Algebra e Matematica di Base

Corso di Laurea in Informatica - Università degli Studi di Verona

Federico Brutti

Federico Brutti
federico.brutti@studenti.univr.it

Indice

16 | Strutture Algebriche

Sto scrivendo questo testo a causa della burocrazia

Insiemi

Onestamente non ho la benché minima idea di cosa tratti matematica di base; tutti gli argomenti sembrano familiari ma allo stesso tempo estranei. Inoltre sembra una materia di cui si sente la mancanza nell'ordinamento precedente. Iniziamo con la definizione formale di **Insieme**, elemento della teoria su cui si basa la matematica tutta:

> **Definizione 1.1. Insieme**
> Gruppo di elementi aventi una stessa proprietà. Si indica con una lettera maiuscola.

Pare ovvio che con questi insiemi sia possibile operare in qualche modo; per prima cosa elenchiamo i simboli utilizzati nel corso:
Connettivi:

- **Congiunzione**: $\wedge$

  Ritorna vero solo se tutti gli elementi sono veri.

- **Disgiunzione**: $\vee$

  Ritorna vero se almeno un elemento è vero.

- **Negazione**: $\neg$

  Rende falso il vero e viceversa.

- **Implicazione**: $\implies$

  Corrisponde a "Se, allora", ritorna vero nei casi $0 \to 1$ oppure $1 \to 1$, mentre è falso se $1 \to 0$ oppure $0 \to 0$.

- **Doppia Implicazione**: $\iff$

  Corrisponde a "se e solo se, allora" e viene rappresentata mediante due implicazioni: $(\phi \to \psi) \wedge (\psi \to \phi)$.

- **Bottom**: $\bot$

  Indica il valore di assurdo, 0.

- **Top**: $\top$

  Indica il valore di verità, 1.

Quantificatori:

- **Esiste**: $\exists$

  Indica l'esistenza di un elemento con una determinata proprietà. Normalmente si usa legato ad una proprietà di un elemento, quindi per dimostrarlo serve quest'ultimo e la prova di tale proprietà.

- **Per ogni**: $\forall$

  Indica che per ogni caso considerato, esiste un elemento con una data proprietà. Per dimostrarlo serve supporre un elemento e trovare una prova della proprietà ad esso associata.

Dai connettivi e i quantificatori abbiamo anche i seguenti assiomi logici:

- **Tautologie**

  Formule che risultano vere in ogni istanza presa in esame. Un esempio di tautologia sono le leggi di De Morgan, fondamentali per l'insiemistica.

  > **Esempio. Tautologia**
  >
  > – **Semplice**:
  > Data una formula P abbiamo che $P \implies P$ è sempre vera, quindi una tautologia. Per dimostrarla troviamo una prova di P e hai fatto.
  >
  > – **Modus Ponens**:
  > Se P, Q sono due formule, allora $(P \implies Q) \implies (\neg Q \implies \neg P)$ è tautologia. Per dimostrarla è necessario trovare le prove di ambo le ipotesi, dopodiché supponi le prove per $[\neg P := (P \implies \bot)]$ e $[\neg Q := (Q \implies \bot)]$.
> Supponi ora P. Da $P \implies Q$ traiamo Q, dalla quale possiamo trarre $Q \implies \bot$, quindi $\bot$. La formula quindi vale perché dall'assurdo si può derivare qualunque cosa.

- **Principio del terzo escluso**:

  Data la formula $(P \vee \neg P)$, non c'è nessun altro elemento fra $P \wedge \neg P$ o $P \vee \neg P$.

- **Eliminazione della doppia negazione**:

  Dall'assurdo possiamo derivare qualunque cosa, di conseguenza possiamo derivare una formula P da $\bot$.

  > **Esempio.** $\neg\neg P \implies P := \neg P \implies \bot := (P \implies \bot) \implies \bot$.

Ed ora introduciamo tutte le varie operazioni insieme alle loro proprietà.

