{1} \oplus \bar{0} = \bar{1} + \bar{0} = \bar{1}$. $\bar{0} \oplus \bar{1} = \bar{0} + \bar{6} \cdot \bar{1} = \bar{6}$.
- **NO, non è commutativa.**

Elemento Neutro a Destra u_R: $a \oplus u_R = a \implies a + \bar{6}u_R = a \implies \bar{6}u_R = \bar{0}$.

- In $\mathbb{Z}_{10}$, $6u_R \equiv 0 \pmod{10}$. $\mathrm{MCD}(6, 10) = 2$. $2 \mid 0$. Ci sono 2 soluzioni.
- $3u_R \equiv 0 \pmod{5}$. $\mathrm{MCD}(3, 5) = 1$. Unica soluzione $u_R \equiv 0 \pmod{5}$.
- In $\mathbb{Z}_{10}$, $u_R = \bar{0}$ o $u_R = \bar{5}$.
- Infatti, $a \oplus \bar{0} = a + \bar{0} = a$. $a \oplus \bar{5} = a + \bar{6} \cdot \bar{5} = a + \overline{30} = a + \bar{0} = a$.
- **Neutri a destra: $\bar{0}, \bar{5}$.**

Elemento Neutro a Sinistra u_L: $u_L \oplus a = a \implies u_L + \bar{6}a = a \implies u_L = a - \bar{6}a = a(\bar{1} - \bar{6}) = a(-\bar{5}) = \bar{5}a$.

- Questo dipende da a. Non esiste un u_L unico. **Nessun neutro a sinistra.**
- Di conseguenza, non c'è elemento neutro bilatero. Non è un monoide.

Stabilità di $P = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$:

- Sia $a = \overline{2h}, b = \overline{2k}$ elementi di P.
- $a \oplus b = \overline{2h} + \bar{6}(\overline{2k}) = \overline{2h} + \overline{12k} = \overline{2h} + \overline{2k} = \overline{2(h+k)}$. Questo è un elemento pari.
- **SÌ, $(P, \oplus)$ è stabile.**
- $(P, \oplus)$ è un semigruppo (associatività ereditata). Ha neutro a destra $\bar{0} \in P$ e $\bar{5} \notin P$? No, $\bar{0}$ è neutro a dx. Se $a \in P$, $a \oplus \bar{0} = a$.
- $u_R = \bar{0}$ è in P. Verifichiamo se è neutro bilatero in P. $u_L \oplus a = a \implies u_L = \bar{5}a$. Se $a \in P$, a è pari. $\bar{5} \cdot (\text{pari})$ è $\bar{0}$ o $\overline{5 \cdot \text{pari}}$. Se $a = \bar{2}$, $\bar{5}\bar{2} = \overline{10} = \bar{0}$. Se $a = \bar{4}$, $\bar{5}\bar{4} = \overline{20} = \bar{0}$. Se $a = \bar{6}$, $\bar{5}\bar{6} = \overline{30} = \bar{0}$. Se $a = \bar{8}$, $\bar{5}\bar{8} = \overline{40} = \bar{0}$. Se $a = \bar{0}$, $\bar{5}\bar{0} = \bar{0}$.
- Quindi, per $a \in P$, $u_L = \bar{0}$ funziona come neutro a sinistra!
- $(P, \oplus, \bar{0})$ è un monoide. È un gruppo? Inverso di $a \in P$: $a \oplus a' = \bar{0} \implies a + \bar{6}a' = \bar{0} \implies \bar{6}a' = -a$.
  Se $a = \bar{2}$, $\bar{6}a' = -\bar{2} = \bar{8}$. $6a' \equiv 8 \pmod{10}$. $\mathrm{MCD}(6, 10) = 2 \mid 8$. Soluzioni: $3a' \equiv 4 \pmod{5}$. $a' \equiv 3 \cdot 4 = 12 \equiv 2 \pmod{5}$. $a' = \bar{2}, \bar{7}$. Solo $\bar{2} \in P$. Inverso di $\bar{2}$ è $\bar{2}$.
  Se $a = \bar{4}$, $\bar{6}a' = -\bar{4} = \bar{6}$. $6a' \equiv 6 \pmod{10}$. $3a' \equiv 3 \pmod{5}$. $a' \equiv 1 \pmod{5}$. $a' = \bar{1}, \bar{6}$. Solo $\bar{6} \in P$. Inverso di $\bar{4}$ è $\bar{6}$.
  $(P, \oplus, \bar{0})$ è un **gruppo abeliano** (la commutatività va verificata su P, ma $a + \bar{6}b = a + b + \bar{5}b$. $a \oplus b - b \oplus a = \bar{5}(b - a)$. Non è abeliano in generale).

Stabilità di D (dispari):

- Sia $a = \overline{2h+1}, b = \overline{2k+1}$ elementi di D.
- $a \oplus b = a + \bar{6}b = (\text{dispari}) + \bar{6}(\text{dispari}) = (\text{dispari}) + (\text{pari}) = (\text{dispari})$.
- **SÌ, $(D, \oplus)$ è stabile.**

Riepilogo Veloce Lezione 14

- Abbiamo analizzato a fondo le proprietà dell'anello $\mathbb{Z}_m$: divisori dello zero ($\mathrm{MCD}(a, m) \neq 1$), invertibili ($\mathrm{MCD}(a, m) = 1$), nilpotenti ($rad(m) \mid a$), idempotenti ($m \mid a(a-1)$).
- Abbiamo visto che $\mathbb{Z}_p$ è un campo se p è primo.
- Abbiamo derivato i **criteri di divisibilità** usando l'aritmetica modulare.

- Abbiamo studiato il teorema e il metodo risolutivo per le **equazioni congruenziali lineari** $ax \equiv b \pmod{m}$.
- Sono stati proposti diversi esercizi su $\mathbb{Z}_m$ e la risoluzione di congruenze.

Prossimi Passi

- Assicurati di aver compreso bene come determinare gli elementi speciali (div. zero, invertibili, etc.) in $\mathbb{Z}_m$.
- Fai pratica con la risoluzione delle equazioni congruenziali, specialmente con l'algoritmo di Euclide esteso.
- Il prossimo argomento, gli anelli dei polinomi, costruirà su queste fondamenta.

Lezione 15: Congruenze Lineari, Studio $\mathbb{Z}_n$, Anelli Prodotto, Relazioni di Equivalenza

Data: 13/05/2025 (come da note)
Argomenti: Risoluzione congruenze lineari, Divisori dello zero ed elementi nilpotenti in $\mathbb{Z}_n$, Funzioni su $\mathbb{Z}_n$ (iniettività/biettività), Strutture prodotto ($\mathbb{Z}_m \times \mathbb{Z}_n$), Relazioni di equivalenza (introduzione).

#tag/number-theory #tag/modular-arithmetic #tag/linear-congruences #tag/zn #tag/rings #tag/zero-divisor #tag/nilpotent #tag/product-rings #tag/equivalence-relations #tag/algebra-avanzata

---

1. Congruenze Lineari

Una congruenza lineare è un'equazione della forma $ax \equiv b \pmod{n}$.

- **Teorema di Risolubilità:** La congruenza lineare $ax \equiv b \pmod{n}$ ammette soluzioni se e solo se $d \mid b$, dove $d = \text{MCD}(a, n)$.
- Se $d \mid b$, allora ci sono esattamente d **soluzioni distinte modulo** n.
- **Procedimento Risolutivo (Esempio Pag 1-4):**
  Consideriamo la congruenza $[45]_{51} \cdot [x]_{51} = [18]_{51}$, cioè $45x \equiv 18 \pmod{51}$.
  1. **Calcolare** $d = \text{MCD}(a, n)$**:**
     $d = \text{MCD}(45, 51)$.
     $51 = 1 \cdot 45 + 6$
     $45 = 7 \cdot 6 + 3$
     $6 = 2 \cdot 3 + 0$
     Quindi $d = 3$.
  2. **Verificare se** $d \mid b$**:**
     $b = 18$. $3 \mid 18$ (poiché $18 = 3 \cdot 6$). **SÌ, la congruenza ammette soluzioni.**
     Ci saranno $d = 3$ soluzioni distinte modulo 51.
  3. **Dividere tutto per** d**:**
     Dividiamo a, b, n per $d = 3$:
     $(45/3)x \equiv (18/3) \pmod{51/3}$
     $15x \equiv 6 \pmod{17}$. Chiamiamo questa $(**)$.
     Le soluzioni di $(*)$ sono le stesse di $(**)$, ma quest'ultima è più semplice.
  4. **Risolvere la congruenza ridotta** $a'x \equiv b' \pmod{n'}$**:**
     Ora dobbiamo risolvere $15x \equiv 6 \pmod{17}$. Poiché $\text{MCD}(15, 17) = 1$ (che divide 6), esiste un'unica soluzione modulo 17.
     Per trovare una soluzione particolare, possiamo risolvere $15x \equiv 1 \pmod{17}$ e poi moltiplicare per 6.
     Usiamo l'algoritmo di Euclide per trovare l'identità di Bézout per 15 e 17:
     $17 = 1 \cdot 15 + 2 \implies 2 = 17 - 1 \cdot 15$
     $15 = 7 \cdot 2 + 1 \implies 1 = 15 - 7 \cdot 2$
     Sostituiamo l'espressione di 2 nella seconda equazione:
     $1 = 15 - 7 \cdot (17 - 1 \cdot 15)$
     $1 = 15 - 7 \cdot 17 + 7 \cdot 15$
     $1 = 8 \cdot 15 - 7 \cdot 17$
     Prendendo questa equazione modulo 17:
     $8 \cdot 15 - 7 \cdot 17 \equiv 1 \pmod{17}$
     $8 \cdot 15 - 0 \equiv 1 \pmod{17}$
     $8 \cdot 15 \equiv 1 \pmod{17}$.
     Quindi, una soluzione a $15x \equiv 1 \pmod{17}$ è $x_0 = 8$.
     Per ottenere la soluzione di $15x \equiv 6 \pmod{17}$, moltiplichiamo x_0 per 6:
     $x_p = x_0 \cdot 6 = 8 \cdot 6 = 48$.
     Riduciamo modulo 17: $48 \equiv 14 \pmod{17}$ (perché $48 = 2 \cdot 17 + 14$).
     Quindi $x \equiv 14 \pmod{17}$ è l'unica soluzione di $15x \equiv 6 \pmod{17}$.
  5. **Trovare tutte le** d **soluzioni modulo** n**:**
     La soluzione generale di $15x \equiv 6 \pmod{17}$ è $x = 14 + 17h$, con $h \in \mathbb{Z}$.

Queste sono anche le soluzioni di $45x \equiv 18 \pmod{51}$.
Vogliamo le $d = 3$ soluzioni distinte modulo 51. Le otteniamo dando a h i valori $0, 1, \ldots, d-1$ (cioè $0, 1, 2$):

- $h = 0 \implies x_1 = 14 + 17 \cdot 0 = 14$. Soluzione: $[14]_{51}$.
- $h = 1 \implies x_2 = 14 + 17 \cdot 1 = 31$. Soluzione: $[31]_{51}$.
- $h = 2 \implies x_3 = 14 + 17 \cdot 2 = 14 + 34 = 48$. Soluzione: $[48]_{51}$.
- (Se $h = 3$, $x_4 = 14 + 17 \cdot 3 = 14 + 51 = 65 \equiv 14 \pmod{51}$, si ripetono).

- **Insieme delle soluzioni:** $\text{Sol}(45x \equiv 18 \pmod{51}) = \{[14]_{51}, [31]_{51}, [48]_{51}\}$.

Congruenza Lineare Algoritmo di Euclide Esteso Identità di Bézout

---

2. Studio di $\mathbb{Z}_n$

2.1 Divisori dello Zero in $\mathbb{Z}_n$

- Un elemento $[a]_n \in \mathbb{Z}_n$, con $[a]_n \neq [0]_n$, è **divisore dello zero** se esiste $[b]_n \in \mathbb{Z}_n$, $[b]_n \neq [0]_n$, tale che $[a]_n \cdot [b]_n = [0]_n$.
- **Teorema:** $[a]_n$ è divisore dello zero in $\mathbb{Z}_n \iff \text{MCD}(a, n) \neq 1$.
- **Corollario:** $\mathbb{Z}_n$ è un dominio di integrità (privo di divisori dello zero non nulli) $\iff n$ è un numero **primo**. Se n è primo, $\mathbb{Z}_n$ è un campo.
- **Esempio $\mathbb{Z}_{60}$ (Pag 5):**
  - $60 = 2^2 \cdot 3 \cdot 5$.
  - $[a]_{60}$ è divisore dello zero $\iff \text{MCD}(a, 60) \neq 1$.
  - Cioè, a è multiplo di 2, o di 3, o di 5 (e $a \not\equiv 0 \pmod{60}$).
  - Gli **elementi invertibili** (unità) $U(\mathbb{Z}_{60})$ sono le classi $[a]_{60}$ tali che $\text{MCD}(a, 60) = 1$. Cioè a non è multiplo di 2, né di 3, né di 5.
  - Numero di invertibili: $\phi(60) = \phi(2^2 \cdot 3 \cdot 5) = \phi(2^2)\phi(3)\phi(5) = (2^2 - 2^1)(3-1)(5-1) = (4-2)(2)(4) = 2 \cdot 2 \cdot 4 = 16$. Ci sono 16 elementi invertibili in $\mathbb{Z}_{60}$.

2.2 Elementi Nilpotenti in $\mathbb{Z}_n$

- Un elemento $[a]_n \in \mathbb{Z}_n$ è **nilpotente** se esiste $k \geq 1$ tale che $([a]_n)^k = [a^k]_n = [0]_n$.
- **Teorema:** $[a]_n$ è nilpotente in $\mathbb{Z}_n \iff$ ogni fattore primo di n è anche un fattore primo di a.
  - Più precisamente, se $n = p_1^{e_1} \ldots p_r^{e_r}$ è la fattorizzazione di n, allora $[a]_n$ è nilpotente $\iff p_1 \mid a, \ldots, p_r \mid a$. Cioè a è un multiplo di $\text{rad}(n) = p_1 p_2 \ldots p_r$.
- **Esempio $\mathbb{Z}_{60}$ (Pag 6):**
  - $n = 60 = 2^2 \cdot 3 \cdot 5$. I fattori primi di 60 sono 2, 3, 5.
  - $[a]_{60}$ è nilpotente $\iff a$ è un multiplo di $2 \cdot 3 \cdot 5 = 30$.
  - Gli elementi nilpotenti sono $[0]_{60}$ e $[30]_{60}$.
    - $[30]^1 = [30] \neq [0]$.
    - $[30]^2 = [900]$. $900 = 15 \cdot 60$, quindi $[900]_{60} = [0]_{60}$.
    - $[0]^1 = [0]$.

Anello Zn Divisore dello zero in Zn Elemento Nilpotente in Zn Funzione di Eulero

---

3. Esercizi su Funzioni e Strutture

Esercizio 1 (Pag 7-10 - Funzione su $\mathbb{Z}_{15}$)

Sia $f : \mathbb{Z}_{15} \to \mathbb{Z}_{15}$ definita da:

$$f([a]_{15}) = \begin{cases} ([a]_{15})^{-1} & \text{se } [a]_{15} \in U(\mathbb{Z}_{15}) \\ [a]_{15} & \text{se } [a]_{15} \notin U(\mathbb{Z}_{15}) \end{cases}$$

Determinare se f è iniettiva e/o suriettiva (e quindi biettiva).

- **Passo 1: Determinare $U(\mathbb{Z}_{15})$ e i non invertibili.**
  - $15 = 3 \cdot 5$.
  - $U(\mathbb{Z}_{15}) = \{[a] \mid \text{MCD}(a, 15) = 1\} = \{[1], [2], [4], [7], [8], [11], [13], [14]\}$. $|\phi(15) = (3-1)(5-1) = 8|$.
  - Non Invertibili (Divisori di zero + [0]): $\{[0], [3], [5], [6], [9], [10], [12]\}$.
- **Passo 2: Verificare Iniettività.**
  Consideriamo $f([a]) = f([b])$. Dobbiamo mostrare che $[a] = [b]$.
  - **Caso i:** $[a], [b] \in U(\mathbb{Z}_{15})$.
    $f([a]) = [a]^{-1}$, $f([b]) = [b]^{-1}$. Se $[a]^{-1} = [b]^{-1}$, allora prendendo l'inverso di entrambi i lati, $([a]^{-1})^{-1} = ([b]^{-1})^{-1}$, che implica $[a] = [b]$. OK.

- **Caso ii:** $[a], [b] \notin U(\mathbb{Z}_{15})$.
  $f([a]) = [a]$, $f([b]) = [b]$. Se $[a] = [b]$, allora $[a] = [b]$. OK.
- **Caso iii:** $[a] \in U(\mathbb{Z}_{15})$, $[b] \notin U(\mathbb{Z}_{15})$.
  $f([a]) = [a]^{-1}$, $f([b]) = [b]$. Se $f([a]) = f([b])$, allora $[a]^{-1} = [b]$.
  Questo implicherebbe che $[b]$ è invertibile (perché è uguale a $[a]^{-1}$ che è invertibile). Ma avevamo supposto che $[b] \notin U(\mathbb{Z}_{15})$. Questo è un assurdo. Quindi questo caso non può portare a $f([a]) = f([b])$.
- Pertanto, $f([a]) = f([b])$ implica che o sono entrambi invertibili e uguali, o sono entrambi non invertibili e uguali. In ogni caso, $[a] = [b]$.
- **Conclusione: f è iniettiva.**

- **Passo 3: Verificare Suriettività (o Biettività).**
  - Poiché $\mathbb{Z}_{15}$ è un insieme **finito**, e $f : \mathbb{Z}_{15} \to \mathbb{Z}_{15}$ è **iniettiva**, allora f è anche **suriettiva** e quindi **biettiva**.
  - *Dimostrazione alternativa suriettività:*
    - Per ogni $[y] \in U(\mathbb{Z}_{15})$, vogliamo trovare $[x]$ t.c. $f([x]) = [y]$. Se prendiamo $[x] = [y]^{-1}$ (che è in $U(\mathbb{Z}_{15})$), allora $f([x]) = ([y]^{-1})^{-1} = [y]$.
    - Per ogni $[y] \notin U(\mathbb{Z}_{15})$, vogliamo trovare $[x]$ t.c. $f([x]) = [y]$. Se prendiamo $[x] = [y]$ (che non è in $U(\mathbb{Z}_{15})$), allora $f([x]) = [x] = [y]$.
    - **Conclusione: f è suriettiva.**

Esercizio 2 (Pag 11-13 - Struttura $(\mathbb{Z}_{15}, *)$)

Studiare la struttura $(\mathbb{Z}_{15}, *)$ dove $a * b = a + b + 2ab$.

- **Associatività e Commutatività:** Valgono perché le operazioni base $(+, \cdot)$ in $\mathbb{Z}_{15}$ le hanno, e la forma è la stessa dell'Esercizio 4 della Lezione 8.
- **Elemento Neutro u:**
  $a * u = a \implies a + u + 2au = a \implies u + 2au = \bar{0} \implies u(1 + 2a) = \bar{0}$.
  Questo deve valere per ogni $a \in \mathbb{Z}_{15}$. In particolare per $a = \bar{0}$, $u(1) = \bar{0} \implies u = \bar{0}$.
  Verifica: $a * \bar{0} = a + \bar{0} + 2a\bar{0} = a$. **Sì, $u = \bar{0}$ è l'elemento neutro.**
  Quindi $(\mathbb{Z}_{15}, *, \bar{0})$ è un **monoide commutativo**.
- **Elementi Invertibili (Simmetrici) a' per a:**
  $a * a' = \bar{0} \implies a + a' + 2aa' = \bar{0} \implies a'(1 + 2a) = -a$.
  a' esiste $\iff (1 + 2a)$ è invertibile in $(\mathbb{Z}_{15}, \cdot)$. Cioè $1 + 2a \in U(\mathbb{Z}_{15})$.
  $U(\mathbb{Z}_{15}) = \{[1], [2], [4], [7], [8], [11], [13], [14]\}$.
  Testiamo i valori di $a \in \mathbb{Z}_{15}$ per vedere quando $1 + 2a$ è invertibile:
  - $a = 0 \implies 1 + 2(0) = 1 \in U$. $0'$ esiste $(0' = -0 \cdot 1^{-1} = 0)$.
  - $a = 1 \implies 1 + 2(1) = 3 \notin U$. 1 non è invertibile per $*$.
  - $a = 2 \implies 1 + 2(2) = 5 \notin U$. 2 non è invertibile per $*$.
  - $a = 3 \implies 1 + 2(3) = 7 \in U$. $3'$ esiste. $3' = -3 \cdot 7^{-1}$. $7 \cdot x \equiv 1 \pmod{15}$. $7 \cdot (-2) = -14 \equiv 1 \pmod{15}$. Quindi $7^{-1} = -2 \equiv 13$. $3' = -3 \cdot 13 = -39 \equiv -39 + 3 \cdot 15 = -39 + 45 = 6$. Verif: $3 * 6 = 3 + 6 + 2 \cdot 3 \cdot 6 = 9 + 36 = 45 \equiv 0 \pmod{15}$. OK.
  - ... e così via. Bisogna testare tutti gli a.
  - $U(\mathbb{Z}_{15}, *) = \{a \in \mathbb{Z}_{15} \mid \text{MCD}(1 + 2a, 15) = 1\}$.

Esercizio 3 (Pag 14 - Funzione $f : \mathbb{Z}_3 \times \mathbb{Z}_5 \to \mathbb{Z}_{15}$)

È definita una funzione $f : (\bar{a}, \tilde{b}) \mapsto [a \cdot b]_{15}$? (dove $\bar{a} \in \mathbb{Z}_3, \tilde{b} \in \mathbb{Z}_5$).

- Una funzione deve essere ben definita. Se prendiamo rappresentanti diversi per la stessa classe, il risultato deve essere lo stesso.
- Sia $(\bar{a}, \tilde{b}) = (\bar{a'}, \tilde{b'})$. Questo significa $a \equiv a' \pmod{3}$ e $b \equiv b' \pmod{5}$.
- Dobbiamo verificare se $a \cdot b \equiv a' \cdot b' \pmod{15}$.
- Controesempio: $(\bar{1}, \tilde{2}) \in \mathbb{Z}_3 \times \mathbb{Z}_5$. $f(\bar{1}, \tilde{2}) = [1 \cdot 2]_{15} = [2]_{15}$.
- Un altro rappresentante per $\bar{1}$ è 4 $(4 \equiv 1 \pmod{3})$.
- Consideriamo $(\bar{4}, \tilde{2})$. $f(\bar{4}, \tilde{2}) = [4 \cdot 2]_{15} = [8]_{15}$.
- Poiché $[2]_{15} \neq [8]_{15}$, ma $(\bar{1}, \tilde{2})$ e $(\bar{4}, \tilde{2})$ rappresentano la stessa coppia se il primo componente è pensato in $\mathbb{Z}_3$ (cioè $\bar{1} = \bar{4}$ in $\mathbb{Z}_3$), la funzione **NON è ben definita** come scritta.
- (La prof probabilmente intendeva una mappa basata sul Teorema Cinese del Resto, che è un isomorfismo $ \mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5 . *Lamappa* $x \mapsto (x \pmod 3, x \pmod 5)$ è un isomorfismo. L'inversa è più complicata da scrivere direttamente come $a \cdot b$).

---

4. Anello Prodotto $\mathbb{Z}_m \times \mathbb{Z}_n$ (Esempio Pratico)

Esercizio 4 (Pag 17-22 - Studio $\mathbb{Z}_4 \times \mathbb{Z}_6$)

Sia $R = \mathbb{Z}_4 \times \mathbb{Z}_6$. Definiamo $+$ e $\cdot$ componente per componente:
$(\bar{a}, \tilde{b}) + (\bar{c}, \tilde{d}) = (\overline{a + c}, \widetilde{b + d})$
$(\bar{a}, \tilde{b}) \cdot (\bar{c}, \tilde{d}) = (\overline{a \cdot c}, \widetilde{b \cdot d})$
Allora $(R, +, \cdot)$ è un **anello commutativo unitario**.

1. **Cardinalità $|R|$:**
   $|R| = |\mathbb{Z}_4| \cdot |\mathbb{Z}_6| = 4 \cdot 6 = 24$.
2. **Elemento Neutro Additivo 0_R e Moltiplicativo 1_R:**
   $0_R = ([0]_4, [0]_6)$.
   $1_R = ([1]_4, [1]_6)$.
3. **Elementi Invertibili $U(R)$, Divisori dello Zero, Nilpotenti, Idempotenti:**
   - $(\bar{a}, \tilde{b}) \in U(R) \iff \bar{a} \in U(\mathbb{Z}_4) \wedge \tilde{b} \in U(\mathbb{Z}_6)$.
     - $U(\mathbb{Z}_4) = \{[1]_4, [3]_4\}$.
     - $U(\mathbb{Z}_6) = \{[1]_6, [5]_6\}$.
     - $U(R) = \{([1],[1]), ([1],[5]), ([3],[1]), ([3],[5])\}$. Ce ne sono $2 \cdot 2 = 4$.
     - Esempio: $([3]_4, [5]_6)^{-1} = ([3]_4^{-1}, [5]_6^{-1}) = ([3]_4, [5]_6)$ (poiché $3 \cdot 3 = 9 \equiv 1 \pmod 4$ e $5 \cdot 5 = 25 \equiv 1 \pmod 6$).
   - **Nilpotenti**: $(\bar{a}, \tilde{b})$ è nilpotente $\iff$ $\bar{a}$ è nilpotente in $\mathbb{Z}_4$ E $\tilde{b}$ è nilpotente in $\mathbb{Z}_6$.
     - Nilpotenti in $\mathbb{Z}_4$: $4 = 2^2$. Multipli di 2: $\{[0]_4, [2]_4\}$.
     - Nilpotenti in $\mathbb{Z}_6$: $6 = 2 \cdot 3$. Multipli di $2 \cdot 3 = 6$: $\{[0]_6\}$.
     - Nilpotenti in R: $(\{[0],[2]\}, \{[0]\}) = \{([0],[0]), ([2],[0])\}$.
   - **Idempotenti**: $(\bar{a}, \tilde{b})$ è idempotente $\iff (\bar{a}, \tilde{b})^2 = (\bar{a}, \tilde{b}) \iff \bar{a}^2 = \bar{a}$ in $\mathbb{Z}_4$ E $\tilde{b}^2 = \tilde{b}$ in $\mathbb{Z}_6$.
     - Idempotenti in $\mathbb{Z}_4$: $[0]^2 = 0, [1]^2 = 1, [2]^2 = 4 \equiv 0, [3]^2 = 9 \equiv 1$. Sono $\{[0], [1]\}$.
     - Idempotenti in $\mathbb{Z}_6$: $[0]^2 = 0, [1]^2 = 1, [2]^2 = 4, [3]^2 = 9 \equiv 3, [4]^2 = 16 \equiv 4, [5]^2 = 25 \equiv 1$. Sono $\{[0], [1], [3], [4]\}$.
     - Idempotenti in R: $2 \cdot 4 = 8$ elementi. Es: $([1]_4, [0]_6), ([0]_4, [1]_6), ([1]_4, [3]_6)$, ecc.
   - **Divisori dello Zero**: Tutti gli elementi non invertibili e non nulli.
4. **R è un Dominio di Integrità? NO**, perché ha divisori dello zero (es. $([2]_4, [0]_6) \cdot ([0]_4, [1]_6) = ([0]_4, [0]_6)$ ma i fattori non sono 0_R).
5. bis. **Caratteristica di R, $char(R)$:**
   $char(R) = \text{mcm}(char(\mathbb{Z}_4), char(\mathbb{Z}_6)) = \text{mcm}(4, 6) = 12$.
6. Sia $M = \mathbb{Z}_4 \times \{[0]_6, [3]_6\}$. Studiare la stabilità di M rispetto a $+$ e $\cdot$. Che struttura hanno $(M, +)$ e $(M, \cdot)$?
   - L'insieme M è costituito dalle coppie $(\bar{a}, \tilde{b})$ dove $\bar{a} \in \mathbb{Z}_4$ e $\tilde{b} \in \{[0]_6, [3]_6\}$.
   - **Stabilità per l'addizione (+):**
     Prendiamo due elementi generici da M: $(\bar{a}, \tilde{b})$ e $(\bar{c}, \tilde{d})$, con $\tilde{b}, \tilde{d} \in \{[0]_6, [3]_6\}$.
     La loro somma è $(\overline{a+c}, \widetilde{b+d})$.
     $\overline{a+c}$ è sempre in $\mathbb{Z}_4$. Dobbiamo verificare $\widetilde{b+d} \in \{[0]_6, [3]_6\}$.
     Le possibili somme in $\{[0]_6, [3]_6\}$ sono: $[0]_6 + [0]_6 = [0]_6$, $[0]_6 + [3]_6 = [3]_6$, $[3]_6 + [0]_6 = [3]_6$, $[3]_6 + [3]_6 = [6]_6 = [0]_6$.
     Tutti i risultati sono in $\{[0]_6, [3]_6\}$. Quindi M **è stabile per l'addizione**.
   - **Struttura di $(M, +)$:**
     L'addizione in M è associativa e commutativa (ereditata da R).
     L'elemento neutro additivo di R, $0_R = ([0]_4, [0]_6)$, appartiene a M (poiché $[0]_4 \in \mathbb{Z}_4$ e $[0]_6 \in \{[0]_6, [3]_6\}$). Quindi 0_R è l'elemento neutro di $(M, +)$.
     Per ogni elemento $(\bar{a}, \tilde{b}) \in M$, il suo opposto additivo è $(-\bar{a}, -\tilde{b})$. $-\bar{a}$ è sempre in $\mathbb{Z}_4$. Se $\tilde{b} \in \{[0]_6, [3]_6\}$, allora $-\tilde{b} \in \{[0]_6, [3]_6\}$ (infatti $-[0]_6 = [0]_6$ e $-[3]_6 = [3]_6$). Quindi l'opposto è in M.
     Pertanto, $(M, +)$ è un **gruppo abeliano**.
   - **Stabilità per la moltiplicazione ($\cdot$):**
     Prendiamo due elementi generici da M: $(\bar{a}, \tilde{b})$ e $(\bar{c}, \tilde{d})$, con $\tilde{b}, \tilde{d} \in \{[0]_6, [3]_6\}$.
     Il loro prodotto è $(\overline{a \cdot c}, \widetilde{b \cdot d})$.
     $\overline{a \cdot c}$ è sempre in $\mathbb{Z}_4$. Dobbiamo verificare $\widetilde{b \cdot d} \in \{[0]_6, [3]_6\}$.
     I possibili prodotti in $\{[0]_6, [3]_6\}$ sono: $[0]_6 \cdot [0]_6 = [0]_6$, $[0]_6 \cdot [3]_6 = [0]_6$, $[3]_6 \cdot [0]_6 = [0]_6$, $[3]_6 \cdot [3]_6 = [9]_6 = [3]_6$.
     Tutti i risultati sono in $\{[0]_6, [3]_6\}$. Quindi M **è stabile per la moltiplicazione**.
   - **Struttura di $(M, \cdot)$:**
     La moltiplicazione in M è associativa e commutativa (ereditata da R).
     Cerchiamo un elemento neutro $([e_1]_4, [e_2]_6) \in M$ tale che moltiplicato per ogni elemento di M lo lasci invariato.
     Abbiamo trovato che questo elemento è $([1]_4, [3]_6)$. Questo elemento appartiene a M (poiché $[1]_4 \in \mathbb{Z}_4$ e $[3]_6 \in \{[0]_6, [3]_6\}$). Quindi $([1]_4, [3]_6)$ è l'elemento neutro di $(M, \cdot)$. Nota che questo *non* è l'elemento neutro moltiplicativo dell'anello R, che è $([1]_4, [1]_6)$.
     Non tutti gli elementi in M hanno un inverso moltiplicativo *dentro* M (ad esempio, $([0]_4, [0]_6)$ non ha inverso).
     Pertanto, $(M, \cdot)$ è un **monoide commutativo**.
   - **Conclusione aggiuntiva:** Poiché M è stabile per entrambe le operazioni, ma non contiene l'elemento neutro moltiplicativo di R, M non è un sottoanello di R.