1.1 Operazioni fra gli insiemi

Distinguiamo inizialmente i due casi in cui è possibile operare con gli insiemi:

- **Coppie**, collezioni di oggetti dove è possibile distinguere il primo elemento dal secondo. Si distinguono in:

  – **Ordinate**: $(A, B) = \{\{x\}, \{x, y\}\}$
  Insieme dove gli elementi sono legati da una determinata relazione di ordinamento.

  - **Non ordinate**: $(A, B) = (B, A)$
    Gli insiemi di questo tipo saranno sempre uguali se contengono gli stessi identici elementi, a prescindere dall'ordine in cui sono scritti.

- **N-uple**, dove sono presenti più di due insiemi, trattato più avanti.

Ed ora possiamo iniziare con le operazioni effettive:

- **Appartenenza, contenimento e sottoinsieme**

  Diciamo che un elemento x appartiene ad un insieme A quando rispetta i criteri per farne parte, come avere una determinata proprietà o caratteristica.

  Definizione 1.2. Appartenenza e non appartenenza

  Data una proprietà P requisito per far parte dell'insieme A, definiamo formalmente:

  - **Appartenenza**: $x \in A$, $A = \{x | P(x)\}$
    All'insieme A appartiene l'elemento x tale che x abbia una data proprietà P.
  - **Non appartenenza**: $y \notin A$
    All'insieme A non appartiene y.

  Diremo poi che un insieme B è sottoinsieme di A quando il primo è interamente contenuto nel secondo. Ciò non necessariamente significa che sia uguale, tuttavia.

  Definizione 1.3. Sottoinsiemi

  Dati due insiemi A e B diremo che B possiamo avere i seguenti casi:

  - **Sottoinsieme Improprio**: $B \subseteq A \iff \forall x.(x \in A \implies x \in B)$
    Quando ogni elemento appartiene a B, appartiene anche ad A.
  - **Uguaglianza**: $A = B \iff \forall x.(x \in A \iff x \in B)$
    Quando due insiemi sono perfettamente uguali.
  - **Sottoinsieme Proprio**: $B \subset A$
    Quando tutti gli elementi di B appartengono ad A e $A \neq B$.

  Abbiamo infine l'elemento neutro, detto **Insieme Vuoto**, scritto con $A = \emptyset$, il quale indica un insieme privo di elementi.

- **Unione**

  L'unione fra due insiemi risulta come un terzo insieme contenente gli elementi di entrambi. Formalmente:

  Definizione 1.4. Unione $A \cup B = \{a | a \in A \vee a \in B\} = C$

  Unisce gli elementi di A a quelli di B per creare un nuovo insieme C che contiene tutti gli elementi dei primi due senza ripetizioni. Detiene inoltre le seguenti proprietà:

  - $A \cup \emptyset = \emptyset$

- $(A \cup B) = (B \cup A)$
- $(A \cup B \cup C) = (A \cup B) \cup C$
- $A \cup A$
- $A \subseteq C \land B \subseteq C = A \cup B \subseteq C$
- $A \subseteq C \iff A \cup Z = C$

- **Intersezione**

  L'intersezione prende solamente gli elementi comuni ad A e B.

Definizione 1.5. Intersezione $A \cap B = \{x | x \in A \land x \in B\}$

Dati due insiemi A, B, crea un insieme C che contiene esclusivamente gli elementi comuni ai primi due. Detiene le seguenti proprietà:

- $A \cap \emptyset = \emptyset$
- $A \cap B = B \cap A$
- $A \cap (B \cap C) = (A \cap C) \cap C$
- $A \cap A = A$
- $C \subseteq A \land C \subseteq B \implies C \subseteq A \cap B$
- $A \subseteq B \iff A \cap B = A$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

- **Prodotto cartesiano**

  Il Prodotto Cartesiano è una relazione fra due insiemi dove a partire dagli elementi di A, crea tutte le coppie possibili con gli elementi di B. Giuro è più semplice a vederlo.