---

5. Esercizio su Funzione e Invertibilità Modulare (Pag 23)

Esercizio 5 (Pag 23 - Funzione e Invertibilità Modulare)

Sia $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ data da $f(a, b) = 30a + b$.

1. È iniettiva? È suriettiva?
2. Sia $T = \{c \in \mathbb{Z} \mid 60 \leq c \leq 70\}$. Determinare gli elementi $(n, a) \in \mathbb{Z} \times T$ (con $n \geq 0$) tali che $f(n, a)$ sia invertibile modulo 45.

1. **Iniettività:** $f(0,30) = 30 \cdot 0 + 30 = 30$. $f(1,0) = 30 \cdot 1 + 0 = 30$. Poiché $(0,30) \neq (1,0)$ ma $f(0,30) = f(1,0)$, la funzione **NON è iniettiva**.
   Suriettività: Per ogni $z \in \mathbb{Z}$, possiamo trovare $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ tale che $f(a,b) = z$? Sì, ad esempio, prendendo $a = 0$, abbiamo $f(0,b) = 30 \cdot 0 + b = b$. Quindi, per ottenere qualsiasi intero z, possiamo semplicemente scegliere la coppia $(0,z)$. Dunque, **È suriettiva**.

2. Vogliamo che $f(n,a) = 30n + a$ sia invertibile modulo 45. Questo significa che $\text{MCD}(30n + a, 45) = 1$.
   Sappiamo che $a \in T = \{60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70\}$ e $n \geq 0$.
   Un numero è invertibile modulo 45 se e solo se non ha fattori primi in comune con 45. I fattori primi di 45 sono 3 e 5 ($45 = 3^2 \cdot 5$).
   Quindi, vogliamo che $30n + a$ non sia divisibile per 3 e non sia divisibile per 5.
   - Modulo 3: $30n + a \equiv 0 \cdot n + a \equiv a \pmod 3$. Vogliamo $a \not\equiv 0 \pmod 3$.
   - Modulo 5: $30n + a \equiv 0 \cdot n + a \equiv a \pmod 5$. Vogliamo $a \not\equiv 0 \pmod 5$.
     Dobbiamo quindi esaminare i valori di a nell'insieme T e vedere quali non sono multipli di 3 e non sono multipli di 5.

a	$a \pmod 3$	$a \pmod 5$	**Condizioni ($\text{MCD}(a,45) = 1$)?**
60	0	0	NO (divisibile per 3 e 5)
61	1	1	SÌ
62	2	2	SÌ
63	0	3	NO (divisibile per 3)
64	1	4	SÌ
65	2	0	NO (divisibile per 5)
66	0	1	NO (divisibile per 3)
67	1	2	SÌ
68	2	3	SÌ
69	0	4	NO (divisibile per 3)
70	1	0	NO (divisibile per 5)

   Gli unici valori di a in T che soddisfano le condizioni ($a \not\equiv 0 \pmod 3$ e $a \not\equiv 0 \pmod 5$) sono: $61, 62, 64, 67, 68$.
   Per questi valori di a, $\text{MCD}(a,45) = 1$. Poiché $30n + a \equiv a \pmod{15}$ (e quindi anche modulo 3 e modulo 5), la condizione $\text{MCD}(30n + a, 45) = 1$ si riduce a $\text{MCD}(a,45) = 1$.
   La condizione su n ($n \geq 0$) non influenza l'invertibilità modulo 45, dato che $30n$ è sempre un multiplo sia di 3 che di 5.

   Gli elementi $(n,a) \in \mathbb{Z} \times T$ con $n \geq 0$ tali che $f(n,a)$ è invertibile modulo 45 sono tutte le coppie (n,a) dove n è un qualsiasi intero non negativo ($n \in \{0,1,2,\ldots\}$) e a è uno dei valori $\{61, 62, 64, 67, 68\}$.
   L'insieme delle soluzioni è: $\{(n,a) \in \mathbb{Z}_{\geq 0} \times \{61, 62, 64, 67, 68\}\}$.

---

6. Relazioni di Equivalenza (Cenno)

Esercizio 6 (Pag 15-16 - Relazione di Equivalenza)

Sia $A = \{n \in \mathbb{N} \mid n \leq 7\} = \{0,1,2,3,4,5,6,7\}$.
Sia ρ una relazione di equivalenza su A. Sappiamo che:

- $0 \rho 7$
- $(1,4) \in G_\rho$ (cioè $1 \rho 4$)
- $\{3,4,7\} \subseteq [2]_\rho$ (la classe di equivalenza di 2 contiene 3, 4, 7)
- Se $1 \rho 3$.

Determinare le classi di equivalenza di ρ.

- Sappiamo che le classi di equivalenza formano una partizione di A.
- Da $\{3,4,7\} \subseteq [2]_\rho$, per simmetria e transitività, $2,3,4,7$ sono tutti nella stessa classe. $[2]_\rho$ contiene almeno $\{2,3,4,7\}$.
- $0 \rho 7$. Poiché $7 \in [2]_\rho$, allora $0 \in [2]_\rho$. Ora $[2]_\rho$ contiene almeno $\{0,2,3,4,7\}$.
- $1 \rho 4$. Poiché $4 \in [2]_\rho$, allora $1 \in [2]_\rho$. Ora $[2]_\rho$ contiene almeno $\{0,1,2,3,4,7\}$.
- Se $1 \rho 3$ (questa info era già implicata da $1 \rho 4$ e $3 \rho 4 \implies 1 \rho 3$).
- Elementi rimasti: $5, 6$.
- Se la domanda "se $1 \rho 3$" è una condizione aggiuntiva che *potrebbe* non essere vera e va considerata come un "se", allora abbiamo due scenari. Ma le altre condizioni la implicano.
- Assumendo che le prime 3 condizioni siano vere, $[2]_\rho = \{0,1,2,3,4,7\}$.
- Gli elementi 5 e 6 devono appartenere a qualche classe.
  - **Scenario 1:** $[5]_\rho = \{5\}$, $[6]_\rho = \{6\}$.
    Partizione: $\{\{0,1,2,3,4,7\}, \{5\}, \{6\}\}$.
  - **Scenario 2:** $5 \rho 6$. $[5]_\rho = \{5,6\}$.
    Partizione: $\{\{0,1,2,3,4,7\}, \{5,6\}\}$.

- La nota dice "[2] = {0,1,2,3,4,5,6,7}" oppure "{6} (isolato)". Se la classe di 2 è tutto A, allora tutti sono in relazione con tutti.
- Se invece la classe di 2 è $\{0,1,2,3,4,7\}$, e vogliamo che $1\rho 3$ sia vera (come lo è), allora dobbiamo capire il significato di "determinare le relazioni di equivalenza". Se l'esercizio chiede di trovare la *più fine* partizione che soddisfa le condizioni o la *più grossolana*.
- Dato che $\{3,4,7\} \subseteq [2]_\rho$, e $1\rho 4$, e $0\rho 7$, allora $0,1,2,3,4,7$ sono tutti nella stessa classe. Se questa è $[2]_\rho$, allora $[2]_\rho = \{0,1,2,3,4,7\}$. Gli elementi restanti sono $\{5,6\}$. Possono formare classi separate $\{5\},\{6\}$ o una classe unica $\{5,6\}$. L'esercizio presenta due possibili soluzioni per $[2]_\rho$ a seconda di come si interpreta "se $1\rho 3$". Tuttavia, $1\rho 4$ e $4\rho 3$ (da $3 \in [2]$ e $4 \in [2]$) implica $1\rho 3$ per transitività. Quindi $1,2,3,4,7,0$ sono tutti in relazione.
- Le classi di equivalenza sono una partizione.
  Soluzione 1: $C_1 = \{0,1,2,3,4,7\}, C_2 = \{5\}, C_3 = \{6\}$.
  Soluzione 2: $C_1 = \{0,1,2,3,4,5,7\}, C_2 = \{6\}$ (se $2\rho 5$).
  Soluzione 3: $C_1 = \{0,1,2,3,4,6,7\}, C_2 = \{5\}$ (se $2\rho 6$).
  Soluzione 4: $C_1 = \{0,1,2,3,4,7\}, C_2 = \{5,6\}$ (se $5\rho 6$ ma non con gli altri).
  Soluzione 5: $C_1 = \{0,1,2,3,4,5,6,7\}$ (tutti in relazione).
  L'informazione nelle note indicano che $[2] = \{0,1,2,3,4,5,6,7\}$ o $[2]$ e $\{6\}$ come classe separata.
  Se $[2]_\rho = \{0,1,2,3,4,5,7\}$ e $\{6\}$, questa è una partizione.
  Se $[2]_\rho = \{0,1,2,3,4,7\}$ e $\{5\}$ e $\{6\}$, questa è una partizione.
  L'esercizio è un po' vago senza specificare se si cerca la partizione più fine o grossolana che soddisfa le condizioni. Le condizioni date implicano che $\{0,1,2,3,4,7\}$ sono nella stessa classe.

Relazione di equivalenza Classe di equivalenza

Riepilogo Veloce Lezione 10 (15)

- Abbiamo imparato a **risolvere congruenze lineari** $ax \equiv b \pmod{n}$.
- Abbiamo caratterizzato i **divisori dello zero** ($MCD(a,n) \neq 1$) e gli **elementi nilpotenti** (multipli di $\text{rad}(n)$) in $\mathbb{Z}_n$.
- Abbiamo svolto esercizi sulla **biettività di funzioni** definite su $\mathbb{Z}_n$.
- Abbiamo analizzato la struttura dell'**anello prodotto** $\mathbb{Z}_m \times \mathbb{Z}_n$, determinando unità, nilpotenti, idempotenti, caratteristica.
- Abbiamo introdotto il concetto di **relazione di equivalenza** e classi di equivalenza.
- Sono stati proposti numerosi **esercizi** per consolidare questi concetti.

Prossimi Passi

- Assicurati di padroneggiare la risoluzione delle congruenze lineari.
- Comprendi bene come identificare gli elementi speciali (invertibili, divisori dello zero, nilpotenti, idempotenti) negli anelli $\mathbb{Z}_n$ e negli anelli prodotto.
- Le relazioni di equivalenza sono fondamentali e portano al concetto di insiemi quoziente.

Lezione 16: Relazioni di Equivalenza, Teoria dei Numeri, Calcolo Combinatorio

Data: 16/05/2025 (come da note)
Argomenti: Relazioni di Equivalenza (esempi, classi, quoziente), Esercizio Struttura Algebrica $\mathbb{Z}_{16}$, Equazioni Diofantee, Funzione di Eulero $\varphi(n)$, Teorema di Fermat-Eulero, Calcolo Combinatorio (fattoriale, binomiale, identità, applicazioni).

#tag/relations #tag/equivalence-relations #tag/quotient-set #tag/number-theory #tag/diophantine-equations #tag/euler-phi #tag/euler-fermat-theorem #tag/combinatorics #tag/algebra-avanzata

---

1. Relazioni di Equivalenza

Una relazione binaria $\mathcal{R}$ su un insieme A si dice **relazione di equivalenza** se è:

1. **Riflessiva:** $\forall x \in A, x\mathcal{R}x$.
2. **Simmetrica:** $\forall x,y \in A, x\mathcal{R}y \implies y\mathcal{R}x$.
3. **Transitiva:** $\forall x,y,z \in A, (x\mathcal{R}y \land y\mathcal{R}z) \implies x\mathcal{R}z$.

1.1 Esempio di Verifica (Pag 1)

Consideriamo le seguenti relazioni su $\mathbb{Z}$:

- α: $a\,\alpha\,b \iff 5a+8 \equiv_{15} 5b-7$
- β: $a\,\beta\,b \iff 5a+8 \equiv_{15} 5b+7$
- γ: $a\,\gamma\,b \iff 5a+8 \equiv_{15} 8b+5$
- δ: $a\,\delta\,b \iff \forall p \in \mathbb{P}(\text{primi}), (p \mid a \iff p \mid b)$ (cioè a e b hanno gli stessi divisori primi, o $a = \pm b$, o $a,b \in \{1,-1\}$ o $a = 0 \iff b = 0$).

Quali definiscono una relazione di equivalenza?

Analisi di α (Pag 1-3)

$a \alpha b \iff 5a + 8 \equiv_{15} 5b - 7$
Questo significa $5a + 8 - (5b - 7)$ è un multiplo di 15.
$5a + 8 - 5b + 7 = 5a - 5b + 15 \equiv_{15} 5a - 5b$.
Quindi, $a \alpha b \iff 5a - 5b \equiv_{15} 0 \iff 5(a - b) \equiv_{15} 0$.
Questo significa che $15 \mid 5(a - b)$, ovvero $3 \cdot 5 \mid 5(a - b)$.
Dividendo per 5 (poiché $\text{MCD}(5, 15) = 5$), otteniamo $3 \mid (a - b)$.
Quindi, $a \alpha b \iff a - b \equiv_3 0 \iff a \equiv_3 b$.
La relazione α è la **congruenza modulo 3**.

- **Riflessiva:** $a \equiv_3 a$ (poiché $a - a = 0$ è multiplo di 3). **SÌ**.
- **Simmetrica:** Se $a \equiv_3 b$, allora $a - b = 3k$. Quindi $b - a = -3k = 3(-k)$. $b \equiv_3 a$. **SÌ**.
- **Transitiva:** Se $a \equiv_3 b$ e $b \equiv_3 c$, allora $a - b = 3k_1$ e $b - c = 3k_2$. Sommando: $(a - b) + (b - c) = 3k_1 + 3k_2 \implies a - c = 3(k_1 + k_2)$. Quindi $a \equiv_3 c$. **SÌ**.
- **Conclusione:** α è una relazione di equivalenza.

Classi di Equivalenza per α (Congruenza modulo 3):

- $[0]_\alpha = \{n \in \mathbb{Z} \mid n \equiv_3 0\} = \{\dots, -3, 0, 3, 6, \dots\} = [0]_3$.
- $[1]_\alpha = \{n \in \mathbb{Z} \mid n \equiv_3 1\} = \{\dots, -2, 1, 4, 7, \dots\} = [1]_3$.
- $[2]_\alpha = \{n \in \mathbb{Z} \mid n \equiv_3 2\} = \{\dots, -1, 2, 5, 8, \dots\} = [2]_3$.
  L'insieme quoziente $\mathbb{Z}/\alpha = \mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$.

Analisi di β (Pag 4)

$a \beta b \iff 5a + 8 \equiv_{15} 5b + 7$
$5a - 5b \equiv_{15} 7 - 8 \implies 5(a - b) \equiv_{15} -1 \equiv_{15} 14$.

- **Riflessiva?** $a \beta a \implies 5(a - a) \equiv_{15} 14 \implies 0 \equiv_{15} 14$. Questo è **FALSO**.
- **Conclusione:** β non è riflessiva, quindi **non è una relazione di equivalenza**.

Analisi di γ (Pag 5)

$a \gamma b \iff 5a + 8 \equiv_{15} 8b + 5$
$5a - 8b \equiv_{15} 5 - 8 \implies 5a - 8b \equiv_{15} -3 \equiv_{15} 12$.

- **Riflessiva?** $a \gamma a \implies 5a - 8a \equiv_{15} 12 \implies -3a \equiv_{15} 12$.
  - Se $a = 0$, $0 \equiv_{15} 12$. Falso.
- **Conclusione:** γ non è riflessiva, quindi **non è una relazione di equivalenza**.

Analisi di δ (Pag 5-6)

$a \delta b \iff \forall p \in \mathbb{P}, (p \mid a \iff p \mid b)$. (Hanno gli stessi divisori primi).

- **Riflessiva:** $\forall p, (p \mid a \iff p \mid a)$. Vero. **SÌ**.
- **Simmetrica:** Se $(\forall p, p \mid a \iff p \mid b)$, allora $(\forall p, p \mid b \iff p \mid a)$. Vero. **SÌ**.
- **Transitiva:** Se $(\forall p, p \mid a \iff p \mid b)$ e $(\forall p, p \mid b \iff p \mid c)$, allora $(\forall p, p \mid a \iff p \mid c)$. Vero. **SÌ**.
- **Conclusione:** δ è una relazione di equivalenza.

Classi di Equivalenza per δ:

- $[0]_\delta = \{0\}$ (solo 0 non ha divisori primi / ha tutti i primi come divisori, a seconda della convenzione).
- $[1]_\delta = \{1, -1\}$ (non hanno divisori primi).
- $[6]_\delta = \{\pm 2^n 3^m \mid n, m \geq 1\}$. (Tutti i numeri i cui unici divisori primi sono 2 e 3).
- $[p]_\delta = \{\pm p^k \mid k \geq 1\}$ per p primo.

Relazione di equivalenza Classe di equivalenza Insieme quoziente Aritmetica Modulare

---

2. Esercizi su Strutture Algebriche

Esercizio 1 (Pag 7)

Sia $(\mathbb{Z}_{16}, *)$ con $a * b = \overline{3}ab$.

1. Verificare che è un monoide commutativo.

2. Determinare l'elemento neutro.
3. Determinare gli elementi invertibili (simmetrici).
4. Sia $H = \{\overline{7}, \overline{11}\}$. Verificare se H è una parte stabile di $(\mathbb{Z}_{16}, *)$.
5. Determinare il tipo di struttura $(\mathbb{H}, *)$

Soluzione Parziale (da completare):

- $\mathbb{Z}_{16} = \{\overline{0}, \overline{1}, \dots, \overline{15}\}$.
- **Associatività:** $(a * b) * c = \overline{3}(ab)c = \overline{3}abc$. $a * (b * c) = a * (\overline{3}bc) = \overline{3}a(\overline{3}bc) = \overline{9}abc$.
  - Perché siano uguali, $\overline{3}abc \equiv_{16} \overline{9}abc \implies \overline{6}abc \equiv_{16} \overline{0}$. Questo deve valere per ogni a, b, c. Se $abc = 1$, $\overline{6} \not\equiv_{16} \overline{0}$.
  - **Attenzione:** L'operazione è definita come $\overline{3} \cdot a \cdot b$ (dove a, b sono rappresentanti).
    - $(a * b) * c = (\overline{3}ab) * c = \overline{3}(\overline{3}ab)c = \overline{9}abc$.
    - $a * (b * c) = a * (\overline{3}bc) = \overline{3}a(\overline{3}bc) = \overline{9}abc$.
    - **SÌ, è associativa** (il prodotto in $\mathbb{Z}_{16}$ è associativo).
- **Commutatività:** $a * b = \overline{3}ab$. $b * a = \overline{3}ba$. Poiché $ab = ba$ in $\mathbb{Z}$. **SÌ**.
- **Elemento Neutro** u**:** $a * u = a \implies \overline{3}au \equiv_{16} a$.
  - Se a è invertibile in $\mathbb{Z}_{16}$ (cioè $\text{MCD}(a, 16) = 1$), possiamo dividere per a: $\overline{3}u \equiv_{16} \overline{1}$.
  - Cerchiamo l'inverso di $\overline{3}$ mod 16: $3x \equiv_{16} 1$. $3 \cdot (-5) = -15 \equiv_{16} 1$. Quindi $x = -5 \equiv_{16} 11$.
  - $u \equiv_{16} 11$. Verifichiamo: $a * \overline{11} = \overline{3}a(\overline{11}) = \overline{33}a \equiv_{16} \overline{1}a = a$.
  - **Elemento neutro** $u = \overline{11}$.
- **Monoide Commutativo:** Sì.
- **Elementi Invertibili:** $a * a' = u \implies \overline{3}aa' \equiv_{16} \overline{11}$.
  - Moltiplichiamo per $\overline{11}$ (inverso di $\overline{3}$ mod 16): $\overline{11} \cdot \overline{3}aa' \equiv_{16} \overline{11} \cdot \overline{11}$.
  - $\overline{33}aa' \equiv_{16} \overline{121}$.
  - $\overline{1}aa' \equiv_{16} \overline{121}$. $121 = 7 \cdot 16 + 9$. Quindi $\overline{121} \equiv_{16} \overline{9}$.
  - $aa' \equiv_{16} \overline{9}$.
  - a' esiste se a è invertibile in $(\mathbb{Z}_{16}, \cdot)$ (cioè a dispari) e $a' = \overline{9}a^{-1}$ (dove a^{-1} è l'inverso di a in $\mathbb{Z}_{16}$ rispetto al prodotto standard).
  - Gli invertibili di $\mathbb{Z}_{16}$ (rispetto al prodotto standard) sono i numeri dispari: $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{15}\}$.
  - Questi sono gli elementi invertibili per l'operazione $*$.
- **Parte Stabile** $H = \{\overline{7}, \overline{11}\}$**:**
  - $\overline{7} * \overline{7} = \overline{3} \cdot \overline{7} \cdot \overline{7} = \overline{3} \cdot \overline{49} \equiv_{16} \overline{3} \cdot \overline{1} = \overline{3}$. $\overline{3} \notin H$.
  - **NO,** H **non è una parte stabile.**

---

3. Teoria dei Numeri Elementare

3.1 Determinare Classi in $\mathbb{Z}_{2024}$ (Pag 8)

- $\overline{2027}$ in $\mathbb{Z}_{2024}$: $2027 = 1 \cdot 2024 + 3$. Quindi $\overline{2027} = \overline{3}$.
- $\overline{1024}$ in $\mathbb{Z}_{2024}$: $\overline{1024}$.
- $\overline{-2}$ in $\mathbb{Z}_{2024}$: $-2 + 2024 = 2022$. Quindi $\overline{-2} = \overline{2022}$.
- $\overline{1001!}$ in $\mathbb{Z}_{2024}$: Poiché $2024 = 8 \cdot 11 \cdot 23 = 2^3 \cdot 11 \cdot 23$. Nel prodotto $1001! = 1 \cdot 2 \cdot \dots \cdot 8 \cdot \dots \cdot 11 \cdot \dots \cdot 23 \cdot \dots \cdot 1001$, ci sono i fattori $2^3, 11, 23$. Quindi $2024 \mid 1001!$.
  - Pertanto, $\overline{1001!} = \overline{0}$ in $\mathbb{Z}_{2024}$.

3.2 Equazioni Diofantee Lineari (Pag 9-10)

Un'equazione della forma $ax + by = c$, dove $a, b, c \in \mathbb{Z}$, e si cercano soluzioni intere x, y.

- Ha soluzioni se e solo se $\text{MCD}(a, b) \mid c$.
- **Algoritmo di Euclide Esteso** per trovare $\text{MCD}(a, b)$ e una soluzione particolare (x_0, y_0) per $ax + by = \text{MCD}(a, b)$.
- **Esempio: Risolvere** $209x \equiv_{165} 44$ **(Pag 9).**
  - Equivalente a $209x - 165y = 44$ per qualche $y \in \mathbb{Z}$.
  - Calcoliamo $\text{MCD}(209, 165)$:
    - $209 = 1 \cdot 165 + 44$
    - $165 = 3 \cdot 44 + 33$
    - $44 = 1 \cdot 33 + 11$
    - $33 = 3 \cdot 11 + 0$. Quindi $\text{MCD}(209, 165) = 11$.
  - Poiché $11 \mid 44$ (infatti $44 = 4 \cdot 11$), l'equazione ha soluzioni.
  - L'equazione $209x - 165y = 44$ è equivalente a (dividendo per 11): $19x - 15y = 4$.
  - Cerchiamo una soluzione per $19x - 15y = 1$ (o $19x \equiv_{15} 1$).

        - $19 = 1 \cdot 15 + 4$
        - $15 = 3 \cdot 4 + 3$
        - $4 = 1 \cdot 3 + 1$
        - A ritroso:
            - $1 = 4 - 1 \cdot 3$
            - $1 = 4 - 1 \cdot (15 - 3 \cdot 4) = 4 - 15 + 3 \cdot 4 = 4 \cdot 4 - 1 \cdot 15$
            - $1 = 4 \cdot (19 - 1 \cdot 15) - 1 \cdot 15 = 4 \cdot 19 - 4 \cdot 15 - 1 \cdot 15 = 4 \cdot 19 - 5 \cdot 15$.
        - Abbiamo $19(4) - 15(5) = 1$. Una soluzione per $19x - 15y = 1$ è $x_0 = 4, y_0 = 5$.
    - Per ottenere $19x - 15y = 4$, moltiplichiamo per 4: $19(4 \cdot 4) - 15(5 \cdot 4) = 4$.
        - $19(16) - 15(20) = 4$. Una soluzione particolare è $x_p = 16$.
    - Le soluzioni della congruenza $19x \equiv_{15} 4$ sono $x \equiv_{15} 16 \equiv_{15} 1$.
    - Quindi $x = 1 + 15k$ per $k \in \mathbb{Z}$.
    - L'equazione originale era $209x \equiv_{165} 44$. Le soluzioni sono $x \equiv_{165/11} 1 \equiv_{15} 1$.
    - Ci sono $\text{MCD}(209, 165) = 11$ soluzioni distinte modulo 165.
    - $x \in \{1, 1 + 15, 1 + 2 \cdot 15, \ldots, 1 + 10 \cdot 15\} \pmod{165}$.
    - $x \in \{1, 16, 31, 46, 61, 76, 91, 106, 121, 136, 151\} \pmod{165}$.

Equazione diofantea lineare Algoritmo di Euclide

3.3 Funzione Totiente di Eulero $\varphi(n)$ (Pag 11-12)

- $\varphi(n)$ conta il numero di interi positivi minori o uguali a n che sono **coprimi** con n (cioè $\text{MCD}(k, n) = 1$ per $1 \leq k \leq n$).
- $\varphi(n) = |U(\mathbb{Z}_n)| = |\{k \in \{0, \ldots, n-1\} \mid \text{MCD}(k, n) = 1\}|$.
- **Proprietà:**
    - $\varphi(p) = p - 1$ se p è primo.
    - $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ se p è primo.
    - $\varphi(ab) = \varphi(a)\varphi(b)$ se $\text{MCD}(a, b) = 1$ (moltiplicativa).
- **Esempi:**
    - $\varphi(2) = 1$ ({1})
    - $\varphi(3) = 2$ ({1, 2})
    - $\varphi(4) = \varphi(2^2) = 2^1(2-1) = 2$ ({1, 3})
    - $\varphi(5) = 4$ ({1, 2, 3, 4})
    - $\varphi(2^3) = \varphi(8) = 2^2(2-1) = 4$ ({1, 3, 5, 7})
    - $\varphi(24) = \varphi(2^3 \cdot 3) = \varphi(2^3)\varphi(3) = 4 \cdot 2 = 8$.
    - $\varphi(1500) = \varphi(15 \cdot 100) = \varphi(3 \cdot 5 \cdot 2^2 \cdot 5^2) = \varphi(2^2 \cdot 3^1 \cdot 5^3)$
        - $= \varphi(2^2)\varphi(3)\varphi(5^3) = (2^1(2-1)) \cdot (3-1) \cdot (5^2(5-1))$
        - $= (2 \cdot 1) \cdot 2 \cdot (25 \cdot 4) = 2 \cdot 2 \cdot 100 = 400$.

Funzione totiente di Eulero

3.4 Teorema di Fermat-Eulero (Pag 13)

- Siano $a, n \in \mathbb{Z}$ con $n \geq 1$. Se $\text{MCD}(a, n) = 1$ (cioè a e n sono coprimi), allora:

$$a^{\varphi(n)} \equiv_n 1$$

- **Piccolo Teorema di Fermat:** Se p è un numero primo e $p \nmid a$ (cioè $\text{MCD}(a, p) = 1$), allora $a^{p-1} \equiv_p 1$.
    - Corollario: Per ogni intero a e primo p, $a^p \equiv_p a$.

Teorema di Eulero (aritmetica modulare) Piccolo teorema di Fermat

---

4. Calcolo Combinatorio

Studio dei modi di contare e arrangiare oggetti.

4.1 Fattoriale e Coefficiente Binomiale (Pag 14)

- **Fattoriale:** $n! = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1$ per $n \geq 1$. $0! = 1$.
- **Coefficiente Binomiale:** "n su k" o "n choose k".

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\ldots(n-k+1)}{k!} \quad \text{per } 0 \leq k \leq n$$

- **Proprietà:**
    - $\binom{n}{0} = 1$, $\binom{n}{n} = 1$.

- $\binom{n}{1} = n$, $\binom{n}{n-1} = n$.
- $\binom{n}{k} = \binom{n}{n-k}$ (Simmetria).

4.2 Identità Combinatorie (Pag 15-18)

1. **Identità di Pascal (o Regola di Stiefel):** Per $1 \leq k \leq n$:

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$$

   - **Dimostrazione (Pag 15):**
     - $\frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!}$
     - $= \frac{n!(n-k+1)}{k!(n-k+1)!} + \frac{n!k}{k!(n-k+1)!}$
     - $= \frac{n!(n-k+1+k)}{k!(n-k+1)!} = \frac{n!(n+1)}{k!((n+1)-k)!} = \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}$.
2. **Numero di Sottoinsiemi (Pag 16):** Un insieme S con $|S| = n$ elementi possiede esattamente $\binom{n}{k}$ sottoinsiemi di cardinalità k.
   - **Dimostrazione per induzione su n (Pag 16-18):**
     - Base $n = 0$: $S = \emptyset$, $|S| = 0$. Unico sottoinsieme è $\emptyset$ (cardinalità 0). $\binom{0}{0} = 1$. Vero.
     - Passo induttivo: Assumiamo P_n vera (per ogni insieme di n elementi, il numero di sottoinsiemi di card k è $\binom{n}{k}$).
       Consideriamo T con $|T| = n+1$. Sia $a \in T$. Sia $S' = T \setminus \{a\}$, quindi $|S'| = n$.
       I sottoinsiemi $C \subseteq T$ di cardinalità k si dividono in due tipi:
       - Tipo $\mathcal{A}$: C non contiene a. Allora $C \subseteq S'$. Per ipotesi induttiva, ce ne sono $\binom{n}{k}$.
       - Tipo $\mathcal{B}$: C contiene a. Allora $C = C' \cup \{a\}$ dove $C' \subseteq S'$ e $|C'| = k-1$. Per ipotesi induttiva, ce ne sono $\binom{n}{k-1}$.
       - Il numero totale di sottoinsiemi di T di cardinalità k è $|\mathcal{A}| + |\mathcal{B}| = \binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ (per Identità di Pascal). P_{n+1} è vera.
3. **Somma dei Coefficienti Binomiali (Corollario di 2, Pag 18):**

$$\sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$$

   - Questo è il numero totale di sottoinsiemi di un insieme di n elementi, cioè $|P(S)| = 2^{|S|}$.
4. **Numero di Applicazioni Iniettive (Pag 18-20):**
   Il numero di applicazioni iniettive $f : S \to T$ con $|S| = n$ e $|T| = m$ (e $n \leq m$) è:

$$m \cdot (m-1) \cdot \cdots \cdot (m-n+1) = \frac{m!}{(m-n)!} = P(m,n) \quad \text{(Disposizioni semplici)}$$

   - **Dimostrazione per induzione su n (Pag 19-20):**
     - Base $n = 1$: $S = \{s_1\}$. Per $f(s_1)$ ci sono m scelte in T. Numero app. iniettive = m. Formula: m. Vero.
     - Passo induttivo: Assumiamo P_n vera. Consideriamo S' con $|S'| = n+1$. Sia $a_{n+1} \in S'$. Sia $S = S' \setminus \{a_{n+1}\}$, $|S| = n$.
       - Per $f(a_{n+1})$ ci sono m scelte in T. Sia $b_i = f(a_{n+1})$.
       - Ora dobbiamo definire f sul resto di S in modo iniettivo su $T \setminus \{b_i\}$ (che ha $m-1$ elementi).
       - Per ipotesi induttiva, ci sono $(m-1)(m-2)\dots((m-1)-n+1)$ modi per farlo.
       - Numero totale: $m \cdot [(m-1)(m-2)\dots(m-n)] = m(m-1)\dots(m-(n+1)+1)$. P_{n+1} è vera.
   - Se $n = m$, il numero di applicazioni biettive (permutazioni di T se S è un insieme di riferimento) è $n!$.

4.3 Binomio di Newton (Pag 21-22)

Per ogni a, b in un anello commutativo (o anche solo elementi che commutano, $ab = ba$) e $n \in \mathbb{N}$:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \cdots + \binom{n}{n} b^n$$

- **Dimostrazione per induzione su n (Pag 21-22):**
  - Base $n = 1$: $(a+b)^1 = a+b$. $\binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = 1a + 1b = a+b$. Vero.
  - Passo induttivo: Assumiamo P_n vera.
    - $(a+b)^{n+1} = (a+b)^n (a+b) = (\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k)(a+b)$
    - $= \sum \binom{n}{k} a^{n-k+1} b^k + \sum \binom{n}{k} a^{n-k} b^{k+1}$
    - Riorganizzando le somme e usando l'identità di Pascal si ottiene la formula per $n+1$.
- **Triangolo di Tartaglia (o di Pascal):** Fornisce i coefficienti binomiali.

Coefficiente binomiale Identità di Pascal Binomio di Newton Triangolo di Tartaglia

4.4 Disuguaglianza $n! \geq 2^n$ (Pag 23)

Verificare per quali $n \in \mathbb{N}$ vale $n! \geq 2^n$.

- $n = 0 : 0! = 1, 2^0 = 1$. $1 \geq 1$. Vero.
- $n = 1 : 1! = 1, 2^1 = 2$. $1 \geq 2$. Falso.
- $n = 2 : 2! = 2, 2^2 = 4$. $2 \geq 4$. Falso.
- $n = 3 : 3! = 6, 2^3 = 8$. $6 \geq 8$. Falso.
- $n = 4 : 4! = 24, 2^4 = 16$. $24 \geq 16$. Vero.
- **Ipotesi:** Vale per $n = 0$ e per $n \geq 4$.
- **Dimostrazione per induzione per $n \geq 4$:**
  - Base P_4: $4! = 24 \geq 2^4 = 16$. Vero.
  - Passo induttivo: Assumiamo P_k vera per $k \geq 4$, cioè $k! \geq 2^k$.
    Vogliamo dimostrare P_{k+1}: $(k+1)! \geq 2^{k+1}$.
    - $(k+1)! = (k+1) \cdot k!$.
    - Per ipotesi induttiva, $k! \geq 2^k$. Quindi $(k+1)! \geq (k+1) \cdot 2^k$.
    - Poiché $k \geq 4$, allora $k + 1 \geq 5 > 2$.
    - Quindi $(k+1) \cdot 2^k > 2 \cdot 2^k = 2^{k+1}$.
    - Dunque $(k+1)! \geq 2^{k+1}$. P_{k+1} è vera.

Riepilogo Veloce Lezione 16

- Abbiamo definito le **Relazioni di Equivalenza** (riflessiva, simmetrica, transitiva) e visto come la congruenza modulo n ne sia un esempio.
- Abbiamo analizzato le **classi di equivalenza** e l'**insieme quoziente**.
- Abbiamo svolto un esercizio su una **struttura algebrica in $\mathbb{Z}_{16}$**.
- Abbiamo rivisto le **Equazioni Diofantee Lineari** e l'uso dell'Algoritmo di Euclide.
- Abbiamo introdotto la **Funzione Totiente di Eulero $\varphi(n)$** e le sue proprietà.
- Abbiamo enunciato il **Teorema di Fermat-Eulero**.
- Abbiamo esplorato il **Calcolo Combinatorio**: fattoriale, coefficiente binomiale, Identità di Pascal, numero di sottoinsiemi, numero di applicazioni iniettive, Binomio di Newton.
- Abbiamo dimostrato la disuguaglianza $n! \geq 2^n$ per $n = 0$ e $n \geq 4$.

Prossimi Passi

- Assicurati di aver compreso bene come si dimostrano le proprietà di una relazione per verificarne l'equivalenza.
- Fai pratica con il calcolo di $\varphi(n)$ e l'applicazione del Teorema di Fermat-Eulero.
- Gli esercizi di calcolo combinatorio sono fondamentali per molte aree della matematica.

Lezione 17: Relazioni d'Ordine

Data: 20/05/2025 (come da note)
Argomenti: Relazione d'Ordine (Largo e Stretto), Corrispondenza tra Ordini, Ordine Totale/Parziale, Copertura, Diagrammi di Hasse, Elementi Minimo/Massimo, Elementi Minimali/Massimali, Insiemi Ben Ordinati, Minoranti/Maggioranti, Inf/Sup.

#tag/relations #tag/order-theory #tag/posets #tag/hasse-diagrams #tag/min-max-elements #tag/well-ordering #tag/algebra-avanzata

---

1. Definizione di Relazione d'Ordine

Sia S un insieme non vuoto e $\mathcal{R}$ una relazione binaria su S.

- **Relazione d'Ordine (Largo) (Pag 1):**
  La coppia $(S, \mathcal{R})$ è un **insieme ordinato** e $\mathcal{R}$ è una **relazione d'ordine** (o ordine parziale, ordine largo) se $\mathcal{R}$ soddisfa le seguenti tre proprietà:
  1. **Riflessiva:** $\forall x \in S, x\mathcal{R}x$.
  2. **Antisimmetrica:** $\forall x, y \in S, (x\mathcal{R}y \wedge y\mathcal{R}x) \implies x = y$.
  3. **Transitiva:** $\forall x, y, z \in S, (x\mathcal{R}y \wedge y\mathcal{R}z) \implies x\mathcal{R}z$.
  - *Notazione comune:* Spesso si usa il simbolo $\leq$ (o $\preceq$) per denotare una generica relazione d'ordine largo.
- **Relazione d'Ordine Stretto (Pag 1):**
  Una relazione $\mathcal{R}'$ su S è una **relazione d'ordine stretto** se soddisfa:
  1. **Antiriflessiva (o Irriflessiva):** $\forall x \in S, \neg(x\mathcal{R}'x)$.
  2. **Transitiva:** $\forall x, y, z \in S, (x\mathcal{R}'y \wedge y\mathcal{R}'z) \implies x\mathcal{R}'z$.
  - *Notazione comune:* Spesso si usa il simbolo $<$ (o $\prec$) per denotare una generica relazione d'ordine stretto.

> **Una relazione d'ordine stretto è automaticamente asimmetrica. Se fosse $x\mathcal{R}'y$ e $y\mathcal{R}'x$, per transitività avremmo $x\mathcal{R}'x$, il che contraddice l'antiriflessività.**

Relazione d'ordine Relazione d'ordine stretto

---

2. Corrispondenza tra Ordine Largo e Stretto (Pag 2)

Esiste una corrispondenza biunivoca tra relazioni d'ordine largo ($\mathcal{R}$) e relazioni d'ordine stretto ($\mathcal{R}'$) sullo stesso insieme S.

- **Da Ordine Largo $\mathcal{R}$ a Ordine Stretto $\mathcal{R}'$:**

$$x\mathcal{R}'y \iff (x\mathcal{R}y \land x \neq y)$$

  - **Spiegazione:** x è strettamente minore di y se x è minore o uguale a y, ma x non è uguale a y.
- **Da Ordine Stretto $\mathcal{R}'$ a Ordine Largo $\mathcal{R}$:**

$$x\mathcal{R}y \iff (x\mathcal{R}'y \lor x = y)$$

  - **Spiegazione:** x è minore o uguale a y se x è strettamente minore di y oppure x è uguale a y.

Esempio Illustrativo

Consideriamo l'insieme $S = \{a, b, c\}$ e una relazione d'ordine largo $\mathcal{R}$ su S definita come:

$$\mathcal{R} = \{(a,a), (b,b), (c,c), (a,b), (a,c), (b,c)\}$$

- **Passaggio a Ordine Stretto $\mathcal{R}'$:**

$$\mathcal{R}' = \{(a,b), (a,c), (b,c)\}$$

  Nota che le coppie (a,a), (b,b), (c,c) sono escluse perché $x \neq y$.
- **Ritorno a Ordine Largo $\mathcal{R}$:**
  Ricostruiamo $\mathcal{R}$ da $\mathcal{R}'$:

$$\mathcal{R} = \{(a,a), (b,b), (c,c), (a,b), (a,c), (b,c)\}$$

  La relazione originale è recuperata.

Verifica che la costruzione funziona (Pag 7-8):

Se $\mathcal{R}'$ è un ordine stretto (antiriflessivo, transitivo) e definiamo $\mathcal{R}$ come $x\mathcal{R}y \iff (x\mathcal{R}'y \lor x = y)$, allora $\mathcal{R}$ è un ordine largo:

1. **Riflessiva:** $x\mathcal{R}x \iff (x\mathcal{R}'x \lor x = x)$. Poiché $x = x$ è vero, $x\mathcal{R}x$ è vero.
2. **Antisimmetrica:** Supponiamo $x\mathcal{R}y \land y\mathcal{R}x$.
   - $x\mathcal{R}y \implies (x\mathcal{R}'y \lor x = y)$.
   - $y\mathcal{R}x \implies (y\mathcal{R}'x \lor y = x)$.
   - Se $x \neq y$: allora deve essere $x\mathcal{R}'y$ e $y\mathcal{R}'x$. Ma questo contraddice l'asimmetria (e quindi l'antiriflessività) di $\mathcal{R}'$.
   - Quindi, l'unica possibilità è $x = y$.
3. **Transitiva:** Supponiamo $x\mathcal{R}y \land y\mathcal{R}z$. Dobbiamo mostrare $x\mathcal{R}z$.
   - Analizziamo i 4 casi possibili dalle definizioni:
     - (i) $x = y \land y = z \implies x = z \implies x\mathcal{R}z$.
     - (ii) $x = y \land y\mathcal{R}'z \implies x\mathcal{R}'z \implies x\mathcal{R}z$.
     - (iii) $x\mathcal{R}'y \land y = z \implies x\mathcal{R}'z \implies x\mathcal{R}z$.
     - (iv) $x\mathcal{R}'y \land y\mathcal{R}'z \implies x\mathcal{R}'z$ (per transitività di $\mathcal{R}'$) $\implies x\mathcal{R}z$.
   - In tutti i casi, $x\mathcal{R}z$.

---

3. Ordine Totale vs. Ordine Parziale (Pag 2)

Sia $(S, \mathcal{R})$ un insieme ordinato (con ordine largo).

- L'ordine $\mathcal{R}$ è **totale** (o lineare) se per ogni coppia di elementi $x, y \in S$, vale sempre che $x\mathcal{R}y$ oppure $y\mathcal{R}x$.

$$\forall x, y \in S, \quad (x\mathcal{R}y \lor y\mathcal{R}x)$$

    - **Spiegazione:** Ogni coppia di elementi è confrontabile.
- Se un ordine non è totale, è detto **parziale**.
- **Esempi:**
    - $(\mathbb{N}, \leq)$ con l'usuale "minore o uguale" è un **ordine totale**.
    - $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$ sono ordini totali.
    - $(P(S), \subseteq)$ (insieme delle parti di S con l'inclusione insiemistica), se $|S| \geq 2$, è un **ordine parziale** (non totale).
        - Esempio (Pag 3): $S = \{a, b\}$. $P(S) = \{\emptyset, \{a\}, \{b\}, S\}$.
        - $\{a\} \not\subseteq \{b\}$ e $\{b\} \not\subseteq \{a\}$. I due elementi $\{a\}$ e $\{b\}$ non sono confrontabili.

Ordine totale Ordine parziale

---

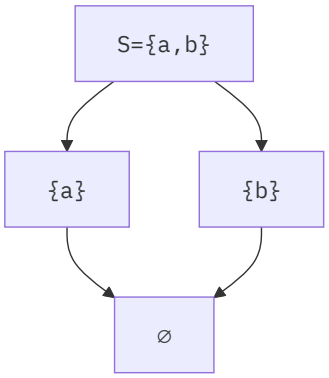
4. Copertura e Diagrammi di Hasse

Per visualizzare insiemi parzialmente ordinati finiti.

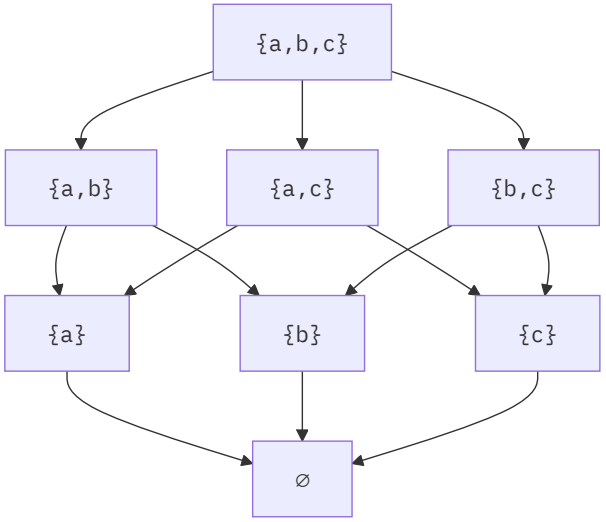
- **Copertura (Pag 3):** Sia $(S, \mathcal{R})$ un insieme ordinato. Diciamo che b **copre** a (o a è coperto da b) se $a\mathcal{R}'b$ (cioè $a\mathcal{R}b$ e $a \neq b$) e non esiste nessun elemento $c \in S$ tale che $a\mathcal{R}'c$ e $c\mathcal{R}'b$.

$$b \text{ copre } a \iff (a\mathcal{R}'b \wedge \neg(\exists c \in S : a\mathcal{R}'c \wedge c\mathcal{R}'b))$$

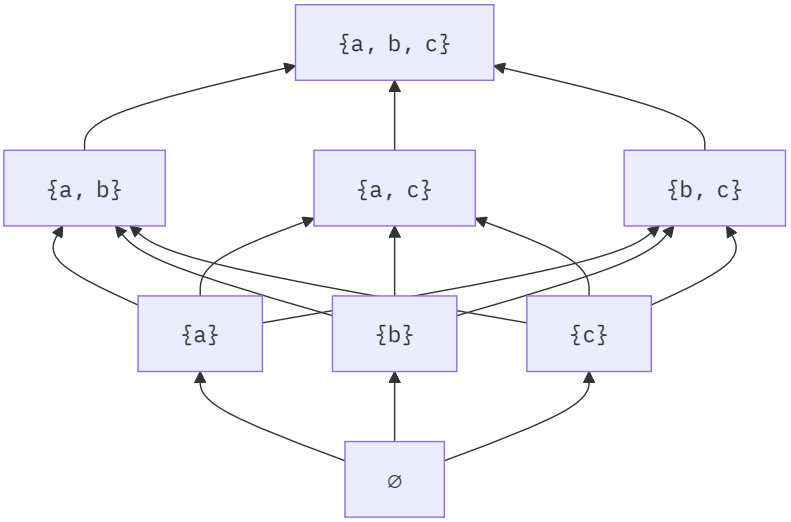
    - **Spiegazione:** b è "immediatamente sopra" ad a nell'ordine, senza elementi intermedi.
- **Diagramma di Hasse (Pag 4):** Una rappresentazione grafica di un insieme finito parzialmente ordinato $(S, \mathcal{R})$.
    1. I vertici del diagramma sono gli elementi di S.
    2. Se b copre a, si disegna un segmento da a a b, con b posizionato più in alto di a.
    3. Non si disegnano:
        - Loop (per riflessività, implicita).
        - Archi che possono essere dedotti per transitività (es. se c copre b e b copre a, non si disegna un arco diretto da a a c).
        - Frecce (la direzione "verso l'alto" è implicita).
- **Esempi di Diagrammi di Hasse:**
    - $(P(S), \subseteq)$ **con** $S = \{a, b\}$ **(Pag 4):**
        - $P(S) = \{\emptyset, \{a\}, \{b\}, S\}$.
        - Coperture: S copre $\{a\}$ e $\{b\}$. $\{a\}$ copre $\emptyset$. $\{b\}$ copre $\emptyset$.



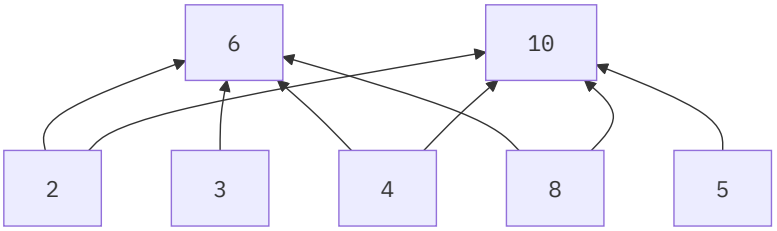
    - $(P(S), \subseteq)$ **con** $S = \{a, b, c\}$ **(Pag 4):**



- $(P(S), \mathcal{R})$ **con** $S = \{a, b, c\}$ **e** $X\mathcal{R}Y \iff (X = Y) \vee (|X| < |Y|)$ **(Pag 5):**
  - Questo è un ordine per livelli basato sulla cardinalità. Un insieme Y copre un insieme X se $|Y| = |X| + 1$.
  - Ecco il diagramma di Hasse che rappresenta questa relazione di copertura:



  - **Spiegazione del Diagramma:** Gli elementi sono disposti verticalmente in base alla loro cardinalità (dal basso verso l'alto). Una freccia da X a Y indica che Y copre X, il che per questa relazione significa che $|Y| = |X| + 1$. Ad esempio, da $\{a\}$ (cardinalità 1) ci sono frecce verso tutti gli insiemi di cardinalità 2 ($\{a, b\}, \{a, c\}, \{b, c\}$), perché tutti questi insiemi hanno cardinalità 2 e non esiste un insieme Z con cardinalità strettamente compresa tra 1 e 2.
- $(\{2, 3, 4, 5, 6, 8, 10\}, \mathcal{R})$ **con** $a\mathcal{R}b \iff (a = b) \vee (\pi(a) \subset \pi(b))$**, dove** $\pi(n)$ **è l'insieme dei divisori primi di** n **(Pag 6):**
  - $\pi(2) = \{2\}$, $\pi(3) = \{3\}$, $\pi(4) = \{2\}$, $\pi(5) = \{5\}$, $\pi(6) = \{2, 3\}$, $\pi(8) = \{2\}$, $\pi(10) = \{2, 5\}$.
  - La relazione d'ordine è basata sull'inclusione stretta tra gli insiemi dei divisori primi. Un elemento b copre a se $\pi(a) \subset \pi(b)$ e non esiste c tale che $\pi(a) \subset \pi(c) \subset \pi(b)$.
  - Ecco il diagramma di Hasse per questo insieme e questa relazione:



  - **Spiegazione del Diagramma:** Gli elementi minimali (quelli i cui insiemi di divisori primi non contengono strettamente altri insiemi dell'insieme) sono 2, 3, 4, 5, 8 e sono posizionati in basso. Gli elementi massimali (quelli i cui insiemi di divisori primi non sono contenuti strettamente in altri insiemi dell'insieme) sono 6 e 10 e sono posizionati in alto. Le frecce indicano le relazioni di copertura: ad esempio, 6 copre 2, 3, 4, e 8 perché i loro insiemi di divisori primi sono strettamente contenuti in $\pi(6) = \{2, 3\}$ e non c'è nessun altro elemento c nell'insieme con un $\pi(c)$ "intermedio".

Diagramma di Hasse

---

5. Elementi Speciali in Insiemi Ordinati

Sia $(S, \leq)$ un insieme parzialmente ordinato.

- **Elemento Minimo (Pag 11):** $a \in S$ è **minimo** di S se $a \leq x$ per ogni $x \in S$.
  - Se esiste, l'elemento minimo è **unico**.
  - **Dimostrazione unicità:** Se m_1, m_2 sono minimi, allora $m_1 \leq m_2$ (perché m_1 è minimo) e $m_2 \leq m_1$ (perché m_2 è minimo). Per antisimmetria, $m_1 = m_2$.
- **Elemento Massimo (Pag 11):** $a \in S$ è **massimo** di S se $x \leq a$ per ogni $x \in S$.
  - Se esiste, l'elemento massimo è **unico**.
- **Esempi:**
  - $(P(S), \subseteq)$: $\min(P(S)) = \emptyset$, $\max(P(S)) = S$.
  - $(\mathbb{N}, \leq)$: $\min(\mathbb{N}) = 0$. Non esiste $\max(\mathbb{N})$.
  - $(\mathbb{N}, |)$ (divisibilità su $\mathbb{N} = \{1, 2, \dots\}$): $\min(\mathbb{N}, |) = 1$. $\max(\mathbb{N}, |)$ non esiste (ma 0 se si include in $\mathbb{N}_0$ sarebbe il massimo, $x|0$ per ogni x).
  - $(\mathbb{N} \setminus \{1\}, |)$: Non esiste minimo (es. 2 e 3 sono incomparabili e non dividono tutti gli altri). Non esiste massimo.

- **Elemento Minimale (Pag 14):** $a \in S$ è **minimale** se non esiste alcun $x \in S$ tale che $x < a$ (cioè $x \leq a \wedge x \neq a$).
  - Equivalentemente: $\forall x \in S, x \leq a \implies x = a$.
- **Elemento Massimale (Pag 16):** $a \in S$ è **massimale** se non esiste alcun $x \in S$ tale che $a < x$.
  - Equivalentemente: $\forall x \in S, a \leq x \implies x = a$.
- **Relazioni tra Minimo/Massimo e Minimale/Massimale (Pag 16-17):**
  - Se a è minimo, allora a è l'**unico** elemento minimale.
  - Se a è massimo, allora a è l'**unico** elemento massimale.
  - Un elemento minimale (o massimale) **non è necessariamente unico**.
  - Se esiste un elemento minimale unico, **non è detto** che sia il minimo dell'insieme (a meno che l'ordine non sia totale).
- **Esempi:**
  - $(\mathbb{N} \setminus \{1\}, |)$: Gli elementi minimali sono tutti i numeri primi. Non c'è un minimo.
  - $(P(S) \setminus \{\emptyset\}, \subseteq)$: Gli elementi minimali sono i singleton $\{s\}$ per ogni $s \in S$.
- **Teorema (Pag 18):** Ogni insieme finito non vuoto parzialmente ordinato possiede almeno un elemento minimale e almeno un elemento massimale.
- **Controesempio per insiemi infiniti (Pag 18):** $(\mathbb{Z}, \leq)$ non ha né minimali né massimali.

Elemento minimale e massimale Elemento minimo e massimo

---

6. Insiemi Ben Ordinati e Operazioni su Insiemi Ordinati

- **Insieme Ben Ordinato (Pag 21):** Un insieme parzialmente ordinato $(S, \leq)$ è **ben ordinato** se ogni suo sottoinsieme non vuoto $X \subseteq S$ ammette un elemento **minimo**.
  - Un insieme ben ordinato è **sempre totalmente ordinato**. (Se non fosse totale, esisterebbero a, b non confrontabili. Allora il sottoinsieme $\{a, b\}$ non avrebbe minimo).
  - Esempio: $(\mathbb{N}, \leq)$ è ben ordinato (Principio del Buon Ordinamento).
  - Controesempio: $(\mathbb{Z}, \leq)$ non è ben ordinato (es. $\mathbb{Z}$ stesso non ha minimo). $(\mathbb{R}_{\geq 0}, \leq)$ non è ben ordinato (es. $(0, 1)$ non ha minimo).

Buon ordinamento

- **Minoranti e Maggioranti (Pag 22):** Sia $(S, \leq)$ un insieme ordinato e $X \subseteq S$ un sottoinsieme.
  - $a \in S$ è un **minorante** di X se $a \leq x$ per ogni $x \in X$.
  - $a \in S$ è un **maggiorante** di X se $x \leq a$ per ogni $x \in X$.
  - Se un minorante a di X appartiene anche a X, allora $a = \min(X)$.
- **Estremo Inferiore (Infimum) e Superiore (Supremum) (Pag 23):**
  - $\inf(X) = \max(\text{insieme dei minoranti di } X)$, se esiste. (Il più grande dei minoranti).
  - $\sup(X) = \min(\text{insieme dei maggioranti di } X)$, se esiste. (Il più piccolo dei maggioranti).
  - Se $\min(X)$ esiste, allora $\inf(X) = \min(X)$. Se $\max(X)$ esiste, allora $\sup(X) = \max(X)$.
  - **Esempio** $(\mathbb{N}, |)$: $X = \{60, 54\}$.
    - $60 = 2^2 \cdot 3 \cdot 5$. $54 = 2 \cdot 3^3$.
    - Minoranti (divisori comuni): $\{1, 2, 3, 6\}$.
    - $\inf(\{60, 54\}) = \max(\{1, 2, 3, 6\}) = 6 = \text{MCD}(60, 54)$.
    - Maggioranti (multipli comuni): $\{2^2 \cdot 3^3 \cdot 5 \cdot k \mid k \in \mathbb{N}^*\} = \{540, 1080, \dots\}$.
    - $\sup(\{60, 54\}) = \min(\{540, 1080, \dots\}) = 540 = \text{mcm}(60, 54)$.

Minorante e maggiorante Estremo superiore e inferiore

---

7. Esercizi Proposti

Esercizio 1 (Pag 24 - Ordine tramite Funzione)

Siano $(S, \leq_S)$ e $(T, \leq_T)$ insiemi ordinati, e $f : S \to T$ una funzione.
Definiamo una relazione $\leq_f$ su S come:

$$a \leq_f b \iff (a = b) \vee (f(a) <_T f(b))$$

(dove $<_T$ è l'ordine stretto associato a $\leq_T$).
Verificare se $\leq_f$ è una relazione d'ordine su S.

Casi specifici da analizzare (Pag 24-28):

1. $S = \mathbb{N} \times \mathbb{N}$, $T = (\mathbb{N}, \leq)$, $f(a, b) = a + b$.
   Determinare $\vec{f}(\mathbb{N} \times \mathbb{N})$, $\min(\vec{f}(\mathbb{N} \times \mathbb{N}))$.

Determinare $\overleftarrow{f}(\{0\})$, $\overleftarrow{f}(\{1\})$.

2. $S = \mathbb{N} \times \mathbb{N}$, $T = (\mathbb{N}, |)$ (divisibilità, $\mathbb{N} = \{0, 1, 2, \dots\}$), $f(a, b) = a \cdot b$.
   Determinare $\vec{f}(\mathbb{N} \times \mathbb{N})$, $\min(\vec{f}(\mathbb{N} \times \mathbb{N}))$, $\max(\vec{f}(\mathbb{N} \times \mathbb{N}))$.
   Determinare $\overleftarrow{f}(\{1\})$, $\overleftarrow{f}(\{0\})$ (se $0 \in T$).
3. $S = \mathbb{N}^* \times \mathbb{N}^*$, $T = (\mathbb{N}, \leq)$, $f(a, b) = a^b$.
   Determinare $\vec{f}(\mathbb{N}^* \times \mathbb{N}^*)$, $\min(\vec{f}(\mathbb{N}^* \times \mathbb{N}^*))$.
   Determinare $\overleftarrow{f}(\{1\})$.
4. S_{10} un insieme con $|S_{10}| = 10$. $S = P(S_{10})$, $T = (\mathbb{N}, |)$, $f(X) = |X|$.
   Determinare $\vec{f}(P(S_{10}))$.
   Disegnare il diagramma di Hasse di $(P(S_{10}), |_f)$ (dove $|_f$ è l'ordine indotto da f e dalla divisibilità su $\mathbb{N}$).
5. $S = \mathbb{Z}$, $T = (\mathbb{Z}, \leq)$, $f(a) = 2^{|a|}$.
   Determinare $\vec{f}(\mathbb{Z})$, $\min(\vec{f}(\mathbb{Z}))$.
   Determinare $\overleftarrow{f}(\{1\})$.

Esercizio 2 (Pag 30 - DA FARE)

Sia $(P(S), \mathcal{R})$ con $S = \{a, b, c\}$ e $X \mathcal{R} Y \iff (X = Y) \vee (|X| < |Y|)$.
Trovare gli elementi minimali e massimali di $P(S) \setminus \{\{a, b\}, \{a, c\}\}$.
Disegnare il diagramma di Hasse di questo sottoinsieme ordinato.

Riepilogo Veloce Lezione 17

- Abbiamo definito le **relazioni d'ordine largo** (riflessiva, antisimmetrica, transitiva) e **stretto** (antiriflessiva, transitiva) e la loro corrispondenza.
- Un ordine è **totale** se tutti gli elementi sono confrontabili, altrimenti è **parziale**.
- I **Diagrammi di Hasse** visualizzano ordini finiti mostrando solo le relazioni di copertura.
- Abbiamo distinto tra elementi **minimo/massimo** (unici, se esistono) ed elementi **minimali/massimali** (possono essere multipli).
- Un insieme è **ben ordinato** se ogni suo sottoinsieme non vuoto ha un minimo (implica ordine totale).
- Abbiamo definito **minoranti, maggioranti, infimum (MCD generalizzato) e supremum (mcm generalizzato)**.