Definizione 1.6. Prodotto Cartesiano $A \times B = \{(x, y) | x \in A \land y \in B\}$

Dati due insiemi A, B, si definisce il loro prodotto cartesiano l'insieme di tutte le coppie ordinate di elementi, indicati da (a, b), tali che il primo elemento a della coppia appartenga all'insieme A e il secondo elemento b della coppia appartenga all'insieme B.

Esempio. Calcolo di un prodotto cartesiano

Non è molto dissimile da un prodotto di polinomi; moltiplichi ogni elemento di A per ogni elemento di B, come segue:

$$A = 1, 2,\ B = 3, 4$$
$$A \times B = C = (1, 3), (1, 4), (2, 3), (2, 4)$$

- **Differenza**

  La differenza fra insiemi sottrae gli elementi di B a quelli di A.

Definizione 1.7. Differenza $A \setminus B = \{x | x \in A \wedge x \notin B\}$

Dati due insiemi A, B, l'operazione differenza sottrae tutti gli elementi di B a quelli di A. Nel caso in cui gli insiemi non abbiano elementi in comune, l'operazione non avrà effetto. Detiene le seguenti proprietà:

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

Un'altra operazione molto utile sempre in questo senso è la **Differenza Simmetrica**, la quale permette di ricavare esclusivamente gli elementi unici da due insiemi.

Definizione 1.8. Differenza Simmetrica $A \triangle B = (A \setminus B) \cup (B \setminus A)$

Dati due insiemi A, B, la differenza simmetrica effettua un'unione fra la differenza $A \setminus B$ e $B \setminus A$, con lo scopo di ottenere Tutti gli elementi appartenenti ai due insiemi che non sono ripetuti. Detiene le seguenti proprietà:

- $A \triangle B = (A \cup B) \setminus (A \cap B)$
- $A \triangle B = B \triangle A$
- $(A \triangle B) \triangle C = A \triangle (B \triangle C)$
- $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$
- $A \triangle \emptyset = A$
- $A \triangle A = \emptyset$
- $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$

- **Famiglie di insiemi**

Definizione 1.9. Famiglie di insiemi - $\chi := \{X_i | i \in I\}$

Se ad ogni elemento i di un insieme non vuoto I corrisponde un insieme $X_i, i \to X_i$, allora l'insieme di insiemi X_i è chiamato **famiglia di insiemi** ed I è il suo insieme di indicizzazione.

INSERISCI ESEMPIO

- **Insieme delle parti**

Definizione 1.10. Insieme delle parti - $P(X) := \{A | A \subseteq X\}$

Definiamo l'insieme delle parti $P(X)$ l'insieme di tutti i sottoinsiemi di X.

INSERIRE ESEMPIO

- **Insieme complementare**
- **Insieme Potenza**
  INFORMATI IN MERITO
- **Generalizzazione di operazioni**
  INFORMATI IN MERITO

1.1.1 Leggi di De Morgan

1.2 Relazioni fra insiemi

Ci è possibile mettere in relazione gli elementi di due o più insiemi diversi[1]. Diciamo infatti che se $x \in X$ e $y \in Y$, i due elementi sono in relazione se la loro coppia (x, y) è in una relazione R, intesa come sottoinsieme R di $X \times Y$. A partire da questo possiamo definire le seguenti relazioni notevoli:

- **Corrispondenze**
- **Relazione inversa**
- **Composizione delle operazioni**
- **Relazione chiusa**

1.3 Principi di dimostrazione

Il processo di dimostrazione matematica è un algoritmo deduttivo utilizzato per provare la verità di ipotesi arbitrarie basandosi sul ragionamento logico. Esistono più metodi per arrivare ad una stessa soluzione:

- **Dimostrazione per assurdo**

  Partiamo dal presupposto che la tesi sia falsa. Se si riesce a concludere il processo senza incappare in contraddizioni si è dimostrato che la tesi è falsa, altrimenti è vera.

  > **Esempio. Dimostrazione per assurdo**
  > INSERISCI ESEMPIO.