Prossimi Passi

- Svolgi gli esercizi proposti per familiarizzare con i diversi tipi di ordine e gli elementi speciali.
- Le relazioni d'ordine sono fondamentali per strutture come i reticoli e le algebre di Boole.
- Le relazioni di equivalenza (che vedremo) sono l'altro tipo principale di relazione con proprietà strutturali importanti.}

Lezione Bonus (18): Introduzione alla Teoria dei Grafi

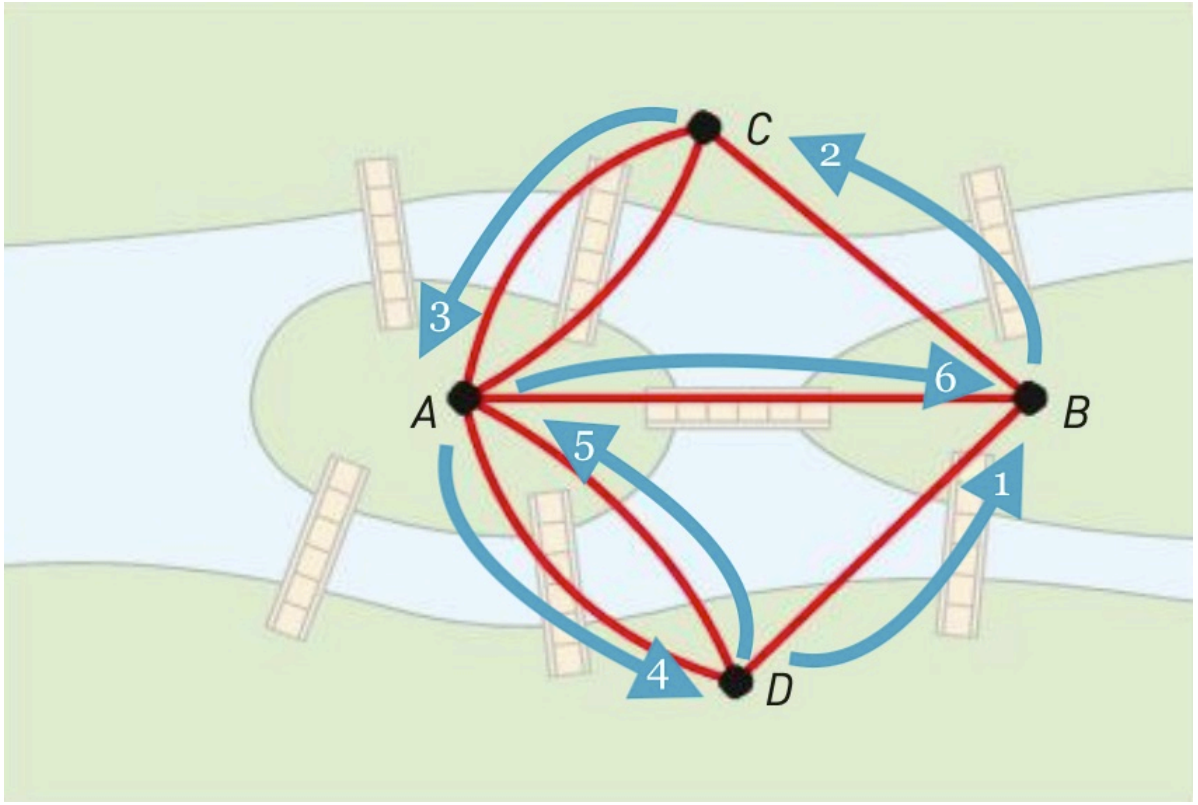
Data: 22/05/2025 (come da note)
Argomenti: Problema Ponti di Königsberg, Definizione Grafo non orientato, Vertici, Lati, Grado, Teorema Somma Gradi, Vertici Dispari, Grafi Regolari, Grafi Completi, Cammini, Connessione, Componenti Connesse, Alberi, Circuiti Euleriani, Grafo Complementare, Multigrafi.

#tag/theory-of-graphs #tag/eulerian-circuits #tag/trees #tag/graph-connectivity #tag/algebra-avanzata

---

1. Il Problema dei Ponti di Königsberg (Eulero, 1736)

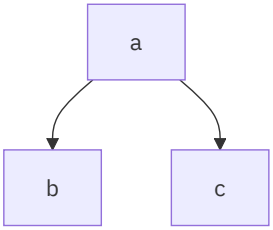
- **Contesto Storico (Pag 1):** La città di Königsberg aveva 7 ponti che collegavano due isole e le sponde del fiume Pregel. Il problema era: è possibile fare una passeggiata attraversando ogni ponte una e una sola volta?
  - Eulero dimostrò che non era possibile e, nel farlo, pose le basi della teoria dei grafi.
- **Modellizzazione con Grafo (Pag 1):**
  - Le aree di terra (A, B, C, D) diventano i **nodi** (o **vertici**) del grafo.
  - I ponti (1, 2, 3, 4, 5, 6, 7) diventano gli **archi** (o **lati**) che collegano i nodi.



---

2. Definizioni Fondamentali dei Grafi (Non Orientati)

- **Relazione Binaria per Grafi Semplici (Pag 2):**
  - Un grafo semplice può essere visto come una coppia $(V, \mathcal{R})$ dove $V \neq \emptyset$ è l'insieme dei **vertici** e $\mathcal{R}$ è una relazione binaria su V che è:
    1. **Antiriflessiva:** $\forall v \in V, \neg(v \mathcal{R} v)$ (non ci sono cappi/loop, cioè lati che collegano un vertice a se stesso).
    2. **Simmetrica:** $\forall v, w \in V, v \mathcal{R} w \implies w \mathcal{R} v$ (se v è collegato a w, allora w è collegato a v; i lati non hanno una direzione).
  - Il **grafo della relazione** $G \subseteq V \times V$ contiene le coppie (v, w) tali che $v \mathcal{R} w$.
  - Per un grafo non orientato, se $(v, w) \in G$, allora anche $(w, v) \in G$.
- **Definizione Formale di Grafo (Non Orientato Semplice) (Pag 3):**
  - Un **grafo** G è una coppia (V, L) dove:
    - V è un insieme finito e non vuoto di elementi chiamati **vertici** (o nodi).
    - L è un insieme di sottoinsiemi di V di cardinalità 2, chiamati **lati** (o archi, spigoli).
      - Un lato $l \in L$ è della forma $\{v, w\}$ con $v, w \in V$ e $v \neq w$. Questo rappresenta un collegamento non orientato tra v e w.
      - Notazione: $L \subseteq P_2(V)$, dove $P_2(V)$ è l'insieme di tutti i sottoinsiemi di V con esattamente 2 elementi.
      - Se $|V| = n$, allora $|P_2(V)| = \binom{n}{2} = \frac{n(n-1)}{2}$ (numero massimo di lati in un grafo semplice con n vertici).
  - **Esempio (Pag 3):** $V = \{a, b, c\}$, $L = \{\{a, b\}, \{a, c\}\}$.
    - Questo grafo ha 3 vertici. Il vertice a è collegato a b e a c. b e c non sono collegati tra loro.
  - Un **grafo** G è una coppia (V, L) dove:
    - V è un insieme finito e non vuoto di elementi chiamati **vertici** (o nodi).
    - L è un insieme di sottoinsiemi di V di cardinalità 2, chiamati **lati** (o archi, spigoli).
      - Un lato $l \in L$ è della forma $\{v, w\}$ con $v, w \in V$ e $v \neq w$. Questo rappresenta un collegamento non orientato tra v e w.
      - Notazione: $L \subseteq P_2(V)$, dove $P_2(V)$ è l'insieme di tutti i sottoinsiemi di V con esattamente 2 elementi.
      - Se $|V| = n$, allora $|P_2(V)| = \binom{n}{2} = \frac{n(n-1)}{2}$ (numero massimo di lati in un grafo semplice con n vertici).
    - **Esempio (Pag 3):** $V = \{a, b, c\}$, $L = \{\{a, b\}, \{a, c\}\}$.
    - Questo grafo ha 3 vertici. Il vertice a è collegato a b e a c. b e c non sono collegati tra loro.



- **Grado di un Vertice (Pag 4):**
  - Il **grado** di un vertice $v \in V$, denotato $d(v)$ (o $\deg(v)$), è il numero di lati incidenti a v.
  - In un grafo semplice, è il numero di vertici adiacenti a v.
  - **Vertice Isolato:** Un vertice v è isolato se $d(v) = 0$.
  - **Esempio (Pag 4):** $V = \{a, b, c, d, e\}$, $L = \{l_1 = \{a, b\}, l_2 = \{b, c\}, l_3 = \{a, d\}, l_4 = \{c, d\}, l_5 = \{d, e\}\}$.
    - $d(a) = 2$ (lati l_1, l_3)
    - $d(b) = 2$ (lati l_1, l_2)
    - $d(c) = 2$ (lati l_2, l_4)
    - $d(d) = 3$ (lati l_3, l_4, l_5)
    - $d(e) = 1$ (lato l_5)
    - Se ci fosse un vertice f non collegato, $d(f) = 0$.
- **Teorema della Somma dei Gradi (Handshaking Lemma) (Pag 4-5):**
  In ogni grafo $G = (V, L)$, la somma dei gradi di tutti i vertici è uguale al doppio del numero dei lati:

$$\sum_{v \in V} d(v) = 2|L|$$

  - **Idea della Dimostrazione:** Ogni lato $\{u, v\}$ contribuisce con 1 al grado di u e con 1 al grado di v. Quindi, sommando i gradi, ogni lato viene contato due volte.
- **Corollario: Numero di Vertici di Grado Dispari (Pag 5):**
  In ogni grafo finito, il numero di vertici con grado dispari è **pari**.
  - **Idea della Dimostrazione:** Sia V_1 l'insieme dei vertici di grado dispari e V_2 quello dei vertici di grado pari.
    - $\sum_{v \in V} d(v) = \sum_{v \in V_1} d(v) + \sum_{v \in V_2} d(v) = 2|L|$.
    - $\sum_{v \in V_2} d(v)$ è una somma di numeri pari, quindi è pari.
    - Poiché $2|L|$ è pari, anche $\sum_{v \in V_1} d(v)$ deve essere pari.
    - Una somma di numeri dispari è pari se e solo se il numero di termini (dispari) è pari.
    - Quindi $|V_1|$ (il numero di vertici di grado dispari) deve essere pari.

Teoria dei Grafi Grado (teoria dei grafi) Lemma della stretta di mano

---

3. Tipi Speciali di Grafi

- **Grafo Regolare (Pag 6):** Un grafo $G = (V, L)$ è **k-regolare** (o regolare di grado k) se ogni vertice ha grado k: $\forall v \in V, d(v) = k$.
  - Esempi: Un ciclo C_n ($n \geq 3$) è 2-regolare. Un grafo completo K_n è $(n-1)$-regolare.
- **Grafo Completo K_n (Pag 6-7):**
  - Un grafo $G = (V, L)$ con $|V| = n$ vertici è **completo** se ogni coppia di vertici distinti è collegata da un lato.
  - È $(n-1)$-regolare.
  - Il numero di lati in K_n è $|L| = \binom{n}{2} = \frac{n(n-1)}{2}$.
  - K_1: un punto. K_2: un segmento. K_3: un triangolo. K_4: un quadrato con le diagonali. K_5: un pentagono con tutte le diagonali.
- **Esercizio (Pag 8):** Esiste un grafo $G = (V, L)$ con $|V| = 7$ e $|L| = 23$?
  - Il numero massimo di lati in un grafo semplice con 7 vertici è $\binom{7}{2} = \frac{7 \cdot 6}{2} = 21$.
  - Poiché $23 > 21$, **NO**, un tale grafo semplice non può esistere. (Potrebbe esistere come multigrafo).

Grafo regolare Grafo completo

---

4. Cammini e Connessione

- **Cammino (Path) (Pag 8):** Un **cammino** da un vertice v a un vertice w è una sequenza di lati $\{l_1, l_2, \ldots, l_t\}$ tale che:
  - v è un estremo di l_1.
  - w è un estremo di l_t.
  - Per ogni $i = 1, \ldots, t-1$, il lato l_i e il lato l_{i+1} condividono un vertice (sono consecutivi).
  - Più formalmente, una sequenza di vertici $(v_0, v_1, \ldots, v_t)$ tale che $v_0 = v$, $v_t = w$, e $\{v_{i-1}, v_i\} \in L$ per ogni $i = 1, \ldots, t$.

    - t è la **lunghezza** del cammino (numero di lati).
- **Grafo Connesso (Pag 9):** Un grafo $G = (V, L)$ è **connesso** se per ogni coppia di vertici distinti $u, v \in V$, esiste un cammino tra u e v.
    - Se un grafo non è connesso, si divide in più "pezzi" connessi.
- **Componente Connessa (Pag 9):** Una **componente connessa** di un grafo G è un sottografo connesso massimale. (Massimale significa che non può essere esteso aggiungendo altri vertici/lati del grafo originale mantenendo la connessione).
    - Un grafo è connesso se e solo se ha una sola componente connessa.
    - **Esempio (Pag 9):** Un grafo con vertici $\{a, b, c, d, e, f, g, h, i, l, m\}$ può avere componenti connesse come $\{a, b, c, d\}$, $\{e, f, g, h\}$, $\{i, l\}$, $\{m\}$.

Cammino (teoria dei grafi) Grafo connesso Componente connessa (teoria dei grafi)

---

5. Alberi

Una classe importante di grafi connessi.

- **Definizione (Pag 10):** Un grafo connesso $G = (V, L)$ è un **albero** se è **privo di circuiti** (o cicli).
    - Un **circuito** (o ciclo) è un cammino che inizia e finisce nello stesso vertice, senza ripetere lati (e, in un grafo semplice, senza ripetere vertici intermedi).
- Una **foresta** è un grafo privo di circuiti (le sue componenti connesse sono alberi).
- **Teorema (Caratterizzazioni degli Alberi, Pag 16):** Sia $G = (V, L)$ un grafo con $|V| = n$ vertici. Le seguenti affermazioni sono equivalenti:
    1. G è un albero (connesso e aciclico).
    2. Per ogni coppia di vertici distinti $a, b \in V$, esiste un **unico** cammino tra a e b.
    3. G è connesso, e se si rimuove un qualsiasi lato $l \in L$, il grafo $G' = (V, L \setminus \{l\})$ non è più connesso. (Minimamente connesso).
    4. G è privo di circuiti, e se si aggiunge un qualsiasi lato $\{u, v\} \notin L$ (tra vertici u, v esistenti), il grafo $G' = (V, L \cup \{\{u, v\}\})$ contiene un circuito. (Massimamente aciclico).
- **Teorema (Proprietà degli Alberi, Pag 17):** Sia $G = (V, L)$ un grafo con $|V| = n$ vertici. Le seguenti affermazioni sono equivalenti:
    1. G è un albero.
    2. G è privo di circuiti e ha $|L| = n - 1$ lati.
    3. G è connesso e ha $|L| = n - 1$ lati.

Albero (teoria dei grafi) Circuito (teoria dei grafi)

---

6. Cammini e Circuiti Euleriani

Ricollegandoci al problema dei Ponti di Königsberg.

- **Multigrafo (Pag 13):** Un grafo in cui sono ammessi **lati multipli** tra la stessa coppia di vertici e/o **cappi** (lati che collegano un vertice a se stesso).
    - Per i multigrafi, la definizione di lato come insieme di 2 vertici non basta. Si introduce una funzione $\varphi : L \to P_{\leq 2}(V)$ che associa a ogni lato l'insieme dei suoi estremi.
    - Il grado di un vertice è il numero di "estremità" di lati che incidono su di esso (un cappio conta 2 per il grado del suo vertice).
- **Cammino Euleriano:** Un cammino in un (multi)grafo che attraversa **ogni lato esattamente una volta**.
- **Circuito Euleriano:** Un cammino euleriano che è anche un circuito (inizia e finisce nello stesso vertice).
- **Teorema di Eulero (Pag 14):** Un multigrafo finito G (privo di vertici isolati) possiede un **circuito euleriano** se e solo se:
    1. G è **connesso**.
    2. Tutti i suoi vertici hanno **grado pari**.
- **Corollario:** Un multigrafo finito G (privo di vertici isolati) possiede un **cammino euleriano** (ma non un circuito) se e solo se:
    1. G è **connesso**.
    2. Ha **esattamente due** vertici di grado dispari (questi saranno l'inizio e la fine del cammino).
- **Ponti di Königsberg (Pag 1):**
    - Vertice A: grado 5 (dispari)
    - Vertice B: grado 3 (dispari)
    - Vertice C: grado 3 (dispari)

- Vertice D: grado 3 (dispari)
- Ci sono 4 vertici di grado dispari. Quindi non esiste né un circuito euleriano né un cammino euleriano.

Cammino euleriano Teorema di Eulero (teoria dei grafi)

---

7. Altri Concetti

- **Teorema (Pag 11):** Sia $G = (V, L)$ un grafo finito con grado minimo dei vertici $d_{min} > 0$. Allora:
  1. G possiede un cammino di lunghezza almeno d_{min}.
  2. Se $d_{min} \geq 2$, allora G possiede un circuito di lunghezza almeno $d_{min} + 1$.
- **Grafo Complementare (Pag 12):** Dato un grafo semplice $G = (V, L)$, il suo grafo complementare $\bar{G} = (V, \bar{L})$ ha lo stesso insieme di vertici V, e un lato $\{u, v\}$ è in $\bar{L}$ se e solo se $\{u, v\}$ non è in L.
  - $L \cap \bar{L} = \emptyset$.
  - $L \cup \bar{L} = P_2(V)$ (l'insieme di tutti i possibili lati, cioè $K_{|V|}$).

Grafo complementare

Riepilogo Veloce Lezione Bonus (Grafi)

- Il problema dei **Ponti di Königsberg** ha dato origine alla teoria dei grafi.
- Abbiamo definito un **grafo semplice non orientato** (V, L) e concetti come **grado**, **somma dei gradi** (pari al doppio dei lati), e il fatto che i **vertici di grado dispari sono in numero pari**.
- Abbiamo visto **grafi regolari** e **grafi completi** K_n.
- Abbiamo definito **cammini**, **connessione** e **componenti connesse**.
- Gli **alberi** sono grafi connessi aciclici, con $|L| = |V| - 1$.
- Un (multi)grafo ha un **circuito euleriano** $\iff$ è connesso e tutti i vertici hanno grado pari.
- Abbiamo accennato al **grafo complementare**.

Prossimi Passi

- La teoria dei grafi è vasta! Si potrebbero esplorare grafi orientati, pesati, algoritmi su grafi (ricerca cammini minimi, alberi ricoprenti, flusso massimo), colorazione, isomorfismo tra grafi.
- Rifletti su come le proprietà delle relazioni binarie (riflessiva, simmetrica, transitiva) si collegano alla struttura dei grafi.

Lezione 19: Relazioni d'Ordine, Insiemi Ordinati, Elementi Notevoli (con Diagrammi Mermaid)

Data: 23/05/2025 (come da note)
Argomenti: Relazioni d'Ordine (larghe e strette), Ordine Totale e Parziale, Diagrammi di Hasse, Elementi Minimali/Massimali, Minimo/Massimo, Minoranti/Maggioranti, Inf/Sup, Insiemi Ben Ordinati, Ordine Indotto da Funzione, Esercizi.

#tag/relations #tag/order-theory #tag/posets #tag/hasse-diagrams #tag/min-max #tag/inf-sup #tag/well-ordering #tag/algebra-avanzata #tag/mermaid

---

1. Relazioni d'Ordine

Una relazione d'ordine definisce una struttura gerarchica tra gli elementi di un insieme.

1.1 Relazione d'Ordine (Larga) (Pag 1, 7)

- Una relazione binaria $\mathcal{R}$ su un insieme S si dice **relazione d'ordine** (o d'ordine largo, parziale) se è:
  1. **Riflessiva:** $\forall x \in S, x\mathcal{R}x$.
  2. **Antisimmetrica:** $\forall x, y \in S, (x\mathcal{R}y \land y\mathcal{R}x) \implies x = y$.
  3. **Transitiva:** $\forall x, y, z \in S, (x\mathcal{R}y \land y\mathcal{R}z) \implies x\mathcal{R}z$.
- Un insieme S dotato di una relazione d'ordine $\mathcal{R}$, denotato $(S, \mathcal{R})$ (o spesso $(S, \leq)$), si chiama **insieme parzialmente ordinato** (poset).

1.2 Relazione d'Ordine Stretto (Pag 1, 7)

- Una relazione binaria $\mathcal{R}'$ su un insieme S si dice **relazione d'ordine stretto** se è:
  1. **Antiriflessiva (o Irriflessiva):** $\forall x \in S, \neg(x\mathcal{R}'x)$.

2. **Transitiva:** $\forall x, y, z \in S, (x\mathcal{R}'y \land y\mathcal{R}'z) \implies x\mathcal{R}'z$.

- *Nota:* L'antiriflessività e la transitività insieme implicano l'**asimmetria** $(x\mathcal{R}'y \implies \neg(y\mathcal{R}'x))$.

1.3 Corrispondenza tra Ordine Largo e Stretto (Pag 2, 7)

Esiste una corrispondenza biunivoca tra relazioni d'ordine largo $(\mathcal{R})$ e relazioni d'ordine stretto $(\mathcal{R}')$ sullo stesso insieme S.

- **Da Ordine Largo $\mathcal{R}$ a Ordine Stretto $\mathcal{R}'$:**

$$x\mathcal{R}'y \iff (x\mathcal{R}y \land x \neq y)$$

- **Da Ordine Stretto $\mathcal{R}'$ a Ordine Largo $\mathcal{R}$:**

$$x\mathcal{R}y \iff (x\mathcal{R}'y \lor x = y)$$

1.4 Ordine Totale vs Parziale (Pag 2)

- Un insieme ordinato $(S, \mathcal{R})$ si dice **totalmente ordinato** (o linearmente ordinato, o una catena) se per ogni coppia di elementi $x, y \in S$ si ha:

$$(x\mathcal{R}y) \lor (y\mathcal{R}x)$$

- Se un ordine non è totale, è detto **parziale**.
- **Esempi:** $(\mathbb{N}, \leq)$ è totale. $(P(S), \subseteq)$ con $|S| \geq 2$ è parziale.

1.5 Relazione di Divisibilità (Pag 9-10)

- $(\mathbb{N}^*, |)$ (divisibilità su interi positivi) è una relazione d'ordine parziale.
- $(\mathbb{Z}, |)$ **NON** è una relazione d'ordine (non è antisimmetrica: $2 \mid -2$ e $-2 \mid 2$ ma $2 \neq -2$).

Relazione d'ordine Insieme parzialmente ordinato Ordine totale

---

2. Rappresentazione e Elementi Notevoli in Insiemi Ordinati

2.1 Relazione di Copertura (Pag 3)

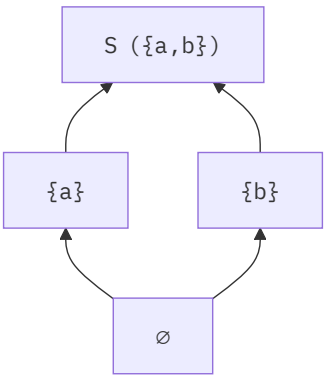
Sia $(S, \mathcal{R})$ un insieme ordinato e $\mathcal{R}'$ la relazione d'ordine stretto associata.

- b **copre** $a \iff (a\mathcal{R}'b) \land (\neg\exists c \in S : a\mathcal{R}'c \land c\mathcal{R}'b)$.
  - b è "immediatamente sopra" a nell'ordine.

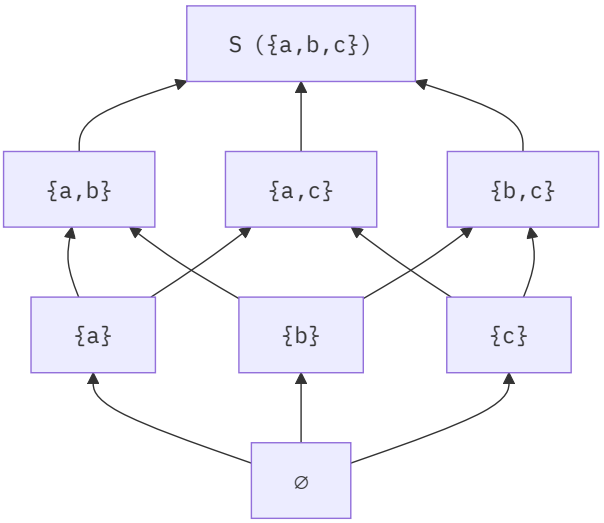
2.2 Diagrammi di Hasse (Pag 4-6)

Per insiemi ordinati **finiti**. Si disegnano nodi per gli elementi e segmenti per le relazioni di copertura, con l'elemento "superiore" più in alto.

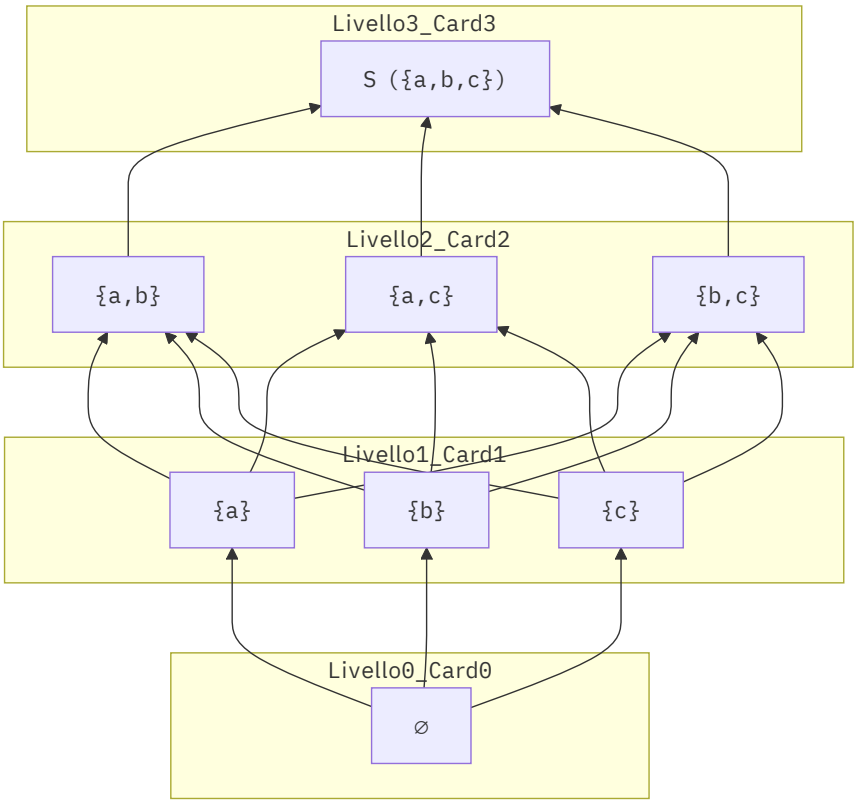
- **Esempio $(P(S), \subseteq)$ con $S = \{a, b\}$ (Pag 4):**
  - $P(S) = \{\emptyset, \{a\}, \{b\}, S = \{a, b\}\}$.



- **Esempio $(P(S), \subseteq)$ con $S = \{a, b, c\}$ (Pag 4):**
  - $P(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, S = \{a, b, c\}\}$.

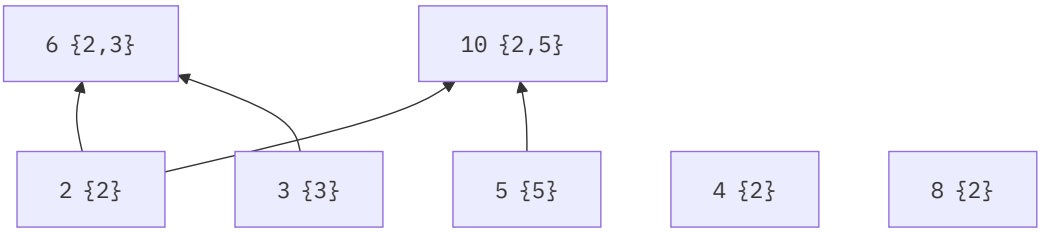


- **Esempio $(P(S), \mathcal{R})$ con $S = \{a, b, c\}$ e $X\mathcal{R}Y \iff (X = Y) \vee (|X| < |Y|)$ (Pag 5):**
  - Y copre $X \iff |Y| = |X| + 1$.
  - Nodi raggruppati per cardinalità. Ogni nodo di cardinalità k è collegato (coperto da) ogni nodo di cardinalità $k+1$.



> **Questo diagramma di Hasse illustra che ogni elemento di cardinalità k è "minore" (secondo $\mathcal{R}$) di ogni elemento di cardinalità $k+1, k+2, \ldots$. La relazione di copertura si ha tra livelli di cardinalità adiacenti.**

- **Esempio $(\{2, 3, 4, 5, 6, 8, 10\}, \mathcal{R})$ con $a\mathcal{R}b \iff (a = b) \vee (\pi(a) \subset \pi(b))$, dove $\pi(n)$ è l'insieme dei divisori primi di n (Pag 6):**
  - $\pi(2) = \{2\}$, $\pi(3) = \{3\}$, $\pi(4) = \{2\}$, $\pi(5) = \{5\}$, $\pi(6) = \{2, 3\}$, $\pi(8) = \{2\}$, $\pi(10) = \{2, 5\}$.
  - Relazione di copertura $\mathcal{R}'$: $x\mathcal{R}'y \iff \pi(x) \subset \pi(y)$ e non esiste z con $\pi(x) \subset \pi(z) \subset \pi(y)$.
  - Coperture:
    - $\pi(2) \subset \pi(6)$ e $\pi(3) \subset \pi(6)$ sono coperture.
    - $\pi(2) \subset \pi(10)$ e $\pi(5) \subset \pi(10)$ sono coperture.
    - $\pi(4)$, $\pi(8)$ hanno lo stesso insieme di fattori primi di $\pi(2)$, quindi non ci sono relazioni di copertura del tipo $\pi(x) \subset \pi(y)$ che li coinvolgano come elemento "minore" in una copertura, né come elemento "maggiore" se non per uguaglianza (che non si disegna in Hasse).



In questo diagramma, i nodi 4 e 8 sono isolati perché $\pi(4) = \pi(2)$ e $\pi(8) = \pi(2)$. La relazione $a\mathcal{R}b$ si verifica se $a = b$ (riflessività, non mostrata in Hasse) oppure se $\pi(a)$ è un *sottoinsieme proprio* di $\pi(b)$. Quindi $2\mathcal{R}4$ non vale in senso stretto, né $2\mathcal{R}8$.

Diagramma di Hasse

2.3 Elemento Minimo e Massimo (Pag 11)

Sia $(S, \leq)$ un insieme ordinato.

- $a \in S$ è **minimo** se $a \leq x, \forall x \in S$. È unico se esiste.
- $a \in S$ è **massimo** se $x \leq a, \forall x \in S$. È unico se esiste.

2.4 Elementi Minimali e Massimali (Pag 14, 16)

Sia $(S, \leq)$ un insieme ordinato.

- $a \in S$ è **minimale** se $\neg\exists x \in S : x < a$ (cioè $x \leq a \wedge x \neq a$).
- $a \in S$ è **massimale** se $\neg\exists x \in S : a < x$.
- Minimo $\implies$ unico minimale. Massimo $\implies$ unico massimale. Il viceversa non sempre.
- Insiemi finiti non vuoti hanno sempre elementi minimali/massimali.

Elemento minimale e massimale Elemento minimo e massimo

2.5 Insieme Ben Ordinato (Pag 26)

- Un insieme totalmente ordinato $(S, \leq)$ è **ben ordinato** se ogni suo sottoinsieme non vuoto $X \subseteq S$ ammette un elemento minimo.
- Esempio: $(\mathbb{N}, \leq)$. Controesempio: $(\mathbb{Z}, \leq)$.

Insieme ben ordinato

2.6 Minoranti, Maggioranti, Infimo, Supremo (Pag 27-28)

Sia $(S, \leq)$ un insieme ordinato e $X \subseteq S$.

- **Minorante** di X: $a \in S$ tale che $a \leq x, \forall x \in X$.
- **Maggiorante** di X: $a \in S$ tale che $x \leq a, \forall x \in X$.
- **Infimo** di X: $\inf(X) = \max(\text{insieme dei minoranti di } X)$, se esiste.
- **Supremo** di X: $\sup(X) = \min(\text{insieme dei maggioranti di } X)$, se esiste.
- Se $\min(X)$ esiste, $\inf(X) = \min(X)$. Se $\max(X)$ esiste, $\sup(X) = \max(X)$.
- Esempio $(\mathbb{N}^*, |)$: Per $X = \{60, 54\}$, $\inf(X) = \text{MCD}(60, 54) = 6$, $\sup(X) = \text{mcm}(60, 54) = 540$.

Minorante e maggiorante Estremo inferiore e superiore

---

3. Ordine Indotto da una Funzione (Pag 20-25)

Sia $f : S \to T$ una funzione, e $(T, \leq_T)$ un insieme ordinato. Definiamo $\leq_f$ su S:

$$\forall a, b \in S, \quad a \leq_f b \iff (a = b) \vee (f(a) <_T f(b))$$

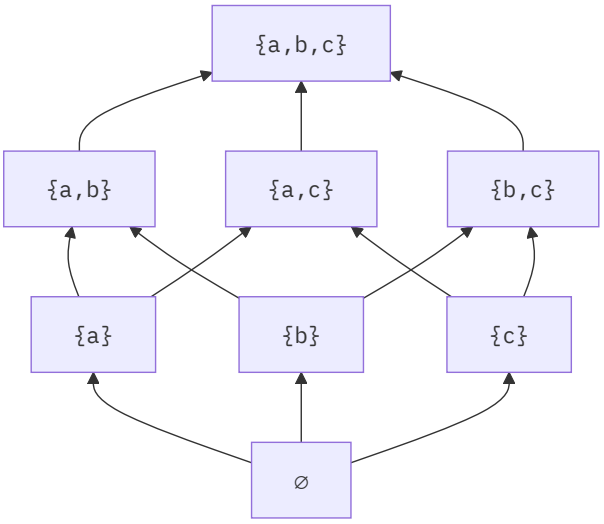
dove $<_T$ è l'ordine stretto associato a $\leq_T$. Questa $\leq_f$ è una relazione d'ordine su S.

Esercizio (Pag 29 - DA FARE)

Sia $(P(S), \mathcal{R})$ con $S = \{a, b, c\}$ e $X\mathcal{R}Y \iff (X = Y) \vee (|X| < |Y|)$.

- Disegnare il diagramma di Hasse.

- Trovare gli elementi minimali e massimali.
- Trovare minimo e massimo, se esistono.
- Considerare il sottoinsieme $H = \{\{a, b\}, \{a, c\}\}$. Trovare minoranti, maggioranti, inf e sup di H in $(P(S), \mathcal{R})$.



(Nota: Il diagramma Mermaid qui sopra è una traccia per l'esercizio. Verifica se rappresenta correttamente la relazione di copertura per l'ordine dato! Il diagramma corretto è quello discusso in precedenza per questa relazione).

Riepilogo Veloce Lezione 19

- Definite **relazioni d'ordine largo** e **stretto** e la loro corrispondenza.
- Distinzione tra ordine **totale** e **parziale**.
- I **Diagrammi di Hasse** visualizzano ordini finiti.
- Definiti **minimo/massimo** e **minimali/massimali**.
- Definito **insieme ben ordinato**.
- Definiti **minoranti, maggioranti, infimo e supremo**.
- Introdotto l'**ordine indotto da una funzione**.

Lezione 20: Insiemi Ordinati (Recap) e Reticoli

Data: 27/05/2025 (come da note)
Argomenti: Insiemi Ordinati (recap, esempi), Catene, Minoranti/Maggioranti, Inf/Sup (recap), Reticoli (definizione tramite ordine e algebrica), Proprietà delle operazioni reticolari (associatività, commutatività, assorbimento, idempotenza), Equivalenza tra le due definizioni di reticolo.

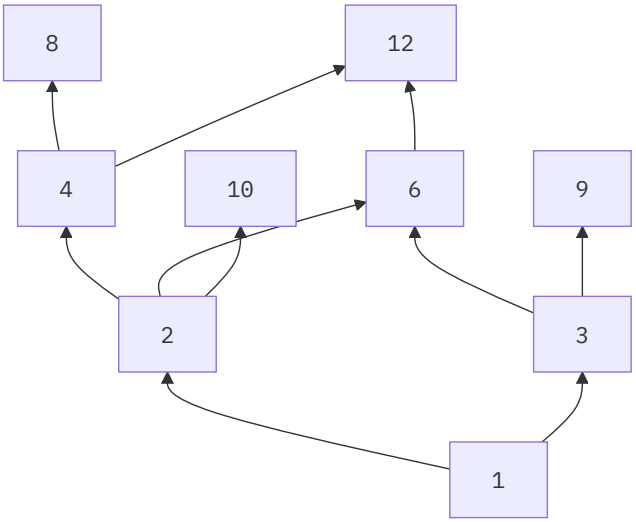
#tag/order-theory #tag/posets #tag/lattices #tag/inf-sup #tag/hasse-diagrams #tag/algebraic-structures #tag/algebra-avanzata #tag/mermaid

---

1. Insiemi Ordinati: Recap e Esempi

- **Ordine Naturale su $\mathbb{Z}$ (Pag 1-2):**
  - $(L, \leq)$ o $(\mathbb{Z}, \leq)$.
  - $a \leq b \iff b - a \in \mathbb{N}$ (dove $\mathbb{N} = \{0, 1, 2, \dots\}$).
  1. **Riflessiva:** $a \leq a \iff a - a = 0 \in \mathbb{N}$. Vero.
  2. **Antisimmetrica:** $(a \leq b \land b \leq a) \implies a = b$.
     - $b - a \in \mathbb{N}$ e $a - b \in \mathbb{N}$.
     - Sia $k_1 = b - a \geq 0$ e $k_2 = a - b \geq 0$.
     - $k_2 = -(b - a) = -k_1$.
     - L'unico numero in $\mathbb{N}$ il cui opposto è anch'esso in $\mathbb{N}$ è 0.
     - Quindi $k_1 = 0 \implies b - a = 0 \implies a = b$. Vero.
  3. **Transitiva:** $(a \leq b \land b \leq c) \implies a \leq c$.
     - $b - a \in \mathbb{N}$ e $c - b \in \mathbb{N}$.
     - $(b - a) + (c - b) = c - a$. Poiché $\mathbb{N}$ è chiuso rispetto a $+$, $c - a \in \mathbb{N}$.
     - Quindi $a \leq c$. Vero.

    - $(\mathbb{Z}, \leq)$ è **totalmente ordinato**.
- **Divisibilità su $\mathbb{N}^* = \{1, 2, 3, \dots\}$ (Pag 2):**
    - $(\mathbb{N}^*, |)$ è parzialmente ordinato (dimostrato in Lez. 19).
    - **Non è totalmente ordinato** (es. $2 \nmid 3$ e $3 \nmid 2$).
    - $\min(\mathbb{N}^*, |) = 1$.
    - $\max(\mathbb{N}^*, |)$ non esiste.
- **Esempio $(L, |)$ con $L = \{1, 2, 3, 4, 6, 8, 9, 10, 12\}$ (Pag 3-4):**
    - Questo è un insieme parzialmente ordinato dalla relazione di divisibilità.
    - **Diagramma di Hasse:**



    - $\min(L, |) = 1$.
    - Elementi Massimali: $\{8, 9, 10, 12\}$. Non c'è un massimo.
    - **Catena:** Un sottoinsieme totalmente ordinato. Es. $\{1, 2, 4, 8\}$, $\{1, 3, 9\}$, $\{1, 2, 6, 12\}$.
    - **Catena Massimale:** Una catena che non può essere estesa aggiungendo altri elementi di L.
    - **Minoranti/Maggioranti (Pag 4):**
        - $Min(\{10\}) = \{1, 2, 10\}$. $\inf(\{10\}) = 10$.
        - $Magg(\{10\}) = \{10\}$. $\sup(\{10\}) = 10$.
        - $Min(\{10, 2\}) = \{1, 2\}$. $\inf(\{10, 2\}) = 2$.
        - $Magg(\{10, 2\}) = \{10\}$. $\sup(\{10, 2\}) = 10$.
        - $Min(\{10, 6\}) = \{1, 2\}$. $\inf(\{10, 6\}) = 2$.
        - $Magg(\{10, 6\}) = \emptyset$. $\sup(\{10, 6\})$ non esiste.
        - $Min(\{8, 12, 6\}) = \{1, 2\}$. $\inf = 2$.
        - $Magg(\{8, 12, 6\}) = \emptyset$. $\sup$ non esiste.
        - $Min(\{2, 3\}) = \{1\}$. $\inf = 1$.
        - $Magg(\{2, 3\}) = \{6, 12\}$. $\sup = 6$.
- **Unicità Minimo/Massimo (Pag 5):** Se esistono, sono unici.
- **Minimo/Massimo $\implies$ Unico Minimale/Massimale (Pag 5):** Vero.

Insieme parzialmente ordinato Diagramma di Hasse Catena (teoria degli ordini) Minorante e maggiorante Estremo inferiore e superiore

---

2. Reticoli (Lattices)

Insiemi parzialmente ordinati con proprietà aggiuntive su inf e sup.

2.1 Definizione di Reticolo tramite Ordine: L'Idea di "Completezza" Locale

Immagina di avere un insieme L dove alcuni elementi sono "più piccoli" o "più grandi" di altri, secondo una relazione d'ordine parziale $\leq$. Un insieme parzialmente ordinato $(L, \leq)$ diventa un **reticolo** se soddisfa una condizione fondamentale:

- Per **ogni singola coppia** di elementi che scegli dall'insieme L, diciamo $\{a, b\}$, devono esistere sempre due cose:
    1. Il loro **estremo inferiore** (inf): Questo è l'elemento più grande in L che è "sotto" (minore o uguale a) sia a che b.
    2. Il loro **estremo superiore** (sup): Questo è l'elemento più piccolo in L che è "sopra" (maggiore o uguale a) sia a che b.

E la cosa cruciale è che questi estremi (inf e sup) devono esistere e appartenere **sempre** all'insieme L stesso.

Notazione:

Per rendere le cose più snelle, usiamo dei simboli speciali per l'estremo inferiore e superiore di una coppia:

- L'estremo inferiore di a e b, $\inf\{a,b\}$, si denota $a \wedge b$. Puoi leggerlo "a meet b" o "a inf b". Pensa a $\wedge$ come a trovare il "punto di incontro più alto" sotto entrambi gli elementi.
- L'estremo superiore di a e b, $\sup\{a,b\}$, si denota $a \vee b$. Puoi leggerlo "a join b" o "a sup b". Pensa a $\vee$ come a trovare il "punto di unione più basso" sopra entrambi gli elementi.

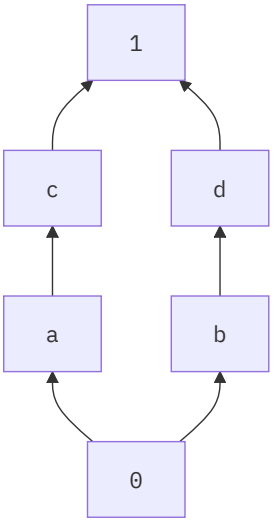
Quindi, la definizione formale si riassume così:

- Un insieme parzialmente ordinato $(L, \leq)$ è un **reticolo** se per ogni $a, b \in L$, esistono $\inf\{a,b\}$ (o $a \wedge b$) e $\sup\{a,b\}$ (o $a \vee b$) in L.

Esempio con un Diagramma Specifico:

Prendiamo il diagramma di Hasse che abbiamo appena analizzato, con gli elementi $L = \{0, a, b, c, d, 1\}$ e le connessioni dirette (frecce) che hai specificato: $0 \to a, 0 \to b, a \to c, b \to d, c \to 1, d \to 1$.

Ecco il diagramma disegnato correttamente con 0 in basso e 1 in alto:



Vediamo perché questo diagramma **è un reticolo** controllando alcune coppie:

- **Coppia $\{a,b\}$:**
  - Minoranti di $\{a,b\}$ (elementi $\leq a$ e $\leq b$): Solo 0. Il massimo dei minoranti è 0. Quindi $\inf\{a,b\} = 0$. (Esiste in L).
  - Maggioranti di $\{a,b\}$ (elementi $\geq a$ e $\geq b$): $a \leq c \leq 1$ e $b \leq d \leq 1$. L'unico elemento $\geq$ sia di a che di b è 1. Il minimo dei maggioranti è 1. Quindi $\sup\{a,b\} = 1$. (Esiste in L).
- **Coppia $\{c,d\}$:**
  - Minoranti di $\{c,d\}$ (elementi $\leq c$ e $\leq d$): $c \geq a \geq 0$ e $d \geq b \geq 0$. L'unico elemento $\leq$ sia di c che di d è 0. Il massimo dei minoranti è 0. Quindi $\inf\{c,d\} = 0$. (Esiste in L).
  - Maggioranti di $\{c,d\}$ (elementi $\geq c$ e $\geq d$): Solo 1. Il minimo dei maggioranti è 1. Quindi $\sup\{c,d\} = 1$. (Esiste in L).

Controllando tutte le altre coppie (es. $\{0,a\}$, $\{b,d\}$, $\{a,c\}$, $\{c,1\}$, ecc.), troveremmo sempre che l'estremo inferiore e l'estremo superiore esistono e sono elementi dell'insieme L.

Poiché per *ogni* coppia di elementi in questo diagramma l'estremo inferiore e l'estremo superiore esistono all'interno dell'insieme stesso, questo diagramma **rappresenta un reticolo**.

Questo esempio specifico *è* un reticolo. A volte, diagrammi che sembrano simili (come quello "a forma di casa" che hai menzionato, o un "diamante" leggermente diverso) *non* lo sono, perché per *almeno una* coppia di elementi, l'inf o il sup non esiste nell'insieme. La chiave è che la proprietà deve valere per **tutte** le coppie!

2.2 Definizione Algebrica di Reticolo (Pag 13-14)

- Una struttura algebrica $(L, \wedge, \vee)$, dove $\wedge$ e $\vee$ sono operazioni binarie su L, è un **reticolo** se valgono le seguenti proprietà per ogni $a, b, c \in L$:
  1. **Associatività:**

- $a \wedge (b \wedge c) = (a \wedge b) \wedge c$
- $a \vee (b \vee c) = (a \vee b) \vee c$

2. **Commutatività:**
   - $a \wedge b = b \wedge a$
   - $a \vee b = b \vee a$
3. **Leggi di Assorbimento:**
   - $a \wedge (a \vee b) = a$
   - $a \vee (a \wedge b) = a$

- **Proprietà Derivata: Idempotenza (Pag 15):** Dalle leggi di assorbimento si può derivare l'idempotenza:
  - $a \wedge a = a$
    - Dim: $a \wedge a = a \wedge (a \vee (a \wedge b))$ (per assorbimento $a = a \vee (a \wedge b)$)
    - $= a$ (per assorbimento $x \wedge (x \vee y) = x$, con $x = a, y = (a \wedge b)$).
  - $a \vee a = a$ (analogo).

2.3 Equivalenza tra le Due Definizioni (Pag 15-17)

Le due definizioni di reticolo (quella basata sull'ordine e quella algebrica) sono equivalenti.

- $(L, \leq)$ **reticolo** $\implies$ $(L, \inf, \sup)$ **è reticolo algebrico:**
  - Se $(L, \leq)$ è un reticolo (ordine), allora $a \wedge b = \inf\{a, b\}$ e $a \vee b = \sup\{a, b\}$ soddisfano le proprietà algebriche (associatività, commutatività, assorbimento). La dimostrazione richiede di usare le proprietà di inf e sup.
- $(L, \wedge, \vee)$ **reticolo algebrico** $\implies$ $(L, \leq)$ **è reticolo (ordine):**
  - Data una struttura algebrica $(L, \wedge, \vee)$ che soddisfa le proprietà algebriche, possiamo definire una relazione d'ordine $\leq$ su L come segue:

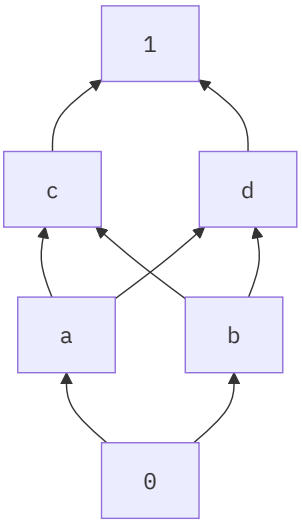
    $$a \leq b \iff a \wedge b = a$$

    (Equivalentemente, $a \leq b \iff a \vee b = b$).
  - Bisogna dimostrare che questa $\leq$ è una relazione d'ordine:
    1. **Riflessiva:** $a \leq a \iff a \wedge a = a$. Vero per idempotenza.
    2. **Antisimmetrica:** $a \leq b \wedge b \leq a \implies a \wedge b = a$ e $b \wedge a = b$. Per commutatività, $a \wedge b = b \wedge a$, quindi $a = b$. Vero.
    3. **Transitiva:** $a \leq b \wedge b \leq c \implies a \wedge b = a$ e $b \wedge c = b$.
       - Dobbiamo mostrare $a \leq c$, cioè $a \wedge c = a$.
       - $a \wedge c = (a \wedge b) \wedge c$ (sostituendo $a = a \wedge b$)
       - $= a \wedge (b \wedge c)$ (associatività di $\wedge$)
       - $= a \wedge b$ (sostituendo $b = b \wedge c$)
       - $= a$. Vero.
  - Infine, bisogna dimostrare che rispetto a questo ordine $\leq$, si ha $\inf\{a, b\} = a \wedge b$ e $\sup\{a, b\} = a \vee b$.
    - Per $\inf\{a, b\} = a \wedge b$:
      - $(a \wedge b) \leq a$? Sì, perché $(a \wedge b) \wedge a = a \wedge b$.
      - $(a \wedge b) \leq b$? Sì, perché $(a \wedge b) \wedge b = a \wedge b$.
      - Se $c \leq a$ e $c \leq b$, allora $c \wedge a = c$ e $c \wedge b = c$. Dobbiamo mostrare $c \leq (a \wedge b)$, cioè $c \wedge (a \wedge b) = c$.
      - $c \wedge (a \wedge b) = (c \wedge a) \wedge b = c \wedge b = c$. Vero.

Reticolo (matematica) Leggi di assorbimento Idempotenza

2.4 Esempio: Un Poset che NON è un Reticolo

Il diagramma di Hasse analizzato nel capitolo 2.4 è il seguente:



Verifica se è un reticolo

Un insieme parzialmente ordinato è un reticolo se per ogni coppia di elementi esistono $\inf$ e $\sup$ *all'interno dell'insieme*.

Prendiamo la coppia $\{a, b\}$:

1. **Minoranti di $\{a, b\}$:**
   - Elementi $\leq a$ e $\leq b$: Solo 0.
   - $\inf\{a, b\} = 0$.
2. **Maggioranti di $\{a, b\}$:**
   - Elementi $\geq a$ e $\geq b$: $c, d, 1$.
     - $c \geq a$ e $c \geq b$ (per transitività, poiché $a \leq c$ e $b \leq c$).
     - $d \geq a$ e $d \geq b$ (per transitività, poiché $a \leq d$ e $b \leq d$).
     - $1 \geq a$ e $1 \geq b$ (per transitività, poiché $a \leq c \leq 1$ e $b \leq c \leq 1$, e $a \leq d \leq 1$ e $b \leq d \leq 1$).
   - I maggioranti sono $\{c, d, 1\}$.
   - Il minimo dei maggioranti dovrebbe essere l'elemento più piccolo tra $c, d, 1$.
     - Ma c e d sono incomparabili (nessuno dei due è $\leq$ l'altro).
     - Quindi, non esiste un minimo dei maggioranti.
   - **Conclusione:** $\sup\{a, b\}$ **non esiste**.

Poiché esiste almeno una coppia (in questo caso $\{a, b\}$) per cui il $\sup$ non esiste, il poset **non è un reticolo**.

Errore nell'analisi iniziale

Nell'analisi iniziale, è stato erroneamente affermato che il $\sup\{a, b\}$ è c o d, ma in realtà non esiste un $\sup$ perché c e d sono incomparabili. La corretta analisi mostra che $\sup\{a, b\}$ non esiste, confermando che il poset non è un reticolo.

Riepilogo

Il diagramma di Hasse analizzato **non è un reticolo** perché la coppia $\{a, b\}$ non ha un estremo superiore (sup) nell'insieme. Questo è dovuto al fatto che i maggioranti di $\{a, b\}$ sono $\{c, d, 1\}$, ma c e d sono incomparabili, quindi non esiste un minimo tra di essi.

---

4. Esempi e Controesempi di Reticoli (Pag 20)

- **$(P(S), \subseteq)$ è un reticolo.**
  - $\inf\{A, B\} = A \cap B$.
  - $\sup\{A, B\} = A \cup B$.
  - Le operazioni $\cap$ e $\cup$ soddisfano le proprietà algebriche dei reticoli.
- **$(P(S), \mathcal{R})$ con $X\mathcal{R}Y \iff (X = Y) \vee (|X| < |Y|)$ (Pag 20, cerchiato in rosso):**
  - Questo è l'esempio dal diagramma di Hasse che raggruppa per cardinalità.
  - **NON è un reticolo** se $|S| \geq 2$.
  - Consideriamo $S = \{a, b, c\}$. $X = \{a, b\}$, $Y = \{a, c\}$. Entrambi hanno cardinalità 2.
  - $Min(X, Y)$ rispetto a $\mathcal{R}$:
    - Un minorante M deve essere $M = X$ o $|M| < |X| = 2$, e $M = Y$ o $|M| < |Y| = 2$.
    - Se $M = X$, $X\mathcal{R}Y$ non vale ($X \neq Y$ e $|X| \not< |Y|$).

- I minoranti sono tutti gli insiemi M con $|M| \leq 1$ (cioè $\emptyset, \{a\}, \{b\}, \{c\}$).
- $\inf\{X, Y\} = \max(Min(X, Y))$. Qual è il massimo tra $\{\emptyset, \{a\}, \{b\}, \{c\}\}$ secondo $\mathcal{R}$?
  - Tutti i singleton $\{a\}, \{b\}, \{c\}$ sono elementi massimali nell'insieme dei minoranti (hanno cardinalità 1, $\emptyset$ ha cardinalità 0). Non c'è un unico massimo.
  - Quindi $\inf\{\{a, b\}, \{a, c\}\}$ **non esiste**.
- L'affermazione "NO minoranti" nella tua nota è riferita al fatto che non c'è un *unico* $\inf$.

Riepilogo Veloce Lezione 20

- Abbiamo rivisto le proprietà degli **insiemi ordinati** e analizzato esempi, inclusi i diagrammi di Hasse.
- Un **reticolo** $(L, \leq)$ è un poset dove ogni coppia di elementi $\{a, b\}$ ammette $\inf\{a, b\}$ (denotato $a \wedge b$) e $\sup\{a, b\}$ (denotato $a \vee b$).
- Equivalentemente, un reticolo è una struttura algebrica $(L, \wedge, \vee)$ dove $\wedge, \vee$ sono binarie, associative, commutative e soddisfano le **leggi di assorbimento** (da cui deriva l'idempotenza).
- Le due definizioni sono equivalenti: una struttura d'ordine reticolare induce operazioni algebriche reticolari, e viceversa.
- $(P(S), \subseteq)$ è un reticolo con $A \wedge B = A \cap B$ e $A \vee B = A \cup B$.
- L'ordine basato sulla stretta inclusione delle cardinalità non è necessariamente un reticolo.
  z
  [!TIP] Prossimi Passi
- Assicurati di aver compreso l'equivalenza tra le due definizioni di reticolo.
- I reticoli possono avere ulteriori proprietà (distributivi, booleani, completi) che definiscono classi più specifiche di strutture.

Lezione 21: Reticoli - Strutture Ordinate e Algebriche

Data: 2025-05-30
Tags: #algebra #algebraavanzata #reticoli #strutturealgebriche #relazionidordine

Oggi esploreremo il concetto affascinante dei **reticoli**. Immaginali come delle strutture speciali che combinano l'ordine con operazioni algebriche, un po' come una scala musicale dove ogni nota ha una relazione precisa con le altre e puoi "combinarle" in modi specifici.

1. Cos'è un Reticolo? Due Facce della Stessa Medaglia!

Un reticolo può essere visto in due modi equivalenti, come due sentieri che portano alla stessa cima della montagna:

1.1. Definizione tramite Insieme Parzialmente Ordinato (Poset)

Definizione (come Poset)

Un insieme parzialmente ordinato $(L, \leq)$ è un **reticolo** se, per ogni coppia di elementi $a, b \in L$, esistono sempre:

1. L'**estremo inferiore** (infimum) di $\{a, b\}$, denotato come $a \wedge b$ (letto "a meet b" o "a inf b").
2. L'**estremo superiore** (supremum) di $\{a, b\}$, denotato come $a \vee b$ (letto "a join b" o "a sup b").

- **Infimum ($a \wedge b$)**: È il "più grande" elemento che è minore o uguale sia ad a sia a b. Pensa al Massimo Comun Divisore se L fosse l'insieme dei numeri naturali e $\leq$ fosse la relazione di divisibilità.
- **Supremum ($a \vee b$)**: È il "più piccolo" elemento che è maggiore o uguale sia ad a sia a b. Pensa al Minimo Comune Multiplo nello stesso esempio.

Visualizza $a \wedge b$ come il punto d'incontro più "basso" raggiungibile da a e b, e $a \vee b$ come il punto d'incontro più "alto". (Puoi associare $\wedge$ e $\vee$ a dei simboli nel tuo dizionario visuale!)

1.2. Definizione tramite Struttura Algebrica

Definizione (come Struttura Algebrica)

Una struttura algebrica $(L, \wedge, \vee)$, dove $\wedge$ e $\vee$ sono operazioni binarie su L, è un **reticolo** se valgono le seguenti proprietà per tutti gli $a, b, c \in L$:

1. **Leggi Associative**:

$$(a \wedge b) \wedge c = a \wedge (b \wedge c)$$

$$(a \vee b) \vee c = a \vee (b \vee c)$$

2. **Leggi Commutative**:

$$a \wedge b = b \wedge a$$

$$a \vee b = b \vee a$$

3. **Leggi di Assorbimento**:

$$a \wedge (a \vee b) = a$$

$$a \vee (a \wedge b) = a$$

Spiegazione Semplice delle Leggi di Assorbimento:
Immagina di avere un numero a. Se prendi a e un numero "più grande o uguale" ($a \vee b$), il loro "minimo comune" ($\wedge$) sarà proprio a. Viceversa, se prendi a e un numero "più piccolo o uguale" ($a \wedge b$), il loro "massimo comune" ($\vee$) sarà ancora a.
Queste leggi sono come dire: "Se combino a con qualcosa che già lo 'contiene' o è 'contenuto' in esso in un certo modo, a stesso 'assorbe' l'operazione."

1.3. Il Ponte tra le Due Definizioni

La relazione d'ordine $\leq$ e le operazioni $\wedge, \vee$ sono intimamente collegate:
Per $a, b \in L$:

$$a \leq b \iff a \wedge b = a \iff a \vee b = b$$

Suggerimento per la Memoria

- $a \wedge b = a \implies a$ è "sotto" b (o uguale), quindi $a \leq b$.
- $a \vee b = b \implies b$ è "sopra" a (o uguale), quindi $a \leq b$.

---

2. Esempi di Reticoli

Vediamo alcuni esempi per rendere il concetto più concreto.

2.1. Insiemi Totalmente Ordinati

Esempio: Insiemi Totalmente Ordinati

Se $(S, \leq)$ è un **insieme totalmente ordinato** (cioè, per ogni $a, b \in S$, o $a \leq b$ o $b \leq a$), allora S è un reticolo.

- **Perché?** Se $a \leq b$:
  - $a \wedge b = a$ (l'infimum è a)
  - $a \vee b = b$ (il supremum è b)
    Analogamente se $b \leq a$. L'infimum e il supremum esistono sempre!
- Un esempio è $(\mathbb{N}, \leq)$, i numeri naturali con l'usuale ordinamento.

2.2. L'Insieme delle Parti $\mathcal{P}(S)$

Esempio: Insieme delle Parti

Sia S un insieme. L'insieme delle sue parti, $\mathcal{P}(S)$, con la relazione di inclusione $\subseteq$, forma un reticolo.
Qui:

- $A \wedge B = A \cap B$ (l'intersezione è il più grande sottoinsieme comune)
- $A \vee B = A \cup B$ (l'unione è il più piccolo sovrainsieme comune)

Quindi, $(\mathcal{P}(S), \cap, \cup)$ è la struttura algebrica del reticolo.

Attenzione!

Non tutti i reticoli sono totalmente ordinati!
Pensa a $\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.
Qui, $\{1\}$ e $\{2\}$ non sono confrontabili (né $\{1\} \subseteq \{2\}$ né $\{2\} \subseteq \{1\}$).
Eppure, è un reticolo:

- $\{1\} \wedge \{2\} = \{1\} \cap \{2\} = \emptyset$
- $\{1\} \vee \{2\} = \{1\} \cup \{2\} = \{1,2\}$

---

3. Reticoli Limitati: Avere un Inizio e una Fine

Alcuni reticoli hanno degli elementi "speciali" che fungono da minimo e massimo assoluto.

Definizione: Reticolo Limitato

Un reticolo L si dice **limitato** se possiede:

- Un **elemento minimo assoluto**, denotato con 0 (o 0_L), tale che $0 \leq a$ per ogni $a \in L$.
- Un **elemento massimo assoluto**, denotato con 1 (o 1_L), tale che $a \leq 1$ per ogni $a \in L$.

Proprietà degli elementi 0 e 1:

- $a \vee 0 = a$ (0 è l'elemento neutro per $\vee$)
- $a \wedge 1 = a$ (1 è l'elemento neutro per $\wedge$)

Immagina 0 come il "punto di partenza" o il "pavimento" del reticolo, e 1 come il "punto di arrivo" o il "soffitto".

Esempi di Reticoli Limitati:

1. **L'insieme delle parti $(\mathcal{P}(S), \subseteq)$ è limitato**:
   - $0_{\mathcal{P}(S)} = \emptyset$ (l'insieme vuoto è incluso in tutti gli altri)
   - $1_{\mathcal{P}(S)} = S$ (l'insieme S include tutti gli altri)
2. **I divisori di un numero naturale $(\mathbb{D}_n, |)$**:
   Sia $\mathbb{D}_n$ l'insieme dei divisori positivi di un numero $n \in \mathbb{N}^*$ (es. $\mathbb{D}_{12} = \{1, 2, 3, 4, 6, 12\}$), con la relazione di divisibilità $|$. Questo è un reticolo limitato.
   - $a \wedge b = \text{MCD}(a, b)$ (Massimo Comun Divisore)
   - $a \vee b = \text{mcm}(a, b)$ (Minimo Comune Multiplo)
   - $0_{\mathbb{D}_n} = 1$ (1 divide tutti gli altri divisori)
   - $1_{\mathbb{D}_n} = n$ (n è divisibile per tutti gli altri divisori)

Reticoli Finiti

Ogni reticolo finito è limitato!
Se hai un numero finito di elementi, puoi sempre trovare un minimo e un massimo (potrebbero non essere unici se non fosse un reticolo, ma in un reticolo l'esistenza di inf/sup per ogni coppia garantisce un minimo e massimo globale unici).

Attenzione con $(\mathbb{N}^*, |)$

L'insieme di **tutti** i numeri naturali positivi $(\mathbb{N}^*, |)$ con la divisibilità è un reticolo:

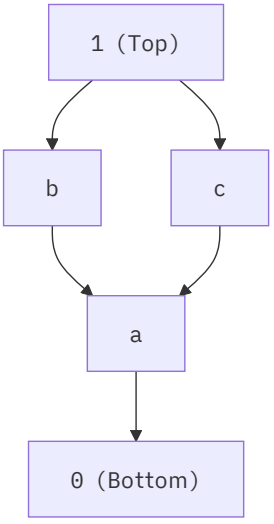
- $a \wedge b = \text{MCD}(a, b)$
- $a \vee b = \text{mcm}(a, b)$
  È **limitato inferiormente** da 1 (il $0_{\mathbb{N}^*} = 1$).
  Tuttavia, **non è limitato superiormente** (non esiste un numero naturale che sia multiplo di tutti gli altri). Quindi, $(\mathbb{N}^*, |)$ non è un reticolo limitato nel senso pieno.