- **Dimostrazione per induzione**

  Algoritmo basato sul passaggio dallo specifico al generale, si compone di due passi:

  1. Passo base, dove si prende un valore comodo per provare la veridicità della tesi nel caso più facile.
  2. Passo induttivo, dove si prova, basandosi sul caso base, che valga anche per tutte le istanze successive.

[1] Il totale degli insiemi nella relazione è dato dall'arietà. Se è unaria, sarà per un insieme, se binaria per due e così via.

Esempio. Dimostrazione per induzione su $\mathbb{N}$

INSERISCI ESEMPIO

Esempio. Dimostrazione per induzione su $\mathbb{N}^*$

Definiamo l'insieme numerico di lavoro come $\mathbb{N}^* = \mathbb{N} \setminus \{0\} = \{1, 2, ..., n\}$

Tesi da provare: $\theta(n) = \forall n \in \mathbb{N}^*.(1 + 2 + ... + n = \frac{n(n+1)}{2})$

- **Passo base**:
  Testiamo se la tesi vale sostituendo n a 1

  $$\theta(1) \iff 1 = \frac{1(1+1)}{2} = 1, \text{ che è vera.}$$

- **Passo induttivo**:
  Espandiamo il ragionamento per $\theta(n+1)$. Va sostituito $(n+1)$ alla singola n presente nella tesi iniziale.

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

  Adesso proviamo che il risultato ottenuto è valido:

  $$\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)+2(n+1)}{2} = \frac{n^2+3n+2}{2} = \frac{(n+1)(n+2)}{2}$$

Come volevasi dimostrare.

- **Dimostrazione per ricorsione**

  La ricorsione si costituisce anch'essa di due casi, ovvero il caso base, da dove inizia tutto, ed il caso ricorsivo, che avanza tenendo conto dei valori precedentemente ottenuti.

Esempio. Dimostrazione per ricorsione

Definiamo la funzione $n!$:

- Passo base
  Se $n = 0 \implies 1$
- Passo ricorsivo
  Se $n > 0 \implies (n-1)! \times n$

Proviamo a ragionare come si comporta tale funzione quando sostituiamo alla n i valori presi in esame. Otterremo che:

$$0! = (0-1)! \times 1 = 1$$
$$1! = (1-1)! \times 1 = 1 \times 1 = 1$$
$$2! = (2-1)! \times 2 = 1 \times 2 = 2$$
$$3! = (3-2)! \times 3 = 2 \times 3 = 6$$

$$4! = (4-3)! \times 4 = 6 \times 4 = 24$$

1.4 Domande di teoria

Teorema 1.11. Here goes a theorem.

Dimostrazione. Here goes the proof □

Corollario 1.12. Here goes a collorary

Esempio. Here goes an example

Nota. Here goes a note

Lemma 1.13. Here goes a lemma

Proposizione 1.14. Here goes a proposition

Definizione 1.15. Here goes a definition

1.4.1 Esercizi

Relazioni e Funzioni

2.1 Tipi di funzioni

Definizione, immagine, immagine inversa

- Funzioni totali
- Funzioni parziali
- Iniettive
- Suriettive
- Biunivoche
- Funzioni composte
- Funzione inversa
- Cancellabilità della funzione

2.2 Relazioni di equivalenza

Equivalenza, transitività, simmetria/antisimmetria, monotonia, proiezione simmetrica, assiomi di peano.

2.3 Partizioni

2.4 Relazioni di ordinamento

2.5 Domande di teoria

2.6 Esercizi

Numeri Naturali

3.1 Definizioni per ricorsione primitiva

3.2 Principali operazioni

Addizione in N, funzione successiva, proprietà commutativa, ordinamento in N, proprietà associativa.

3.3 Costruzione di interi e razionali

3.4 Fattorizzazione e teorema fondamentale dell'aritmetica

3.5 Congruenze

3.6 Domande di teoria

3.7 Esercizi

Cardinalità

Strutture Algebriche

5.1 Monodi

5.2 Gruppi

5.3 Anelli

5.4 Reticoli

5.5 Domande di teoria

5.6 Esercizi