---

4. Diagrammi di Hasse di Reticoli Famosi

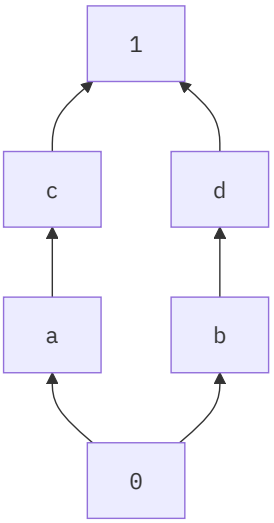
I diagrammi di Hasse sono un modo fantastico per visualizzare i reticoli finiti. Ecco due esempi classici che spesso saltano fuori:

- **Reticolo Pentagonale (N5)**: Non è modulare (e quindi non distributivo).

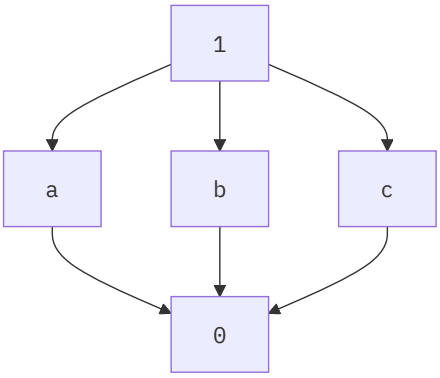


In N5, gli elementi sono $0, a, b, c, 1$ con $0 < a < b < 1$ e $0 < a < c < 1$. b e c non sono confrontabili.
(Nota: il tuo disegno a pag. 7 è leggermente diverso, con b e c direttamente sopra a. Il "pentagono" standard ha $0 < x < y < 1$ e $0 < x < z < 1$ e $0 < w < z < 1$ con y, w non confrontabili. Il tuo disegno è più simile a M3 con un elemento in più. Il diagramma N5 standard è: $0 < a$, $0 < b$, $a < c$, $b < d$, $c < 1$, $d < 1$ dove a, b non sono confrontabili, c, d non

sono confrontabili, a non è confrontabile con d, b non è confrontabile con c.
Il tuo "Reticolo pentagonale" a pag. 7 ha $0 < a < b < 1$ e $0 < a < \text{nodo\_intermedio\_dx} < c < 1$. Assumendo che il tuo disegno sia quello che intendi, lo chiameremo "Pentagono acquilone".
Per chiarezza, ecco N5 standard:



E M3 (il "diamante"):



Il tuo "Reticolo Trizettangolo golo" (M3 o diamante) è corretto.

Proviamo a Riflettere

Guardando i diagrammi M3 e N5 (quello standard), riesci a trovare coppie di elementi e calcolare il loro $\wedge$ (meet) e $\vee$ (join)?
Ad esempio, in M3, cosa sono $a \wedge b$ e $a \vee b$?

---

5. Sottoreticoli

Proprio come gli insiemi hanno sottoinsiemi e i gruppi hanno sottogruppi, i reticoli hanno i sottoreticoli!

Definizione: Sottoreticolo

Sia $(L, \wedge_L, \vee_L)$ un reticolo e sia $A \subseteq L$ un sottoinsieme non vuoto di L.
A è un **sottoreticolo** di L se A è chiuso rispetto alle operazioni $\wedge_L$ e $\vee_L$.
Cioè, per ogni $x, y \in A$:

- $x \wedge_L y \in A$
- $x \vee_L y \in A$
  In tal caso, $(A, \wedge_L|_A, \vee_L|_A)$ è esso stesso un reticolo.

Esempi e Non-Esempi:

- **Ogni singolo elemento:** Per ogni $a \in L$, l'insieme $\{a\}$ è un sottoreticolo banale, perché $a \wedge a = a$ e $a \vee a = a$ (leggi di idempotenza, che derivano dall'assorbimento).
- **Coppie di elementi:** Un insieme $\{a, b\}$ è un sottoreticolo se e solo se a e b sono **confrontabili** (cioè $a \leq b$ o $b \leq a$).
  - Se $a \leq b$, allora $a \wedge b = a \in \{a, b\}$ e $a \vee b = b \in \{a, b\}$.
  - Se a e b non sono confrontabili, $a \wedge b$ potrebbe essere un terzo elemento $c \notin \{a, b\}$, e allora $\{a, b\}$ non sarebbe un sottoreticolo. (Vedi pag. 17 dei tuoi appunti, dove $a \wedge b = c \notin A$).
- **Esempio da pag. 22:**
  Sia $(\mathbb{D}_{36}, |)$ il reticolo dei divisori di 36.

- $L = \{1, 2, 3, 6, 36\}$. È un sottoreticolo?
  - $0_L = 1, 1_L = 36$.
  - $\text{mcm}(2, 3) = 6 \in L$. $\text{MCD}(2, 3) = 1 \in L$. Sembra di sì per questa coppia. Bisognerebbe controllare tutte le coppie. (Sì, è un sottoreticolo).
- $M = \{1, 2, 3, 36\}$. È un sottoreticolo?
  - $\text{mcm}(2, 3) = 6 \notin M$. Quindi M **non** è un sottoreticolo di $(\mathbb{D}_{36}, |)$.

---

6. Isomorfismi tra Reticoli

Come per altre strutture algebriche, possiamo parlare di "uguaglianza strutturale" tra reticoli.

6.1. Isomorfismo di Insiemi Parzialmente Ordinati (Poset)

Definizione: Isomorfismo di Poset

Siano $(S, \leq_S)$ e $(T, \leq_T)$ due poset. Una funzione $f : S \to T$ è un **isomorfismo di poset** se:

1. f è **biettiva** (corrispondenza uno-a-uno e suriettiva).
2. f **preserva l'ordine**: per ogni $a, b \in S$, $a \leq_S b \iff f(a) \leq_T f(b)$.
   (Questo implica anche che f^{-1} preserva l'ordine).

6.2. Isomorfismo di Reticoli

Definizione: Isomorfismo di Reticoli

Siano $(L, \wedge_L, \vee_L)$ e $(M, \wedge_M, \vee_M)$ due reticoli. Una funzione $f : L \to M$ è un **isomorfismo di reticoli** se:

1. f è **biettiva**.
2. f **preserva le operazioni** (è un omomorfismo):
   - $f(a \wedge_L b) = f(a) \wedge_M f(b)$
   - $f(a \vee_L b) = f(a) \vee_M f(b)$

Isomorfismo di Poset vs. Isomorfismo di Reticoli

Se L e M sono reticoli, un isomorfismo di poset $f : L \to M$ è **sempre** anche un isomorfismo di reticoli, e viceversa. Cioè, se f è biettiva e $a \leq_L b \iff f(a) \leq_M f(b)$, allora automaticamente f preserverà le operazioni $\wedge$ e $\vee$.

MA ATTENZIONE: I tuoi appunti (pag. 10-11) mostrano un caso cruciale:
Considera $L_1 = (\mathbb{N}^*, |)$ (naturali positivi con divisibilità) e $L_2 = (\mathbb{N}^*, \leq)$ (naturali positivi con ordine usuale). Entrambi sono reticoli.
La funzione identità $i(x) = x$ da L_1 a L_2 è un isomorfismo di insiemi, ma **NON** di poset (e quindi non di reticoli).

- In L_1: $2 \wedge_1 3 = \text{MCD}(2, 3) = 1$. $i(2 \wedge_1 3) = i(1) = 1$.
- In L_2: $i(2) \wedge_2 i(3) = 2 \wedge_2 3 = \min(2, 3) = 2$.
  Poiché $1 \neq 2$, $i(2 \wedge_1 3) \neq i(2) \wedge_2 i(3)$.
  Quindi i non è un isomorfismo di reticoli.

La frase "Essere isomorfismo tra insiemi ordinati NON garantisce isomorfismo reticolare" (pag. 11) si riferisce al fatto che se hai due strutture che SONO reticoli, e una funzione che è un isomorfismo di poset TRA DI LORO, allora è anche un isomorfismo di reticoli. Il problema dell'esempio è che $(\mathbb{N}^*, |)$ e $(\mathbb{N}^*, \leq)$ sono strutture reticolari *diverse* sullo stesso insieme sottostante. L'identità i non è un isomorfismo di poset tra $((\mathbb{N}^*, |)$ e $(\mathbb{N}^*, \leq))$. Ad esempio, $2|6$ in L_1 ma $2 \leq 6$ in L_2. Questo è vero. Ma $3 \nmid 2$ e $3 \not\leq 2$.
Il punto chiave è: se $f : L \to M$ è un isomorfismo di poset *e L, M sono reticoli*, allora f è anche un isomorfismo di reticoli.

---

7. Reticoli Complementati

Questa è una proprietà molto importante, specialmente per le algebre di Boole!

Definizione: Reticolo Complementato

Un reticolo $(L, \wedge, \vee)$ si dice **complementato** se:

1. L è **limitato** (possiede 0 e 1).
2. Per ogni elemento $a \in L$, esiste almeno un **complemento** $\bar{a} \in L$ tale che:

$$a \wedge \bar{a} = 0 \quad \text{e} \quad a \vee \bar{a} = 1$$

Non tutti i reticoli limitati sono complementati!

Esempi:

1. **Reticolo** $(\mathcal{P}(S), \cap, \cup)$: È complementato.
   - È limitato con $0 = \emptyset$ e $1 = S$.
   - Per ogni $A \in \mathcal{P}(S)$, il suo complemento è il complemento insiemistico $A^c = S \setminus A$.
     - $A \cap A^c = \emptyset = 0$
     - $A \cup A^c = S = 1$
   - In questo caso, il complemento è **unico**. (Questo è vero per i reticoli distributivi complementati, chiamati Algebre di Boole).
2. **Catena a 3 elementi**: $L = \{0, x, 1\}$ con $0 < x < 1$.
   - È limitato (0 e 1).
   - L'elemento x ha un complemento? Cerchiamo $\bar{x}$ tale che $x \wedge \bar{x} = 0$ e $x \vee \bar{x} = 1$.
     - Se $\bar{x} = 0$: $x \wedge 0 = 0$ (OK), ma $x \vee 0 = x \neq 1$ (NO).
     - Se $\bar{x} = x$: $x \wedge x = x \neq 0$ (NO).
     - Se $\bar{x} = 1$: $x \wedge 1 = x \neq 0$ (NO).
   - Quindi x non ha complemento. Il reticolo non è complementato. (Vedi pag. 14 dei tuoi appunti, l'esempio $L = \{1, 2, 3\}$ con $\leq$ è una catena di questo tipo, dove 2 non ha complemento).
3. **Reticolo N5 (Pentagono)**: Non è complementato. L'elemento a nel diagramma standard (o l'elemento b o c nel tuo disegno a pag. 7, a seconda di come si interpretano meet/join) di solito non ha complemento.
4. **Reticolo M3 (Diamante)**: È complementato. Se gli atomi (elementi subito sopra 0) sono a, b, c:
   - a ha come complementi b e c (se $a \wedge b = 0, a \vee b = 1$, etc.).
   - In M3, ogni elemento $x \notin \{0, 1\}$ ha almeno un complemento. Ad esempio, a è complemento di b e c.
5. **Reticolo dei divisori** $(\mathbb{D}_n, |)$: In generale **non** è complementato.
   - Esempio $\mathbb{D}_{12} = \{1, 2, 3, 4, 6, 12\}$. $0 = 1, 1 = 12$.
     - Prendiamo $a = 2$. Cerchiamo $\bar{a}$ t.c. $\text{MCD}(2, \bar{a}) = 1$ e $\text{mcm}(2, \bar{a}) = 12$.
     - $\text{MCD}(2, \bar{a}) = 1 \implies \bar{a}$ deve essere dispari. In $\mathbb{D}_{12}$, gli unici dispari sono $1, 3$.
     - Se $\bar{a} = 1$: $\text{mcm}(2, 1) = 2 \neq 12$.
     - Se $\bar{a} = 3$: $\text{mcm}(2, 3) = 6 \neq 12$.
     - Nessun elemento funziona. 2 non ha complemento.

> ⚠ $(\mathbb{N}^*, |)$ **(pag. 21)**
>
> Questo reticolo non è limitato superiormente, quindi per definizione non può essere complementato. Le tue note $(10, 9) = 1, (10, 3) = 1$ mostrano che puoi trovare elementi il cui MCD è 1 (il 0_L), ma questo è solo metà del lavoro. Devi anche avere $\text{mcm}(10, \bar{a}) = 1_L$, ma 1_L non esiste!

---

8. Reticolo Prodotto (pag. 23-24)

Possiamo costruire nuovi reticoli a partire da reticoli esistenti, ad esempio con il prodotto diretto.

Siano $(L_1, \leq_1)$ e $(L_2, \leq_2)$ due reticoli. Il **reticolo prodotto** è $L = L_1 \times L_2$ con la relazione d'ordine ρ (o $\leq_L$) definita componente per componente:

$$(a, b) \rho (c, d) \iff a \leq_1 c \text{ e } b \leq_2 d$$

Le operazioni di meet e join sono anch'esse definite componente per componente:

$$(a, b) \wedge_L (c, d) = (a \wedge_1 c, b \wedge_2 d)$$

$$(a, b) \vee_L (c, d) = (a \vee_1 c, b \vee_2 d)$$

- **Esempio** $(\mathbb{N}^* \times \mathbb{N}^*, \rho)$ **dove** ρ **è basata sulla divisibilità** $|$:
  - $(a, b) \rho (c, d) \iff a | c \text{ e } b | d$.
  - $(a, b) \wedge (c, d) = (\text{MCD}(a, c), \text{MCD}(b, d))$.
  - $(a, b) \vee (c, d) = (\text{mcm}(a, c), \text{mcm}(b, d))$.
  - L'elemento minimo è $(1, 1)$. Non c'è un elemento massimo.
- **Esempio di calcolo (pag. 24)**: Trovare l'infimum (meet) di $\{(2, 5), (4, 3)\}$ in $(\mathbb{N}^* \times \mathbb{N}^*, \rho)$.
  - $(2, 5) \wedge (4, 3) = (\text{MCD}(2, 4), \text{MCD}(5, 3)) = (2, 1)$.
  - I minoranti di $\{(2, 5), (4, 3)\}$ sono le coppie (x, y) tali che $x | \text{MCD}(2, 4) = 2$ e $y | \text{MCD}(5, 3) = 1$.
    - $x \in \{1, 2\}$, $y \in \{1\}$.
    - Minoranti: $(1, 1), (2, 1)$. L'infimum è il massimo tra questi, cioè $(2, 1)$.
  - (Nota: i tuoi appunti a pag. 24 sembrano calcolare $\text{mcm}(5, 3) = 15$ per la seconda componente, che sarebbe per il supremum/join).
  - Supremum: $(2, 5) \vee (4, 3) = (\text{mcm}(2, 4), \text{mcm}(5, 3)) = (4, 15)$.

9. Un Ordine Speciale su $\mathbb{N}^*$ (pag. 25-28)

Questa parte è un po' più avanzata e introduce un ordine specifico.

Sia $a \in \mathbb{N}^*$. Se la sua fattorizzazione in primi distinti è $a = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$, definiamo una funzione $f : \mathbb{N}^* \to \mathbb{N}_0$ (naturali incluso lo zero):

$$f(a) = n_1 + n_2 + \cdots + n_t$$
$$f(1) = 0$$

($f(a)$ è la somma degli esponenti nella fattorizzazione in primi distinti, a volte chiamata $\Omega(a)$ se i primi non sono necessariamente distinti, o $\omega(a)$ se sono distinti e si contano i fattori primi distinti. Qui sembra la somma degli esponenti, quindi $\Omega(a)$).

Definiamo una relazione d'ordine σ su $\mathbb{N}^*$:

$$a \,\sigma\, b \iff (a = b) \text{ oppure } (a|b \text{ propriamente (cioè } a \neq b) \text{ E } f(a) < f(b))$$

(I tuoi appunti dicono $a \,\sigma\, b \iff (a = b) \vee ((a|b \text{ propriamente}) \wedge (f(b) = f(a) + \text{qualcosa positivo}))$ che è equivalente a $f(a) < f(b)$ quando $a|b$ e $a \neq b$).

- **Esempi con f:**
  - $f(1) = 0$
  - $f(p) = 1$ per p primo (es. $f(5) = 1$)
  - $f(p^k) = k$ (es. $f(8) = f(2^3) = 3$, $f(9) = f(3^2) = 2$)
  - $f(p_1^{n_1} p_2^{n_2}) = n_1 + n_2$ (es. $f(10) = f(2^1 \cdot 5^1) = 1 + 1 = 2$)
- **Esempi con σ:**
  - $2 \,\sigma\, 4$? $2|4$, $2 \neq 4$. $f(2) = 1, f(4) = 2$. $f(2) < f(4)$. Sì, $2 \,\sigma\, 4$.
  - $2 \,\sigma\, 6$? $2|6$, $2 \neq 6$. $f(2) = 1, f(6) = f(2 \cdot 3) = 2$. $f(2) < f(6)$. Sì, $2 \,\sigma\, 6$.
  - $6 \,\sigma\, 12$? $6|12$, $6 \neq 12$. $f(6) = 2, f(12) = f(2^2 \cdot 3) = 2 + 1 = 3$. $f(6) < f(12)$. Sì, $6 \,\sigma\, 12$.
  - $4 \,\sigma\, 6$? $4 \nmid 6$. Quindi non sono in relazione σ (a meno che $4 = 6$, falso).
- **L'insieme $L = \{5, 10, 9, 8, 27, 64\}$ con l'ordine σ (pag. 27):**
  - $f(5) = 1$
  - $f(10) = 2$ ($5|10, f(5) < f(10) \implies 5 \,\sigma\, 10$)
  - $f(9) = 2$
  - $f(8) = 3$
  - $f(27) = 3$ ($9|27, f(9) < f(27) \implies 9 \,\sigma\, 27$)
  - $f(64) = 6$ ($8|64, f(8) < f(64) \implies 8 \,\sigma\, 64$)
  - Come sono 10 e 9? $10 \nmid 9$, $9 \nmid 10$. Non confrontabili.
  - Come sono 8 e 9? $8 \nmid 9$, $9 \nmid 8$. Non confrontabili.
  - La domanda se questo L forma un reticolo sotto σ è complessa. Richiederebbe di verificare l'esistenza di inf e sup per tutte le coppie usando l'ordine σ all'interno di L.
  - I tuoi appunti a pag. 28 dicono che $M = \{5, 10, 9, 16, 81, 256\}$ con $f(16) = f(2^4) = 4, f(81) = f(3^4) = 4, f(256) = f(2^8) = 8$ **NON è un reticolo**. Questo suggerisce che tali strutture non sono facilmente reticoli.

Affrontare Concetti Complessi

La parte sull'ordine σ è un po' un rompicapo! È un ottimo esercizio per capire come si possono definire ordini non standard. Se ti senti bloccato, concentrati sulla definizione di f e σ, prova con coppie piccole, e non preoccuparti se l'analisi completa di un insieme come L o M sembra difficile. È normale!

Punti Chiave della Lezione

- Un **reticolo** può essere definito sia come un poset dove ogni coppia ha inf/sup, sia come una struttura algebrica con operazioni $\wedge, \vee$ che soddisfano leggi associative, commutative e di assorbimento.
- Esempi importanti: insiemi totalmente ordinati, $(\mathcal{P}(S), \subseteq, \cap, \cup)$, $(\mathbb{D}_n, |, \text{MCD}, \text{mcm})$.
- Un reticolo è **limitato** se ha un elemento minimo 0 e massimo 1. I reticoli finiti sono sempre limitati.
- Un **sottoreticolo** è un sottoinsieme chiuso rispetto a $\wedge$ e $\vee$.
- Un **isomorfismo di reticoli** è una biiezione che preserva $\wedge$ e $\vee$ (e quindi anche l'ordine).
- Un reticolo limitato è **complementato** se ogni elemento a ha un complemento $\bar{a}$ ($a \wedge \bar{a} = 0, a \vee \bar{a} = 1$). Non tutti i reticoli limitati lo sono (es. catene lunghe, $\mathbb{D}_n$ in generale).

Domande per la Riflessione Personale

1. Riesci a pensare a un esempio di poset che *non* è un reticolo? (Suggerimento: cerca una coppia di elementi che non abbiano un infimum o un supremum unico).
2. Prendi il reticolo $\mathbb{D}_{30}$ (divisori di 30). Disegna il suo diagramma di Hasse. È limitato? È complementato?
3. Se L è un reticolo, $0, 1 \in L$ sono i suoi limiti. Qual è il complemento di 0? E di 1?

Lezione 22 di Algebra Avanzata - 03 Giugno 2025

Docente: Maria Rosaria Celentani
Argomenti Principali: Sottoanelli, Reticoli (Dualità, Complementati, Distributivi, Booleani), Algebre di Boole, Anelli Booleani.

Ricorda!

- Usa il tuo **dizionario visuale** per i simboli che incontriamo. Se un simbolo è nuovo o ostico, disegnalo e associalo a un'immagine o a una parola chiave che ti aiuti a ricordarlo!
- Non esitare a **fare pause** quando ne senti il bisogno. Il cervello impara meglio quando è riposato.
- Se un concetto sembra un mostro, spezzettiamolo in parti più piccole. Insieme, possiamo domarlo!

---

1. Sottoanelli: Piccoli Mondi negli Anelli

Ricordi cosa sia un **anello** $(A, +, \cdot)$? È una struttura algebrica con due operazioni, un po' come i numeri interi che puoi sommare e moltiplicare.

Ora, immaginiamo di trovare un "piccolo mondo" all'interno di un anello più grande, che si comporta esso stesso come un anello. Quello è un **sottoanello**!

Definizione: Sottoanello

Sia $(A, +, \cdot)$ un anello e sia B un sottoinsieme **non vuoto** di A ($B \subseteq A$, $B \neq \emptyset$).
Diciamo che $(B, +, \cdot)$ è un **sottoanello** di A se soddisfa queste condizioni:

1. **B è stabile (o chiuso) rispetto a entrambe le operazioni $+$ e $\cdot$:**
   - Per ogni $b_1, b_2 \in B$, anche $b_1 + b_2 \in B$ (in realtà questa si deduce dal punto 2, ma spesso si verifica la chiusura rispetto alla sottrazione).
   - Per ogni $b_1, b_2 \in B$, anche $b_1 \cdot b_2 \in B$.
   - Più sinteticamente (e comunemente): per ogni $b_1, b_2 \in B$, $b_1 - b_2 \in B$ e $b_1 \cdot b_2 \in B$.
2. **$(B, +)$ è un gruppo abeliano.** (Deve contenere lo zero dell'anello A, e l'opposto di ogni suo elemento).
3. **$(B, \cdot)$ è un semigruppo.** (L'operazione $\cdot$ è associativa in B, ma questo è ereditato da A).

In pratica, se B è chiuso per sottrazione e per moltiplicazione, e non è vuoto, allora è un sottoanello!

Esempio Visto a Lezione (Pagina 1 degli appunti):

Consideriamo l'anello $A = M_{2,2}(\mathbb{R})$ delle matrici 2×2 con coefficienti reali, con le usuali operazioni di somma $(+)$ e prodotto $(\cdot)$ tra matrici.
Sia B il seguente sottoinsieme di A:

$$B = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}$$

Questo insieme B è un sottoanello di A? Vediamo!

- **B non è vuoto?** Certo, se $a = 0$, la matrice nulla $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ appartiene a B.
- **Chiusura rispetto alla sottrazione:**
  Prendiamo due matrici generiche in B:
  $X = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ e $Y = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$, con $a, b \in \mathbb{R}$.
  La loro differenza è:

  $$X - Y = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a-b & 0 \\ 0 & 0 \end{pmatrix}$$

  Poiché $a - b$ è ancora un numero reale, la matrice $X - Y$ ha la forma richiesta per appartenere a B. Quindi, B è chiuso rispetto alla sottrazione.
- **Chiusura rispetto alla moltiplicazione:**
  Il loro prodotto è:

  $$X \cdot Y = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a \cdot b + 0 \cdot 0 & a \cdot 0 + 0 \cdot 0 \\ 0 \cdot b + 0 \cdot 0 & 0 \cdot 0 + 0 \cdot 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$$

Poiché ab è ancora un numero reale, la matrice $X \cdot Y$ appartiene a B. Quindi, B è chiuso rispetto alla moltiplicazione.

Conclusione: Sì, B è un sottoanello di $M_{2,2}(\mathbb{R})$!

Un dettaglio menzionato negli appunti (pag. 1):

$I_A \neq I_B$ in generale. $I_A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
L'elemento $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ agisce come identità moltiplicativa *all'interno* di B (se B fosse un anello unitario a sé stante), ma non è l'identità di A.
In questo specifico esempio B, l'elemento $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ è l'unità di B.
Chiamiamolo $1_B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Se moltiplichi qualsiasi matrice $X \in B$ per 1_B, ottieni X.

---

2. Reticoli: L'Arte dell'Ordine

Passiamo ora ai **reticoli**. Immagina una struttura dove gli elementi sono "ordinati" in qualche modo, e per ogni coppia di elementi possiamo trovare un "punto d'incontro superiore" e un "punto d'incontro inferiore".

Definizione: Reticolo (con relazione d'ordine $\leq$)

Un insieme parzialmente ordinato $(L, \leq)$ (cioè $\leq$ è riflessiva, antisimmetrica, transitiva) si dice un **reticolo** se, per ogni coppia di elementi $a, b \in L$, esistono:

1. L'**estremo inferiore** (o *meet* o *infimum*), indicato con $a \wedge b$ (leggi "a meet b" o "a inf b"). È il più grande elemento che è $\leq a$ e $\leq b$.
2. L'**estremo superiore** (o *join* o *supremum*), indicato con $a \vee b$ (leggi "a join b" o "a sup b"). È il più piccolo elemento che è $\geq a$ e $\geq b$.

Possiamo anche definire un reticolo algebricamente con le operazioni $\wedge$ (meet) e $\vee$ (join) che soddisfano certe proprietà (associatività, commutatività, assorbimento).

2.1. Principio di Dualità (Pagina 2)

Questo è un concetto super potente e elegante! È come guardare un'immagine allo specchio.

Principio di Dualità per Reticoli

Se un enunciato (una proprietà, un teorema) è valido per **tutti** i reticoli, allora anche l'enunciato **duale** è valido per tutti i reticoli.

Come si ottiene l'enunciato duale?

- Si scambia $\leq$ con $\geq$.
- Si scambia $\wedge$ con $\vee$.
- Se presenti, si scambiano gli eventuali elementi 0_L (minimo) e 1_L (massimo).

Se hai un reticolo $(L, \leq)$, il suo **reticolo duale** è $(L^*, \geq^*)$, dove $L^* = L$ e la relazione $a \leq^* b$ in L^* è definita come $b \leq a$ in L (o, come scritto negli appunti, $a \leq^* b \iff a \geq b$). Le operazioni diventano:

- $\wedge^*$ (meet nel duale) corrisponde a $\vee$ (join nell'originale).
- $\vee^*$ (join nel duale) corrisponde a $\wedge$ (meet nell'originale).

Esempi di Enunciati Duali (dalla Pagina 3):

Sia $(L, \leq)$ un reticolo.

- **Enunciato** a: $\forall a \in L, \exists b \in L \mid b \leq a$. (Per ogni elemento, ne esiste uno più piccolo o uguale).
  - **Enunciato duale** a^*: $\forall a \in L, \exists b \in L \mid b \geq a$. (Per ogni elemento, ne esiste uno più grande o uguale).
- **Enunciato** a: $\forall a, b \in L, \exists c \in L \mid c \leq a \wedge b$.
  - **Enunciato duale** a^*: $\forall a, b \in L, \exists c \in L \mid c \geq a \vee b$.
- **Enunciato** a: Se esiste 0_L (elemento minimo), allora $0_L \leq a, \forall a \in L$.
  - **Enunciato duale** a^*: Se esiste 1_L (elemento massimo), allora $1_L \geq a, \forall a \in L$.

Pensa alla musica! Se hai una melodia che sale, la sua "duale" potrebbe essere una melodia che scende in modo speculare. Il principio di dualità ci dice che se certe armonie funzionano con la melodia originale, armonie "speculari" funzioneranno con la melodia duale.

2.2. Esempio Pratico: Una Relazione d'Ordine su $\mathbb{N} \times \mathbb{N}$ (Pagine 4-6)

Consideriamo l'insieme $\mathbb{N} \times \mathbb{N}$ (coppie di numeri naturali, assumendo $\mathbb{N} = \{0, 1, 2, \dots\}$ o $\{1, 2, 3, \dots\}$ a seconda della convenzione usata a lezione – qui l'uso di $3^0 \cdot 7^0$ implica $0 \in \mathbb{N}$ per gli esponenti).
Definiamo una relazione ρ (che indicheremo con $\leq_\rho$ per chiarezza) su $\mathbb{N} \times \mathbb{N}$ così:
Per $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$:

$$(a, b) \leq_\rho (c, d) \iff 3^a \cdot 7^b \leq 3^c \cdot 7^d$$

dove $\leq$ è la solita relazione d'ordine sui numeri naturali.

Dimostriamo che $(\mathbb{N} \times \mathbb{N}, \leq_\rho)$ è un insieme parzialmente ordinato (POSET):

1. **Riflessività**: $(a, b) \leq_\rho (a, b)$?
   Questo significa $3^a \cdot 7^b \leq 3^a \cdot 7^b$. Vero, per la riflessività di $\leq$ su $\mathbb{N}$.
2. **Antisimmetria**: Se $(a, b) \leq_\rho (c, d)$ e $(c, d) \leq_\rho (a, b)$, allora $(a, b) = (c, d)$?
   - $(a, b) \leq_\rho (c, d) \implies 3^a \cdot 7^b \leq 3^c \cdot 7^d$.
   - $(c, d) \leq_\rho (a, b) \implies 3^c \cdot 7^d \leq 3^a \cdot 7^b$.
     Se entrambi sono veri, allora $3^a \cdot 7^b = 3^c \cdot 7^d$. Per il **Teorema Fondamentale dell'Aritmetica** (unicità della scomposizione in fattori primi), questo implica che $a = c$ e $b = d$. Quindi $(a, b) = (c, d)$. Vera.
3. **Transitività**: Se $(a, b) \leq_\rho (c, d)$ e $(c, d) \leq_\rho (e, f)$, allora $(a, b) \leq_\rho (e, f)$?
   - $(a, b) \leq_\rho (c, d) \implies 3^a \cdot 7^b \leq 3^c \cdot 7^d$.
   - $(c, d) \leq_\rho (e, f) \implies 3^c \cdot 7^d \leq 3^e \cdot 7^f$.
     Per la transitività di $\leq$ su $\mathbb{N}$, segue che $3^a \cdot 7^b \leq 3^e \cdot 7^f$.
     Quindi $(a, b) \leq_\rho (e, f)$. Vera.

Quindi, $(\mathbb{N} \times \mathbb{N}, \leq_\rho)$ è un POSET.

È un ordine totale? (Pagina 5)
Sì. Dati due elementi qualsiasi (a, b) e (c, d), i numeri $N_1 = 3^a \cdot 7^b$ e $N_2 = 3^c \cdot 7^d$ sono numeri naturali. Tra N_1 e N_2 vale sempre $N_1 \leq N_2$ oppure $N_2 \leq N_1$. Quindi, o $(a, b) \leq_\rho (c, d)$ o $(c, d) \leq_\rho (a, b)$.
L'insieme è **totalmente ordinato**.

È un reticolo? (Pagina 6)
Sì, ogni insieme totalmente ordinato è un reticolo!
Dati (a, b) e (c, d):

- $(a, b) \wedge (c, d) = \min((a, b), (c, d))$ secondo $\leq_\rho$.
- $(a, b) \vee (c, d) = \max((a, b), (c, d))$ secondo $\leq_\rho$.
  Ad esempio, se $3^a \cdot 7^b \leq 3^c \cdot 7^d$, allora $(a, b) \wedge (c, d) = (a, b)$ e $(a, b) \vee (c, d) = (c, d)$.

Funzione f (Pagina 6):
La funzione $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definita come $f((a, b)) = 3^a \cdot 7^b$ è un **isomorfismo d'ordine** tra $(\mathbb{N} \times \mathbb{N}, \leq_\rho)$ e l'immagine $Im(f) = \{3^a \cdot 7^b \mid a, b \in \mathbb{N}\}$ con la solita relazione $\leq$.
L'immagine $Im(f)$ è un sottoinsieme di $\mathbb{N}$.
Il minimo di $(\mathbb{N} \times \mathbb{N}, \leq_\rho)$ è $(0, 0)$, poiché $f((0, 0)) = 3^0 \cdot 7^0 = 1$ (se $0 \in \mathbb{N}$ per gli esponenti). Se invece $\mathbb{N} = \{1, 2, \dots\}$, il minimo sarebbe $(1, 1)$ e $f((1, 1)) = 3^1 \cdot 7^1 = 21$. L'appunto dice `min(N x N) = 1` e poi `f( (1) ) = { (0,0) }` (sembra una notazione un po' confusa, ma probabilmente si riferisce al fatto che 1 è il minimo dell'immagine e corrisponde a $(0, 0)$).

Esercizio Proposto (Pagina 7):
Ripetere l'esercizio con la relazione σ (che indicheremo con $\leq_\sigma$):

$$(a, b) \leq_\sigma (c, d) \iff (3^a \cdot 7^b) \text{ divide } (3^c \cdot 7^d)$$

Questa è la relazione di **divisibilità**.
Questo definisce un altro POSET. Sarà un reticolo? Sarà totalmente ordinato? (Spoiler: è un reticolo, ma non totalmente ordinato. Ad esempio $(1, 0)$ e $(0, 1)$ non sono confrontabili, cioè $3^1 \cdot 7^0 = 3$ non divide $3^0 \cdot 7^1 = 7$, e viceversa).
Prova a verificarlo! È un ottimo esercizio.

---

3. Tipi Speciali di Reticoli

Non tutti i reticoli sono uguali! Alcuni hanno proprietà speciali.

3.1. Reticoli Limitati (Pagina 8, 10)

Definizione: Reticolo Limitato

Un reticolo $(L, \leq)$ (o $(L, \wedge, \vee)$) si dice **limitato** se possiede:

- Un elemento minimo, chiamato **zero** (0_L o 0), tale che $0_L \leq x$ per ogni $x \in L$.
- Un elemento massimo, chiamato **uno** (1_L o 1), tale che $x \leq 1_L$ per ogni $x \in L$.

Nelle notazioni algebriche:

- $x \vee 0_L = x$ e $x \wedge 0_L = 0_L$
- $x \wedge 1_L = x$ e $x \vee 1_L = 1_L$
  (L'appunto a pag. 10 dice che 0_L è l'elemento neutro per $\vee$, e 1_L è l'elemento neutro per $\wedge$).

3.2. Reticoli Complementati (Pagine 8-9)

Questa è come trovare l' "opposto" o il "contrario" di un elemento, ma in senso reticolare.

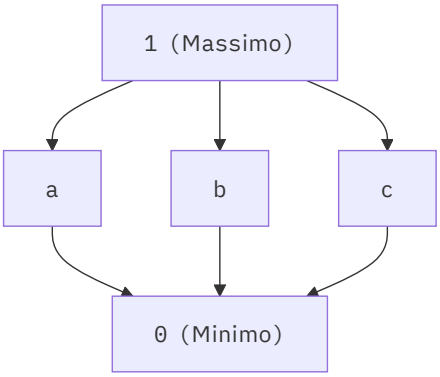
Definizione: Reticolo Complementato

Un reticolo **limitato** $(L, \leq, 0_L, 1_L)$ si dice **complementato** se per ogni elemento $a \in L$ esiste almeno un **complemento** $\bar{a} \in L$ tale che:

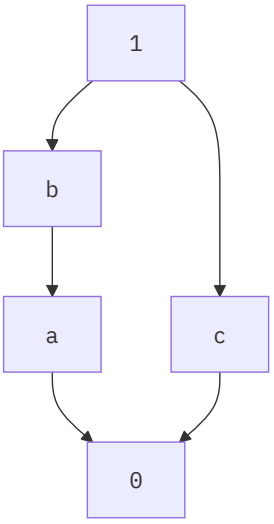
$$a \wedge \bar{a} = 0_L \quad \text{e} \quad a \vee \bar{a} = 1_L$$

Esempi Visivi (dai disegni nelle pagine 8-9):

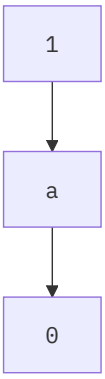
- **Diagramma a diamante (Pagina 8):**



  In questo diagramma (che assomiglia al reticolo dei sottospazi di uno spazio vettoriale di dimensione 2, o a un reticolo M_3 se a, b, c sono atomi non confrontabili), se prendiamo l'elemento a:
  - Un suo complemento potrebbe essere b se $a \wedge b = 0$ e $a \vee b = 1$.
  - Un suo complemento potrebbe essere c se $a \wedge c = 0$ e $a \vee c = 1$.
    L'appunto dice: "a ha come complementi b e c". Questo implica che i complementi non sono necessariamente unici.
- **Diagramma a pentagono (Pagina 9, sinistra):**



  In un reticolo a forma di pentagono (chiamato N_5), l'elemento a potrebbe avere c come complemento, ma l'elemento b potrebbe non averne.
  L'appunto dice: "c ha come complementi sia a che b". Questo è un po' strano, bisogna verificare le relazioni esatte nel diagramma fornito (che è stilizzato). Un tipico N_5 è $0 < a < b < 1$ e $0 < c < 1$ con a, b non confrontabili con c. In tal caso, per a, c è un complemento se $a \wedge c = 0$ e $a \vee c = 1$. Per b, c è complemento se $b \wedge c = 0$ e $b \vee c = 1$. L'elemento a nel pentagono standard non ha complemento.
- **Non tutti i reticoli limitati sono complementati (Pagina 9, destra):**
  Una catena $0 < a < 1$.



L'elemento a non ha complemento. Infatti:

- $a \wedge x = 0 \implies x = 0$. Ma $a \vee 0 = a \neq 1$.
- $a \vee x = 1 \implies x = 1$. Ma $a \wedge 1 = a \neq 0$.
  L'appunto dice: "a non ha complemento". Corretto!

Importante (Pagina 10):
In un reticolo limitato, 0_L ha come unico complemento 1_L, e viceversa.
$0_L \wedge 1_L = 0_L$ e $0_L \vee 1_L = 1_L$.

3.3. Reticoli Distributivi (Pagine 11-14)

La distributività è una proprietà che conosciamo bene dall'aritmetica (la moltiplicazione distribuisce sulla somma). Nei reticoli è simile.

Definizione: Reticolo Distributivo

Un reticolo $(L, \wedge, \vee)$ si dice **distributivo** se valgono le seguenti leggi distributive (basta che ne valga una, l'altra segue per dualità):

1. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ per ogni $a, b, c \in L$. (meet distribuisce su join)
2. $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ per ogni $a, b, c \in L$. (join distribuisce su meet)

Non tutti i reticoli sono distributivi (Pagine 11-12):
I "cattivi ragazzi" che impediscono la distributività sono due reticoli specifici:

- M_3 **(il "diamante"):** Un reticolo con 5 elementi: $0, 1$ e tre elementi a, b, c tra loro non confrontabili, ma tutti compresi tra 0 e 1. (Quello dell'esempio di pag. 8).
  Nell'esempio di pag. 11, si mostra che per M_3:
  $a \wedge (b \vee c) = a \wedge 1 = a$.
  $(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0$.
  Poiché $a \neq 0$, M_3 non è distributivo.
- N_5 **(il "pentagono"):** Un reticolo con 5 elementi: $0 < x < y < 1$ e un altro elemento z tale che $0 < z < 1$, con z non confrontabile con x e y. (Quello dell'esempio di pag. 9, sinistra, se interpretato correttamente).
  Nell'esempio di pag. 12 (che è un N_5 con $a, b, c, 0, 1$ dove $0 < a < b < 1$ e $0 < c < 1$, c non confrontabile con a, b; b al posto di y, a al posto di x e c al posto di z):
  Si verifica la seconda legge distributiva con gli elementi a, b, c come nell'immagine.
  $a \vee (b \wedge c) = a \vee 0 = a$.
  $(a \vee b) \wedge (a \vee c) = b \wedge 1 = b$. (Assumendo $a \vee b = b$ perché $a < b$, e $a \vee c = 1$ e $b \wedge c = 0$).
  Poiché $a \neq b$, N_5 non è distributivo.

Teorema Fondamentale per i Reticoli Distributivi (Pagina 13)

Un reticolo L è **distributivo** se e solo se **non contiene** alcun sottoreticolo isomorfo a M_3 o N_5.
(I disegni a pag. 13 mostrano N_5 e M_3).
Questo è un risultato molto potente per "diagnosticare" la distributività guardando la struttura del reticolo!

Esempio di Test di Distributività (Pagina 14):
Sia $L = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$ l'insieme dei divisori di 36, con la relazione di divisibilità. Questo forma un reticolo. ($a \wedge b = \text{MCD}(a, b)$, $a \vee b = \text{mcm}(a, b)$).
L'appunto prende $M = \{1, 2, 4, 9, 36\}$ e verifica:
$2 \vee (4 \wedge 9) = 2 \vee (\text{MCD}(4, 9)) = 2 \vee 1 = \text{mcm}(2, 1) = 2$.
$(2 \vee 4) \wedge (2 \vee 9) = (\text{mcm}(2, 4)) \wedge (\text{mcm}(2, 9)) = 4 \wedge 18 = \text{MCD}(4, 18) = 2$.
Qui sembra funzionare. (L'appunto dice $2 \vee (4 \wedge 9) = 2$ (X), e $(2 \vee 4) \wedge (2 \vee 9) = 4 \wedge 36 = 4$. Questo non è corretto, $\text{mcm}(2, 9) = 18$, $\text{MCD}(4, 18) = 2$. Sembra ci sia un errore di calcolo o trascrizione negli appunti manoscritti. Il reticolo dei divisori di 36 è distributivo).
Rifacciamo il calcolo come nell'appunto, ma con i simboli corretti:

$a = 2, b = 4, c = 9$.
$a \vee (b \wedge c) = 2 \vee \text{MCD}(4, 9) = 2 \vee 1 = 2$.
$(a \vee b) \wedge (a \vee c) = \text{mcm}(2, 4) \wedge \text{mcm}(2, 9) = 4 \wedge 18 = \text{MCD}(4, 18) = 2$.
Quindi per questa terna a, b, c la proprietà è verificata.

Controesempio (Pagina 15): "No reticolo"
Il diagramma a pagina 15 mostra una struttura che non è un reticolo. Probabilmente perché per alcuni elementi (es. a e d) non esiste un unico estremo superiore o inferiore. Ad esempio, b e c sono entrambi "sopra" a e d. Se non c'è un *minimo* tra questi "limiti superiori comuni", non è un reticolo.

Unicità del Complemento (Pagina 16):

Proposizione

Sia $(L, \wedge, \vee)$ un reticolo **distributivo** e **limitato**. Se un elemento $a \in L$ possiede un complemento, allora tale complemento è **unico**.

Dimostrazione (idea):
Supponiamo che $\bar{a}$ e $\hat{a}$ siano due complementi di a.
Cioè:

1. $a \wedge \bar{a} = 0_L$, $a \vee \bar{a} = 1_L$
2. $a \wedge \hat{a} = 0_L$, $a \vee \hat{a} = 1_L$

Vogliamo dimostrare che $\bar{a} = \hat{a}$.
Consideriamo $\bar{a}$:
$\bar{a} = \bar{a} \wedge 1_L$ (perché 1_L è massimo)
$\bar{a} = \bar{a} \wedge (a \vee \hat{a})$ (sostituisco 1_L usando la proprietà di $\hat{a}$)
$\bar{a} = (\bar{a} \wedge a) \vee (\bar{a} \wedge \hat{a})$ (**uso la distributività!**)
$\bar{a} = 0_L \vee (\bar{a} \wedge \hat{a})$ (sostituisco $\bar{a} \wedge a = 0_L$)
$\bar{a} = \bar{a} \wedge \hat{a}$ $(*)$

In modo simmetrico (scambiando i ruoli di $\bar{a}$ e $\hat{a}$), si ottiene:
$\hat{a} = \hat{a} \wedge \bar{a}$ $(**)$

Poiché $\wedge$ è commutativa, $\bar{a} \wedge \hat{a} = \hat{a} \wedge \bar{a}$.
Quindi, da $(*)$ e $(**)$, segue che $\bar{a} = \hat{a}$.
Il complemento è unico! Fantastico, vero? La distributività è la chiave qui.

Esempi di Reticoli Distributivi (Pagina 17):

1. $(\mathcal{P}(S), \subseteq)$ (l'insieme delle parti di un insieme S, ordinato per inclusione). Le operazioni di meet e join sono $\cap$ (intersezione) e $\cup$ (unione).

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

   Queste sono le note proprietà distributive dell'intersezione e dell'unione. Quindi $(\mathcal{P}(S), \cap, \cup)$ è distributivo.
2. Un **insieme totalmente ordinato** è sempre distributivo.
   Se $a \leq b \leq c$ (o qualsiasi altra permutazione d'ordine), le leggi distributive si riducono a identità semplici. Ad esempio, se $a \leq b \leq c$:
   $a \wedge (b \vee c) = a \wedge c = a$.
   $(a \wedge b) \vee (a \wedge c) = a \vee a = a$. Funziona!

Esempio di Reticolo NON Distributivo (Pagina 18):
Il reticolo $(\mathbb{N}_+, |)$ dei numeri naturali positivi con la relazione di divisibilità **non è** in generale distributivo.
Prendiamo i divisori di 30: $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$.
Scegliamo $a = 2, b = 3, c = 5$. Questi sono gli "atomi" sopra l'1.
$a \wedge (b \vee c) = 2 \wedge \text{mcm}(3, 5) = 2 \wedge 15 = \text{MCD}(2, 15) = 1$.
$(a \wedge b) \vee (a \wedge c) = \text{MCD}(2, 3) \vee \text{MCD}(2, 5) = 1 \vee 1 = 1$.
Questo funziona. Ma dobbiamo trovare un controesempio.
Gli elementi $a = 6, b = 10, c = 15$ formano un M_3 (con $0_L = \text{MCD}(6, 10, 15)$ e $1_L = \text{mcm}(6, 10, 15)$)? No.
Il diagramma disegnato a pagina 18 per $(\mathbb{N}, |)$ è quello dei divisori di 30, che è isomorfo a $\mathcal{P}(\{p_1, p_2, p_3\})$, quindi *dovrebbe* essere distributivo.
Ah, l'appunto dice "NO" riferendosi a $(\mathbb{N}, |)$ in generale. L'esempio sotto con D_{30} (elementi $1, 2, 3, 5, 30$ e altri impliciti) è fatto per mostrare un N_5.
Se $a = 2$, $b = 3 \cdot 5 = 15$, $c = 5 \cdot k$ (no, questo non forma N5).
Il tipico esempio di non distributività in $(\mathbb{N}_+, |)$ si ha considerando i divisori di un numero che abbia almeno due fattori primi con esponente ≥ 1 e un altro fattore primo. Esempio: $D_{12} = \{1, 2, 3, 4, 6, 12\}$. Scegli $a = 2, b = 3, c = 2$.
$a \vee (b \wedge c)$ vs $(a \vee b) \wedge (a \vee c)$.
In D_{12}, M_3 è dato da $\{2, 3, \text{mcm}(2, 3) = 6, \text{MCD}(2, 3) = 1\}$. No, M_3 è $\{d, dp_1, dp_2, dp_3, dp_1p_2p_3\}$.
Un N_5 in $(\mathbb{N}_+, |)$ può essere formato da $\{1, p, q, p^2, p^2q\}$ (dove p, q sono primi distinti). E.g. $\{1, 2, 3, 4, 12\}$.
$0 = 1, x = 2, y = 4, 1 = 12, z = 3$.

$x \vee (z \wedge y) = 2 \vee (3 \wedge 4) = 2 \vee \text{MCD}(3,4) = 2 \vee 1 = 2$.
$(x \vee z) \wedge (x \vee y) = (\text{mcm}(2,3)) \wedge (\text{mcm}(2,4)) = 6 \wedge 4 = \text{MCD}(6,4) = 2$.
Questo esempio non mostra la non-distributività.

> ⚠ **L'esempio della non distributività di $(\mathbb{N}, |)$ va chiarito meglio. Il reticolo dei divisori di un numero $n = p_1^{a_1} \cdots p_k^{a_k}$ è distributivo se e solo se tutti gli $a_i \leq 1$ oppure $k \leq 2$. Quindi D_{30} (divisori di $2 \cdot 3 \cdot 5$) è distributivo. D_{12} (divisori di $2^2 \cdot 3$) è distributivo. D_{p^2qr} non lo è. Ad esempio D_{60} (divisori di $2^2 \cdot 3 \cdot 5$) contiene un M_3 (ad es. $\{2, 6, 10\}$ non è un M_3, i tre elementi "intermedi" sono $2 \cdot 3 = 6$, $2 \cdot 5 = 10$, $2 \cdot 2 = 4$). Gli elementi $2, 6, 10$ non sono in M_3.**

Il reticolo D_{pqr} (come D_{30}) è isomorfo a $\mathcal{P}(\{p, q, r\})$ ed è distributivo.
Il reticolo D_{p^2q} (come D_{12}) è distributivo.
Un reticolo L è non distributivo se contiene M_3 o N_5.
Il disegno a pagina 18 con $1, 2, 3, 5$ e un 30 in alto sembra l'ossatura di D_{30}, che è distributivo. Forse si intende che l'intero $(\mathbb{N}, |)$ non è distributivo.

3.4. Reticoli Booleani (Pagine 18-20)

Questi sono i reticoli "perfetti": distributivi E complementati.

Definizione: Reticolo Booleano

Un reticolo $(L, \leq)$ si dice **booleano** se:

1. È **distributivo**.
2. È **complementato**.
   (Essendo complementato, deve essere anche limitato, quindi avere 0_L e 1_L).

L'Esempio per Eccellenza (Pagina 19):
$(\mathcal{P}(S), \subseteq)$ è un reticolo booleano!

- Abbiamo visto che è distributivo.
- È limitato: $0_L = \emptyset$ (insieme vuoto), $1_L = S$ (insieme universo).
- È complementato: per ogni $A \subseteq S$, il suo complemento è $A^c = S \setminus A$ (il complemento insiemistico).
  $A \cap A^c = \emptyset = 0_L$.
  $A \cup A^c = S = 1_L$.
  L'appunto dice: "non è 'un' esempio, è L'ESEMPIO". Questo sottolinea la sua importanza!

Teorema di Rappresentazione per Reticoli Booleani Finiti (Pagina 19)

Sia $(L, \leq)$ un reticolo booleano.

- $(L, \leq)$ è isomorfo a un sottoreticolo di $(\mathcal{P}(S), \subseteq)$ per qualche insieme S. (Questo S è l'insieme degli atomi di L o degli ideali primi/massimali).
- Se L è **finito**, allora esiste un insieme finito S tale che $(L, \leq)$ è isomorfo a $(\mathcal{P}(S), \subseteq)$.
- Inoltre, se L è finito, allora la sua cardinalità (numero di elementi) è una potenza di 2: $|L| = 2^n$ per qualche intero $n \geq 0$ (dove $n = |S|$).

Esempi Grafici (Pagina 20):

- Una catena $0 - a - b - 1$ (4 elementi) **non è booleana** (a meno che non sia $0 - 1$, o $0 - a - 1$ con a auto-complementare, il che non succede). Ad esempio, in $0 < a < b < 1$, a non ha complemento. L'appunto a pag. 20 mostra una catena $0 - a - b - 1$ e dice "non è booleano".
- Un reticolo booleano con $|L| = 2^n$ ha la forma di un ipercubo n-dimensionale.
  $n = 0 \implies |L| = 1$ *(un punto, $0 = 1$).*
  $n = 1 \implies |L| = 2$ (la catena $0 - 1$). Booleano.
  $n = 2 \implies |L| = 4$ *(il "quadrato" $0, a, b, 1$ con a, b complementi l'uno dell'altro). Booleano.*
  $n = 3 \implies |L| = 8$ (il "cubo", come D_{30}). Booleano.
  L'appunto mostra un disegno che potrebbe essere la struttura di D_{30} (un cubo) e un altro che è una lunga catena lineare (non booleana se ha più di 2 elementi).
  La nota $|L| = 2^n$ con un X sopra ($|L| = 2^n\mathbb{X}$) forse significa che *non tutti* i reticoli hanno cardinalità 2^n, solo quelli booleani finiti.

---

4. Algebre di Boole (Pagine 21-23)

Strettamente collegate ai reticoli booleani, le algebre di Boole formalizzano le operazioni.

Definizione: Algebra di Boole

Un'**algebra di Boole** è una struttura $(A, \wedge, \vee, ', 0, 1)$ dove:

- A è un insieme non vuoto.
- $\wedge$ (meet) e $\vee$ (join) sono operazioni binarie su A.
- $'$ (complemento o negazione) è un'operazione unaria su A.
- 0 e 1 sono elementi distinti di A (costanti, o elementi nullari).

Queste operazioni devono soddisfare le seguenti proprietà per ogni $a, b, c \in A$:

1. **Associatività:**
   - $a \wedge (b \wedge c) = (a \wedge b) \wedge c$
   - $a \vee (b \vee c) = (a \vee b) \vee c$
2. **Commutatività:**
   - $a \wedge b = b \wedge a$
   - $a \vee b = b \vee a$
3. **Leggi di Assorbimento:** (Collegano $\wedge$ e $\vee$)
   - $a \wedge (a \vee b) = a$
   - $a \vee (a \wedge b) = a$
4. **Distributività:** (Ognuna implica l'altra)
   - $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
   - $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
5. **Esistenza di Elementi Neutri (0 e 1):**
   - $a \wedge 1 = a$
   - $a \vee 0 = a$
6. **Leggi del Complemento:** (Con l'operazione unaria $'$)
   - $a \wedge a' = 0$
   - $a \vee a' = 1$

Connessione tra Reticoli Booleani e Algebre di Boole (Pagina 22):
Un reticolo booleano $(L, \leq)$ definisce un'algebra di Boole $(L, \wedge, \vee, ', 0_L, 1_L)$ dove 0_L è il minimo, 1_L il massimo, e a' è l'**unico** complemento di a (sappiamo che è unico perché i reticoli booleani sono distributivi).
Viceversa, un'algebra di Boole $(A, \wedge, \vee, ', 0, 1)$ definisce un reticolo booleano $(A, \leq)$ ponendo $a \leq b \iff a \wedge b = a$ (o equivalentemente $a \leq b \iff a \vee b = b$).

Esempio Primario (Pagina 23):
$(\mathcal{P}(S), \cap, \cup, (\cdot)^c, \emptyset, S)$ è l'algebra di Boole per eccellenza.

- Operazione unaria $'$: $A' = S \setminus A$ (complemento insiemistico).

Teorema di Rappresentazione di Stone per Algebre di Boole Finite (Pagina 23)

Ogni algebra di Boole **finita** $(A, \wedge, \vee, ', 0, 1)$ è isomorfa all'algebra di Boole $(\mathcal{P}(S), \cap, \cup, (\cdot)^c, \emptyset, S)$ per qualche insieme finito S. (Questo è essenzialmente lo stesso teorema visto per i reticoli booleani finiti, ma formulato per le algebre).

---

5. Anelli Booleani (Pagine 24-26)

Ora colleghiamo questi concetti con gli anelli!

Definizione: Anello Booleano

Un **anello** $(A, +, \cdot)$ (solitamente unitario, cioè con un'identità moltiplicativa 1_A) si dice **booleano** se ogni suo elemento è **idempotente**, cioè:

$$a^2 = a \cdot a = a \quad \text{per ogni } a \in A$$

Proprietà Fondamentali degli Anelli Booleani (Pagina 24):
Se $(A, +, \cdot)$ è un anello booleano:

1. $a + a = 0$ **(elemento nullo dell'addizione) per ogni** $a \in A$.
   Questo significa che ogni elemento è il suo opposto additivo ($a = -a$).
   L'anello ha **caratteristica 2**.
   Dimostrazione (come negli appunti):
   $(a+b)^2 = a + b$. Ma $(a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$.
   Quindi $a + b = a + ab + ba + b$. Semplificando a e b, otteniamo $ab + ba = 0$.
   Questo vale per ogni a, b. Se $b = a$, allora $a \cdot a + a \cdot a = 0$, cioè $a^2 + a^2 = 0$, quindi $a + a = 0$.
   (Un'altra derivazione più diretta: $(2a)^2 = 2a$. D'altra parte $(2a)^2 = (a+a)^2 = a + a = 2a$. Ma anche $(2a)^2 = (2a)(2a) = 4a^2 = 4a$. Quindi $2a = 4a \implies 2a = 0$.)

L'appunto (pag. 24) parte da $(2a) = (a + a) = 0 \implies a = -a$. Poi $2a = (2a)^2 = 4a^2 = 4a \implies 2a = 0 \quad \forall a \in A$. (corretto: $2a = 0$).

2. L'anello booleano è **commutativo** (cioè $ab = ba$ per ogni $a, b \in A$).
   Dimostrazione (come negli appunti):
   Abbiamo visto sopra che $ab + ba = 0$. Poiché $ba = -ba$ (dalla proprietà $x + x = 0 \implies x = -x$), allora $ab - ba = 0$, quindi $ab = ba$.

Esempio Principale (Pagina 25):
Sia S un insieme. L'insieme delle parti $\mathcal{P}(S)$ con le operazioni:

- $+$: Differenza Simmetrica Δ. ($X \Delta Y = (X \setminus Y) \cup (Y \setminus X)$)
- $\cdot$: Intersezione $\cap$. ($X \cap Y$)
  forma un anello booleano $(\mathcal{P}(S), \Delta, \cap)$.
- L'elemento 0 dell'anello è $\emptyset$. ($X \Delta \emptyset = X$).
- L'elemento 1 dell'anello è S. ($X \cap S = X$).
- Verifichiamo l'idempotenza: $A^2 = A \cap A = A$. Sì!
  L'appunto dice: "CNO se considero $(\mathcal{P}(S), \Delta, \cup)$ non vale la distributività". Qui si riferisce alla distributività di $\cup$ rispetto a Δ, che non è una delle leggi degli anelli. L'anello è $(\mathcal{P}(S), \Delta, \cap)$. La distributività richiesta è $\cap$ su Δ: $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$. Questa è vera.

Teorema di Rappresentazione per Anelli Booleani Finiti (Pagina 26)

Ogni anello booleano **finito** $(A, +, \cdot)$ è isomorfo a un anello $(\mathcal{P}(S), \Delta, \cap)$ per qualche insieme finito S.
(Se A non è finito, è isomorfo a un sottoanello di $(\mathcal{P}(S), \Delta, \cap)$).

---

6. Collegamenti Strutturali: Da Reticoli ad Anelli (Pagine 27-29)

Possiamo costruire un anello booleano a partire da un reticolo booleano!

Sia $(L, \wedge, \vee, ', 0, 1)$ un reticolo booleano. Definiamo le operazioni di anello $(L, +, \cdot)$:

- **Prodotto ($\cdot$):** $a \cdot b = a \wedge b$
  - Questa operazione è associativa e commutativa (ereditato da $\wedge$).
  - L'elemento 1_L (massimo del reticolo) è l'unità per il prodotto: $a \cdot 1_L = a \wedge 1_L = a$.
  - $(L, \cdot)$ è un monoide commutativo con unità 1_L.
- **Somma ($+$):** $a + b = (a \wedge b') \vee (b \wedge a')$
  - Questa è la **differenza simmetrica** espressa con le operazioni del reticolo.
  - $a \wedge b'$ significa "a ma non b". $b \wedge a'$ significa "b ma non a".
  - L'unione ($\vee$) di queste due parti dà $a + b$.

Verifichiamo alcune proprietà dell'anello (Pagine 28):

1. **Elemento nullo per la somma:** È 0_L (minimo del reticolo).
   $a + 0_L = (a \wedge 0_L') \vee (0_L \wedge a')$
   Sappiamo che $0_L' = 1_L$.
   $a + 0_L = (a \wedge 1_L) \vee (0_L \wedge a') = a \vee 0_L = a$. Sì!
2. $a + a = 0_L$ **(ogni elemento è opposto di sé stesso):**
   $a + a = (a \wedge a') \vee (a \wedge a') = 0_L \vee 0_L = 0_L$. Sì!
3. **Idempotenza per il prodotto:** $a \cdot a = a \wedge a = a$. (Questo era già una proprietà di $\wedge$).
   Quindi, $(L, +, \cdot)$ è un anello booleano.

L'appunto a pagina 28 verifica $a \cdot (b + c) = a \cdot b + a \cdot c$ (distributività del prodotto sulla somma):
$a \wedge ((b \wedge c') \vee (c \wedge b')) \neq (a \wedge b) + (a \wedge c)$.
Attenzione! La riga sopra sembra indicare che NON è uguale, il che sarebbe un problema. Deve essere uguale.
$a \cdot (b + c) = a \wedge ((b \wedge c') \vee (c \wedge b'))$.
Per la distributività di $\wedge$ su $\vee$ nel reticolo:
$= (a \wedge (b \wedge c')) \vee (a \wedge (c \wedge b'))$
$= ((a \wedge b) \wedge c') \vee ((a \wedge c) \wedge b')$.
D'altra parte:
$a \cdot b + a \cdot c = (a \wedge b) + (a \wedge c)$.
Sia $X = a \wedge b$ e $Y = a \wedge c$.
$X + Y = (X \wedge Y') \vee (Y \wedge X')$.
$X \wedge Y' = (a \wedge b) \wedge (a \wedge c)' = (a \wedge b) \wedge (a' \vee c')$.
$Y \wedge X' = (a \wedge c) \wedge (a \wedge b)' = (a \wedge c) \wedge (a' \vee b')$.
Questa uguaglianza è una proprietà nota e si può dimostrare (anche se è un po' laboriosa).

Relazione d'Ordine nell'Anello Booleano (Pagina 29):
Se partiamo da un anello booleano $(A, +, \cdot)$, come possiamo recuperare la relazione d'ordine del reticolo booleano associato?

$$a \leq b \iff a \cdot b = a$$

Ricorda che $a \cdot b = a \wedge b$. Quindi $a \leq b \iff a \wedge b = a$, che è una delle definizioni standard di $\leq$ in un reticolo.

- Se $a \leq b$ e $b \leq a$, allora $a \cdot b = a$ e $b \cdot a = b$. Poiché $\cdot$ è commutativa, $a = b$. (Antisimmetria)
- Se $a \leq b$ e $b \leq c$, allora $a \cdot b = a$ e $b \cdot c = b$.
  $a \cdot c = (a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot b = a$. Quindi $a \leq c$. (Transitività)

Riepilogo della Lezione: Punti Chiave

Cosa abbiamo imparato oggi:

- Un **sottoanello** è un sottoinsieme di un anello che è esso stesso un anello con le stesse operazioni.
- Un **reticolo** è un insieme parzialmente ordinato dove ogni coppia di elementi ha un estremo superiore (join $\vee$) e un estremo inferiore (meet $\wedge$).
- Il **Principio di Dualità** ci permette di ottenere nuovi teoremi validi scambiando $\leq / \geq$ e $\wedge / \vee$.
- I reticoli possono essere **limitati** (con 0 e 1), **complementati** (ogni elemento ha un complemento), e **distributivi** (le operazioni $\wedge, \vee$ si distribuiscono l'una sull'altra).
- Un reticolo è distributivo se e solo se non contiene sottoreticoli M_3 (diamante) o N_5 (pentagono).
- Nei reticoli distributivi e limitati, il complemento (se esiste) è **unico**.
- Un **reticolo booleano** è distributivo e complementato. $(\mathcal{P}(S), \subseteq)$ è l'esempio fondamentale. I reticoli booleani finiti sono isomorfi a $\mathcal{P}(S)$ con $|L| = 2^{|S|}$.
- Un'**algebra di Boole** è la struttura algebrica $(A, \wedge, \vee, ', 0, 1)$ che cattura le proprietà dei reticoli booleani.
- Un **anello booleano** è un anello $(A, +, \cdot)$ dove $a^2 = a$ per ogni a. Questo implica che $a + a = 0$ (caratteristica 2) e l'anello è commutativo. $(\mathcal{P}(S), \Delta, \cap)$ è l'esempio chiave.
- Esiste una stretta **corrispondenza** tra reticoli booleani, algebre di Boole e anelli booleani. Possiamo definire le operazioni dell'uno a partire dall'altro.

Domande per Te! (Spunti di Riflessione)

1. Prova a pensare a un altro esempio di sottoanello, magari usando i numeri interi o i polinomi. Quali condizioni devi verificare?
2. Riguarda l'esercizio sulla relazione $(a, b) \leq_\sigma (c, d) \iff (3^a \cdot 7^b)$ divide $(3^c \cdot 7^d)$.
   - È un ordine parziale?
   - È un ordine totale? (Suggerimento: pensa a $(2, 0)$ e $(0, 1)$ cioè $3^2 = 9$ e $7^1 = 7$. 9 divide 7? 7 divide 9?)
   - Se è un reticolo, come sono definiti *meet* e *join*?
3. Disegna il diagramma di Hasse del reticolo dei divisori di 12 (D_{12}). È distributivo? È booleano?
4. Nell'anello booleano $(\mathcal{P}(S), \Delta, \cap)$, se $S = \{1, 2, 3\}$, prendi $A = \{1, 2\}$ e $B = \{2, 3\}$. Calcola $A + B$ e $A \cdot B$.
5. Qual è la cosa più sorprendente o interessante che hai imparato oggi sui reticoli o sulle strutture booleane? C'è qualcosa che ti ricorda un concetto musicale o di un'altra tua passione?

#tag/algebra #tag/algebraavanzata #tag/lezione #tag/anelli #tag/sottoanelli #tag/reticoli #tag/dualità #tag/reticolibimitati #tag/reticolicomplementati #tag/reticolidistributivi #tag/M3N5 #tag/reticolibooleani #tag/algebreBoole #tag/anelliBooleani #tag/teoremiRappresentazione

Lezione (Bonus) 23: Il Mondo dei Polinomi

#tag/algebra #tag/polinomi #tag/lezione23

Indice della Lezione

1. Definizioni di Base sui Polinomi
2. Operazioni tra Polinomi
3. Grado di un Polinomio e Teorema dei Gradi
4. Elementi Speciali: Unità, Associati e Polinomi Monici
5. Divisione tra Polinomi: L'Algoritmo Euclideo
6. Radici di un Polinomio e Teorema di Ruffini
7. Polinomi e Funzioni Polinomiali

8. Divisibilità e Irriducibilità
9. Teorema di Fattorizzazione Unica
10. Punti Chiave della Lezione
11. Domande per la Riflessione

Definizioni di Base sui Polinomi

Definizione: Anello dei Polinomi

Dato un anello commutativo unitario $(A, +, \cdot)$, l'insieme dei polinomi a coefficienti in A nell'indeterminata x, indicato con $A[x]$, è l'insieme di tutte le espressioni formali del tipo:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

dove i coefficienti a_i appartengono all'anello A e n è un numero intero non negativo.

Spiegazione Semplice: Pensa a un polinomio come a una "ricetta" matematica. Gli **ingredienti** sono i numeri dell'anello A (i **coefficienti** a_i), e li combiniamo con potenze crescenti di una variabile "magica" x (l'**indeterminata**).

- **Polinomio nullo:** Il polinomio con tutti i coefficienti uguali a zero. Lo indichiamo con 0.
- **Polinomi costanti:** Polinomi del tipo $f(x) = a_0$. Praticamente, solo un numero.

Operazioni tra Polinomi

Possiamo sommare e moltiplicare i polinomi in modo molto intuitivo.

Somma di Polinomi

Come sommare due polinomi

Per sommare due polinomi, $f(x)$ e $g(x)$, semplicemente **sommiamo i coefficienti dei termini con lo stesso grado**.

Se $f(x) = a_0 + a_1x + \dots$ e $g(x) = b_0 + b_1x + \dots$, allora:

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots$$

Esempio di Somma

- $f(x) = 3 - 5x^2 + 7x^4$
- $g(x) = 1 + 3x + 4x^2 - 2x^3$

$(f + g)(x) = (3 + 1) + 3x + (-5 + 4)x^2 - 2x^3 + 7x^4 = \mathbf{4 + 3x - x^2 - 2x^3 + 7x^4}$

Prodotto di Polinomi

Il prodotto è un po' più elaborato, ma segue la regola "tutti per tutti".

Formula del Prodotto

Se $f(x) \cdot g(x) = c_0 + c_1x + c_2x^2 + \dots$, il coefficiente c_k si ottiene sommando tutti i prodotti $a_i \cdot b_j$ tali che $i + j = k$.

$$c_k = \sum_{i+j=k} a_ib_j$$

Spiegazione Semplice: È come la normale moltiplicazione che hai sempre fatto, distribuendo ogni termine del primo polinomio per ogni termine del secondo.

Con queste operazioni, $(A[x], +, \cdot)$ diventa a sua volta un **anello commutativo unitario**. L'elemento neutro della somma è il polinomio nullo, e quello del prodotto è il polinomio costante 1.

Grado di un Polinomio e Teorema dei Gradi

#tag/definizione #tag/teorema

Definizione: Grado di un Polinomio

Il **grado** di un polinomio non nullo $f(x)$, indicato con $\mathrm{gr}(f)$ o $\delta(f)$, è il **massimo esponente** della x con un coefficiente diverso da zero.

- Il coefficiente di grado massimo è detto **coefficiente direttore**.
- Per convenzione, il grado del polinomio nullo è $-\infty$.

Proprietà dei Gradi

1. **Grado della Somma:** $\mathrm{gr}(f+g) \leq \max\{\mathrm{gr}(f), \mathrm{gr}(g)\}$
   - **Perché "minore o uguale"?** Perché se i gradi sono uguali e i coefficienti direttori sono opposti, si annullano!
   - **Esempio:** Se $f(x) = x$ e $g(x) = -x$, allora $\mathrm{gr}(f) = 1, \mathrm{gr}(g) = 1$. Ma $f(x) + g(x) = 0$, che ha grado $-\infty$.
2. **Grado del Prodotto:** $\mathrm{gr}(f \cdot g) \leq \mathrm{gr}(f) + \mathrm{gr}(g)$

Questa seconda proprietà diventa un'uguaglianza in un caso molto importante.

Teorema: Additività dei Gradi (DIM)

Teorema dei Gradi

Siano $f(x), g(x) \in A[x]$.

1. $\mathrm{gr}(f \cdot g) \leq \mathrm{gr}(f) + \mathrm{gr}(g)$
2. Se A è un **dominio di integrità**, allora vale l'uguaglianza:

$$\mathrm{gr}(f \cdot g) = \mathrm{gr}(f) + \mathrm{gr}(g)$$

Dimostrazione

1. **Ipotesi:** Sia A un dominio di integrità. Questo significa che se prendiamo due elementi non nulli $a, b \in A$, il loro prodotto $a \cdot b$ è anch'esso non nullo.
2. **Polinomi:** Prendiamo due polinomi non nulli:
   - $f(x) = a_n x^n + \cdots + a_0$ con $\mathrm{gr}(f) = n$ (quindi $a_n \neq 0$).
   - $g(x) = b_m x^m + \cdots + b_0$ con $\mathrm{gr}(g) = m$ (quindi $b_m \neq 0$).
3. **Prodotto:** Calcoliamo il prodotto $f(x) \cdot g(x)$. Il termine di grado più alto possibile si ottiene moltiplicando i termini di grado più alto di f e g:

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

4. **Coefficiente Direttore:** Il coefficiente direttore del prodotto è $c_{n+m} = a_n \cdot b_m$.
5. **Conclusione:** Poiché siamo in un dominio di integrità e $a_n \neq 0$ e $b_m \neq 0$, allora anche il loro prodotto $a_n \cdot b_m \neq 0$. Dato che il coefficiente del termine di grado $n+m$ non è zero, il grado del polinomio prodotto è esattamente $n+m$.

$$\mathrm{gr}(f \cdot g) = n + m = \mathrm{gr}(f) + \mathrm{gr}(g)$$

Q.E.D. (Quod Erat Demonstrandum - Come Volevasi Dimostrare)

Cosa succede se A non è un dominio di integrità?

Prendiamo l'anello $\mathbb{Z}_6[x]$. $\mathbb{Z}_6$ non è un dominio perché $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$.

- $f(x) = \bar{5} + \bar{2}x$ (grado 1)
- $g(x) = \bar{1} + \bar{3}x$ (grado 1)
- $f(x) \cdot g(x) = (\bar{5} + \bar{2}x)(\bar{1} + \bar{3}x) = \bar{5} + \overline{15}x + \bar{2}x + \bar{6}x^2 = \bar{5} + (\bar{3} + \bar{2})x + \bar{0}x^2 = \bar{5} + \bar{5}x$
  Il grado del prodotto è 1, che è **diverso** da $\mathrm{gr}(f) + \mathrm{gr}(g) = 1 + 1 = 2$.

Corollario: Se A è un dominio di integrità, allora anche $A[x]$ è un dominio di integrità.

Elementi Speciali: Unità, Associati e Polinomi Monici

Unità in A[x]

Teorema sulle Unità

Se A è un **dominio di integrità**, allora le unità dell'anello dei polinomi $A[x]$ sono esattamente le unità dell'anello dei coefficienti A.

$$\mathcal{U}(A[x]) = \mathcal{U}(A)$$

Spiegazione Semplice: In un dominio (come i numeri interi $\mathbb{Z}$ o i reali $\mathbb{R}$), gli unici polinomi che hanno un "inverso moltiplicativo" sono i polinomi costanti che erano già invertibili nell'anello di partenza. Per esempio, in $\mathbb{Z}[x]$, gli unici polinomi invertibili sono 1 e -1.

Elementi Associati

Definizione: Elementi Associati

Due polinomi $f(x)$ e $g(x)$ si dicono **associati** (e si scrive $f \sim g$) se esiste un'unità $c \in \mathcal{U}(A[x])$ tale che:

$$f(x) = c \cdot g(x)$$

Analogia Musicale: Pensa a due melodie identiche, ma una è suonata a un volume "forte" e l'altra a un volume "piano". La melodia di base è la stessa, cambia solo un "fattore di scala" (l'unità). In $\mathbb{Z}[x]$, $f(x) = x + 1$ è associato a $g(x) = -x - 1$ perché $g(x) = (-1) \cdot f(x)$ e -1 è un'unità.

Polinomi Monici

Definizione: Polinomio Monico

Un polinomio si dice **monico** se il suo coefficiente direttore è **1**.

Esempi di Polinomi Monici

- $x^2 - 3x + 5$ è monico.
- $2x^3 + x - 1$ **non** è monico.

Il Superpotere dei Polinomi Monici: Se il coefficiente direttore di un polinomio $f(x)$ è un'unità, allora $f(x)$ è associato a un **unico** polinomio monico. Basta moltiplicare $f(x)$ per l'inverso del suo coefficiente direttore!

Esercizio Guidato

Verificare se in $\mathbb{Z}_{42}[x]$ il polinomio $f(x) = \overline{25}x^3 + \overline{7}x - \overline{2}$ è associato a un polinomio monico.

1. **Domanda:** Il coefficiente direttore, $\overline{25}$, è un'unità in $\mathbb{Z}_{42}$?
2. **Controllo:** Un elemento $\bar{a}$ è invertibile in $\mathbb{Z}_n$ se e solo se $\text{MCD}(a, n) = 1$.
3. **Calcolo:** $\text{MCD}(25, 42) = \text{MCD}(5^2, 2 \cdot 3 \cdot 7) = 1$. Sì, è invertibile!
4. **Trovare l'inverso:** Usiamo l'algoritmo di Euclide per trovare x, y tali che $25x + 42y = 1$.
   - $42 = 1 \cdot 25 + 17$
   - $25 = 1 \cdot 17 + 8$
   - $17 = 2 \cdot 8 + 1$
     Andando a ritroso:
   - $1 = 17 - 2 \cdot 8 = 17 - 2(25 - 1 \cdot 17) = 3 \cdot 17 - 2 \cdot 25$
   - $1 = 3(42 - 1 \cdot 25) - 2 \cdot 25 = 3 \cdot 42 - 3 \cdot 25 - 2 \cdot 25 = 3 \cdot 42 - 5 \cdot 25$
     In $\mathbb{Z}_{42}$, questo significa $-5 \cdot 25 \equiv 1 \pmod{42}$.
     L'inverso di $\overline{25}$ è $\overline{-5} = \overline{37}$.
5. **Trovare il monico associato:** Moltiplichiamo $f(x)$ per $\overline{37}$.
   - $\overline{37} \cdot (\overline{25}x^3 + \overline{7}x - \overline{2}) = (\overline{37} \cdot \overline{25})x^3 + (\overline{37} \cdot \overline{7})x - (\overline{37} \cdot \overline{2})$
   - $= \overline{1}x^3 + \overline{259}x - \overline{74}$
   - Calcolando i resti modulo 42: $259 = 6 \cdot 42 + 7 \implies \overline{259} = \overline{7}$. $74 = 1 \cdot 42 + 32 \implies \overline{74} = \overline{32}$.
   - Il polinomio monico associato è $\mathbf{x^3 + \overline{7}x - \overline{32}}$.

Divisione tra Polinomi: L'Algoritmo Euclideo

#tag/teorema #tag/dimostrazione

Proprio come per i numeri interi, possiamo fare la divisione con resto anche per i polinomi!

Teorema: Divisione Euclidea tra Polinomi (DIM)

Teorema della Divisione

Siano $f(x), g(x) \in A[x]$, con $g(x) \neq 0$. Se il **coefficiente direttore di $g(x)$ è un'unità** in A, allora esistono e sono **unici** due polinomi $q(x)$ (quoziente) e $r(x)$ (resto) tali che:

$$f(x) = g(x) \cdot q(x) + r(x)$$

con $\text{gr}(r) < \text{gr}(g)$.

Dimostrazione (Esistenza)

La dimostrazione si fa per **induzione sul grado di $f(x)$**.

1. **Caso Base:** Se $\text{gr}(f) < \text{gr}(g)$, la divisione è già fatta! Basta scegliere $q(x) = 0$ e $r(x) = f(x)$. La condizione $\text{gr}(r) < \text{gr}(g)$ è soddisfatta.
2. **Passo Induttivo:** Assumiamo che il teorema sia vero per tutti i polinomi con grado minore di $n = \text{gr}(f)$. Vogliamo dimostrarlo per $f(x)$.
   - Siano $f(x) = a_n x^n + \dots$ e $g(x) = b_m x^m + \dots$, con $n \geq m$.
   - Sia b_m il coefficiente direttore di $g(x)$. Per ipotesi, b_m è invertibile e il suo inverso è b_m^{-1}.
   - **Costruiamo un nuovo polinomio** $\tilde{f}(x)$ per "abbassare il grado" di $f(x)$:

$$\tilde{f}(x) = f(x) - (a_n b_m^{-1} x^{n-m}) \cdot g(x)$$

   - **Analizziamo il termine di grado n:** Il termine di grado n di $(a_n b_m^{-1} x^{n-m}) \cdot g(x)$ è $(a_n b_m^{-1} x^{n-m}) \cdot (b_m x^m) = a_n x^n$.
   - Quando sottraiamo questo da $f(x)$, il termine $a_n x^n$ si cancella! Quindi, $\text{gr}(\tilde{f}) < n$.
   - **Applichiamo l'ipotesi induttiva:** Poiché $\tilde{f}(x)$ ha grado minore di n, esistono $\tilde{q}(x)$ e $\tilde{r}(x)$ tali che:

$$\tilde{f}(x) = g(x) \cdot \tilde{q}(x) + \tilde{r}(x) \quad \text{con } \text{gr}(\tilde{r}) < \text{gr}(g)$$

   - **Sostituiamo e risolviamo per f(x):**

$$f(x) - (a_n b_m^{-1} x^{n-m}) \cdot g(x) = g(x) \cdot \tilde{q}(x) + \tilde{r}(x)$$
$$f(x) = g(x) \cdot \tilde{q}(x) + (a_n b_m^{-1} x^{n-m}) \cdot g(x) + \tilde{r}(x)$$
$$f(x) = g(x) \cdot \underbrace{[\tilde{q}(x) + a_n b_m^{-1} x^{n-m}]}_{q(x)} + \underbrace{\tilde{r}(x)}_{r(x)}$$

   - Abbiamo trovato il nostro quoziente $q(x)$ e il nostro resto $r(x)$, e il resto ha il grado giusto. L'esistenza è provata.

Esempio di Divisione

Dividiamo $f(x) = 2x^3 + 7x^2 - 5x + 3$ per $g(x) = x - 1$ in $\mathbb{Q}[x]$.

```
       2x^2 + 9x + 4   <-- q(x)
     ________________
x-1 | 2x^3 + 7x^2 - 5x + 3
    -(2x^3 - 2x^2)
    ________________
          9x^2 - 5x
         -(9x^2 - 9x)
         ___________
                4x + 3
               -(4x - 4)
               ________
                     7   <-- r(x)
```

Quindi, $q(x) = 2x^2 + 9x + 4$ e $r(x) = 7$.

Radici di un Polinomio e Teorema di Ruffini

#tag/teorema #tag/radici

Funzione Polinomiale e Radici

Ad ogni polinomio formale $f(x) \in A[x]$ possiamo associare una **funzione polinomiale** $\tilde{f} : A \to A$ che calcola il valore del polinomio per ogni elemento $c \in A$.

$$\tilde{f}(c) = a_0 + a_1 c + a_2 c^2 + \dots + a_n c^n$$

Definizione: Radice (o Zero)

Un elemento $c \in A$ è una **radice** (o **zero**) del polinomio $f(x)$ se $\tilde{f}(c) = 0$.

Lemma del Resto (DIM)

Lemma del Resto

Il resto della divisione di un polinomio $f(x)$ per un binomio $(x-c)$ è uguale al valore che il polinomio assume in c, cioè $\tilde{f}(c)$.

$$\text{rest}(f(x), x-c) = \tilde{f}(c)$$

Dimostrazione

1. Dal teorema della divisione, dividendo $f(x)$ per $(x-c)$, otteniamo:

$$f(x) = (x-c) \cdot q(x) + r(x)$$

2. Il divisore $(x-c)$ ha grado 1. Quindi il resto $r(x)$ deve avere grado minore di 1, cioè grado 0 o $-\infty$. In ogni caso, $r(x)$ è un polinomio costante. Chiamiamolo r_0.

$$f(x) = (x-c) \cdot q(x) + r_0$$

3. Valutiamo entrambi i lati dell'equazione in c:

$$\tilde{f}(c) = (c-c) \cdot \tilde{q}(c) + r_0$$

$$\tilde{f}(c) = 0 \cdot \tilde{q}(c) + r_0$$

$$\tilde{f}(c) = r_0$$

Il resto è proprio $\tilde{f}(c)$. **Q.E.D.**

Teorema di Ruffini (DIM)

Teorema di Ruffini

Un elemento $c \in A$ è una radice di $f(x)$ se e solo se il polinomio $(x-c)$ divide $f(x)$.

$$\tilde{f}(c) = 0 \iff (x-c) \mid f(x)$$

Dimostrazione

È una conseguenza diretta del Lemma del Resto.

- ($\Rightarrow$) **Se c è una radice**, allora $\tilde{f}(c) = 0$. Per il Lemma del Resto, il resto della divisione per $(x-c)$ è 0. Se il resto è zero, significa che $(x-c)$ divide $f(x)$.
- ($\Leftarrow$) **Se $(x-c)$ divide $f(x)$**, allora il resto della divisione è 0. Per il Lemma del Resto, $\tilde{f}(c)$ è uguale al resto, quindi $\tilde{f}(c) = 0$. Questo significa che c è una radice. **Q.E.D.**

Teorema di Ruffini Generalizzato

Teorema di Ruffini Generalizzato

Se A è un **dominio di integrità** e $c_1, c_2, \ldots, c_k$ sono k radici **distinte** di $f(x)$, allora il prodotto $(x-c_1)(x-c_2)\ldots(x-c_k)$ divide $f(x)$.

Polinomi e Funzioni Polinomiali

#tag/funzioni

Se due polinomi generano la stessa funzione, sono per forza lo stesso polinomio?

La risposta, sorprendentemente, è... **dipende dall'anello A!**

Teorema: Identità dei Polinomi (DIM)

Teorema sull'Identità dei Polinomi

Siano $f(x), g(x) \in A[x]$ dove $(A, +, \cdot)$ è un **campo**.

1. Se A è un **campo infinito** (come $\mathbb{Q}, \mathbb{R}, \mathbb{C}$), allora:

$$\tilde{f} = \tilde{g} \iff f = g$$

(Due polinomi sono uguali se e solo se generano la stessa funzione).

2. Se A è un **campo finito** con $|A| = m$ elementi, allora $\tilde{f} = \tilde{g}$ se e solo se il polinomio $x^m - x$ divide la loro differenza $f(x) - g(x)$.

Dimostrazione (idea chiave)

- **Caso Infinito:** Se $\tilde{f} = \tilde{g}$, allora il polinomio differenza $h(x) = f(x) - g(x)$ ha la proprietà che $\tilde{h}(c) = 0$ per ogni $c \in A$. Ma un polinomio non nullo può avere solo un numero finito di radici (al massimo il suo grado). Poiché A è infinito, l'unico modo per avere infinite radici è che il polinomio $h(x)$ sia il polinomio nullo. Se $h(x) = 0$, allora $f(x) = g(x)$.
- **Caso Finito:** Se $\tilde{f} = \tilde{g}$, allora il polinomio differenza $h(x) = f(x) - g(x)$ ha come radici tutti gli m elementi del campo A. Per il Teorema di Ruffini Generalizzato, il prodotto $(x - c_1)\dots(x - c_m)$ deve dividere $h(x)$. Si può dimostrare che questo prodotto è esattamente il "polinomio fondamentale" $x^m - x$.

Esempio in un Campo Finito

In $\mathbb{Z}_3[x]$, consideriamo $f(x) = x^3 + 1$ e $g(x) = x + 1$.

- $f \neq g$ come polinomi formali.
- Valutiamo le funzioni $\tilde{f}$ e $\tilde{g}$:
  $\tilde{f}(\bar{0}) = \bar{0}^3 + \bar{1} = \bar{1}$
  $\tilde{f}(\bar{1}) = \bar{1}^3 + \bar{1} = \bar{2}$
  $\tilde{f}(\bar{2}) = \bar{2}^3 + \bar{1} = \bar{8} + \bar{1} = \bar{9} = \bar{0}$
  $\tilde{g}(\bar{0}) = \bar{0} + \bar{1} = \bar{1}$
  $\tilde{g}(\bar{1}) = \bar{1} + \bar{1} = \bar{2}$
  $\tilde{g}(\bar{2}) = \bar{2} + \bar{1} = \bar{3} = \bar{0}$
  Le funzioni non sono uguali! C'è un errore negli appunti originali. Vediamo un esempio che funziona: $f(x) = x^3$ e $g(x) = x$ in $\mathbb{Z}_3$.
- $\tilde{f}(\bar{0}) = \bar{0}, \tilde{f}(\bar{1}) = \bar{1}, \tilde{f}(\bar{2}) = \bar{8} = \bar{2}$.
- $\tilde{g}(\bar{0}) = \bar{0}, \tilde{g}(\bar{1}) = \bar{1}, \tilde{g}(\bar{2}) = \bar{2}$.
  In questo caso $\tilde{f} = \tilde{g}$ ma $f \neq g$. La loro differenza è $h(x) = x^3 - x$, che è esattamente il polinomio fondamentale di $\mathbb{Z}_3$.

Divisibilità e Irriducibilità

Questi concetti sono l'analogo dei numeri primi per i polinomi.

Definizione: Polinomio Irriducibile

Un polinomio non costante $f(x) \in A[x]$ si dice **irriducibile** su A se non può essere scritto come prodotto di due polinomi non costanti di grado inferiore.
Formalmente, se $f(x) = g(x) \cdot h(x)$, allora o $g(x)$ o $h(x)$ deve essere un'unità (cioè un polinomio costante invertibile).

Spiegazione Semplice: Un polinomio è irriducibile se non puoi "spezzarlo" in polinomi più semplici. È un "atomo" polinomiale. Se è possibile spezzarlo, si dice **riducibile**.

Irriducibilità e Radici

Se un polinomio $f(x)$ di grado 2 o 3 **ha una radice** in un campo A, allora è **riducibile** su A.
Perché? Se c è una radice, per Ruffini $(x - c)$ divide $f(x)$. Quindi $f(x) = (x - c) \cdot q(x)$. Poiché $\text{gr}(f) > 1$, anche $q(x)$ non sarà costante. Abbiamo spezzato $f(x)$!

Attenzione!

Il viceversa non è sempre vero! Un polinomio può essere riducibile anche senza avere radici.
Esempio: $f(x) = (x^2 + 1)^2$ in $\mathbb{R}[x]$ non ha radici reali, ma è chiaramente riducibile.

Proposizione: Irriducibilità per gradi 2 e 3 (DIM)

Proposizione

Sia A un **campo** e $f(x) \in A[x]$ un polinomio di grado 2 o 3. Allora:

$$f(x) \text{ è irriducibile} \iff f(x) \text{ non ha radici in } A$$

Dimostrazione

- ($\Rightarrow$) **Se f è irriducibile, allora non ha radici.**
  Lo dimostriamo per assurdo. Supponiamo che f abbia una radice $c \in A$. Allora per il Teorema di Ruffini, $(x - c)$ divide $f(x)$. Possiamo scrivere $f(x) = (x - c) \cdot q(x)$.
  Poiché $\text{gr}(f) \geq 2$ e $\text{gr}(x - c) = 1$, il quoziente $q(x)$ deve avere grado $\text{gr}(f) - 1 \geq 1$.
  Quindi, abbiamo scritto $f(x)$ come prodotto di due polinomi non costanti, il che contraddice l'ipotesi che f sia irriducibile. Assurdo. Dunque f non può avere radici.
- ($\Leftarrow$) **Se f non ha radici, allora è irriducibile.**
  Lo dimostriamo per assurdo. Supponiamo che f sia riducibile. Allora possiamo scrivere $f(x) = g(x) \cdot h(x)$, dove g e h

non sono costanti.
Poiché A è un campo, $\text{gr}(f) = \text{gr}(g) + \text{gr}(h)$.
Dato che $\text{gr}(f)$ è 2 o 3, e $\text{gr}(g), \text{gr}(h) \geq 1$, uno dei due fattori (diciamo $g(x)$) deve avere per forza **grado 1**.
Un polinomio di grado 1 su un campo ha sempre una radice. Se $g(x) = ax + b$ con $a \neq 0$, la sua radice è $c = -ba^{-1}$.
Ma se c è una radice di $g(x)$, allora $\tilde{g}(c) = 0$, e quindi $\tilde{f}(c) = \tilde{g}(c) \cdot \tilde{h}(c) = 0 \cdot \tilde{h}(c) = 0$.
Questo significa che $f(x)$ ha una radice c, il che contraddice l'ipotesi. Assurdo. Dunque f deve essere irriducibile.
Q.E.D.

Teorema di Fattorizzazione Unica

Questo è uno dei risultati più importanti, l'equivalente del Teorema Fondamentale dell'Aritmetica per i polinomi.

Teorema Fondamentale dell'Aritmetica (per confronto)

Ogni intero $a \in \mathbb{Z} \setminus \{0, 1, -1\}$ è un numero primo oppure può essere scritto in modo **unico** (a meno dell'ordine e di fattori ± 1) come prodotto di numeri primi.

Teorema di Fattorizzazione Unica per Polinomi (DIM)

Teorema di Fattorizzazione Unica

Sia A un **campo**. Ogni polinomio non costante $f(x) \in A[x]$ è irriducibile oppure può essere scritto in modo **unico** (a meno dell'ordine e di fattori associati) come prodotto di polinomi irriducibili.

Dimostrazione (Cenno)

La dimostrazione è molto simile a quella per i numeri interi e si basa su due pilastri:

1. **Esistenza:** Si dimostra per induzione sul grado del polinomio.
   - **Caso Base:** Se $f(x)$ è irriducibile, abbiamo finito.
   - **Passo Induttivo:** Se $f(x)$ è riducibile, lo spezziamo in $f(x) = g(x)h(x)$. I gradi di g e h sono minori di quello di f. Per ipotesi induttiva, g e h si possono fattorizzare in irriducibili. Mettendo insieme le loro fattorizzazioni, otteniamo quella di f.
2. **Unicità:** Si basa su un risultato analogo al Lemma di Euclide: se un polinomio irriducibile $p(x)$ divide un prodotto $g(x)h(x)$, allora deve dividere o $g(x)$ o $h(x)$. Usando questa proprietà, si mostra che due fattorizzazioni diverse devono in realtà contenere gli stessi "atomi" irriducibili.

Punti Chiave della Lezione

Riepilogo Super-Sintetico

- I **polinomi** formano un anello $A[x]$ con le operazioni di somma e prodotto.
- Il **grado** è l'esponente più alto. Se i coefficienti sono in un **dominio di integrità**, il grado del prodotto è la somma dei gradi.
- La **divisione con resto** è possibile se il coefficiente direttore del divisore è un'unità.
- **Teorema di Ruffini:** c è una **radice** di $f(x)$ se e solo se $(x - c)$ divide $f(x)$.
- Un polinomio è **irriducibile** se non può essere spezzato in fattori più semplici (non costanti).
- **Fattorizzazione Unica:** Se i coefficienti sono in un **campo**, ogni polinomio si scompone in modo unico in un prodotto di irriducibili (come i numeri si scompongono in primi).

Domande per la Riflessione

Mettiti alla Prova!

1. Perché è così importante che l'anello dei coefficienti A sia un dominio di integrità per il teorema dei gradi? Cosa "si rompe" se non lo è?
2. Prendi il polinomio $f(x) = x^2 + 1$. È irriducibile su $\mathbb{R}[x]$? E su $\mathbb{C}[x]$? (Suggerimento: cerca le radici!)
3. Sai spiegare a parole tue la differenza tra un polinomio *formale* $f(x)$ e la sua *funzione* associata $\tilde{f}$? Perché questa distinzione è importante nei campi finiti?