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

23 | 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**: $\perp$

  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:
  > - $A \cup \emptyset = \emptyset$

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

- **Intersezione**

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

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

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

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

- **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 $A \times B = \{(x, y)|x \in A \wedge y \in B\}$

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

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 $X \times Y$. Segue definizione formale:

Definizione 1.11. Corrispondenza
Una corrispondenza dell'insieme X nell'insieme Y è un qualunque insieme $R.R \subseteq X \times Y$. Se la coppia $(x, y) \in R$ si dice che x corrisponde a y nella corrispondenza R. Si scrive anche

$$xRy :\iff (x, y) \in R$$

A partire da questo possiamo trovare i seguenti casi:

- Un elemento di X può corrispondere a più elementi di Y e viceversa.
- Un elemento di X può corrispondere a più elementi di Y, i quali a loro volta corrispondono ad altri elementi di X.
- Relazione vuota, dove in X non ci sono elementi che corrispondono agli elementi di Y.

Esempio. INSERISCI ESEMPIO DI RELAZIONE

Ed ora possiamo definire questi altri casi notevoli

- **Relazione inversa**

  Definizione 1.12. Relazione inversa - $R^{-1} \subseteq Y \times X$
  La relazione inversa sussiste solamente se abbiamo la certezza che esista la coppia $(x, y) \in R$. La definiamo formalmente come:

  $$R^{-1} := \{(y, x) \in Y \times X.(y, x) \in R\}$$

  INSERISCI ESEMPIO

- **Composizione delle operazioni**

  Ti ricorderai il problema delle funzioni composte; è esattamente la stessa cosa: più funzioni messe insieme.

  Definizione 1.13. Composizione delle operazioni
  Se $R \subseteq X \times Y \wedge S \subseteq Y \times Z$, la loro composizione $S \circ R \subseteq X \times Z$ è definita come segue:

[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.

$$S \circ R := \{(x, z) \in X \times Z. \exists y \in Y.((x, y) \in R \wedge (y, z) \in S)\}$$

INSERISCI ESEMPIO CON LA DIAGONALE.

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.

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

  - **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:

$$\begin{gathered} 0! = (0-1)! \times 1 = 1 \\ 1! = (1-1)! \times 1 = 1 \times 1 = 1 \\ 2! = (2-1)! \times 2 = 1 \times 2 = 2 \\ 3! = (3-2)! \times 3 = 2 \times 3 = 6 \\ 4! = (4-3)! \times 4 = 6 \times 4 = 24 \end{gathered}$$

1.4 Domande di teoria

Teorema 1.14. Here goes a theorem.

Dimostrazione. Here goes the proof □

Corollario 1.15. Here goes a collorary

Esempio. Here goes an example

Nota. Here goes a note

Lemma 1.16. Here goes a lemma

Proposizione 1.17. Here goes a proposition

Definizione 1.18. Here goes a definition

1.4.1 Esercizi

Relazioni e Funzioni

2.1 Tipi di funzioni

Le **funzioni**, o applicazioni, sono le relazioni più importanti fra gli insiemi. Si definiscono formalmente come:

> **Definizione 2.1. Funzione** - $f : X \implies Y$
> Siano due insiemi X, Y. Un'applicazione $f(X)$ in Y è una corrispondenza $f \subseteq X \times Y$ con la seguente proprietà:
> Per ogni elemento $x \in X$, esiste un unico elemento $y \in Y$ tale che $(x, y) \in f$, ovvero che valga quanto segue:
>
> $$\forall x, x' \in X.\{(x = x') \implies (f(x) = f(x'))\}$$
>
> Per indicare l'elemento corrispondente a x scriviamo $f(x) = y$.

Questa definizione porta tutti nuovi concetti come conseguenze logiche. Essendo che stiamo lavorando su insiemi, diciamo di avere una funzione $f : \mathbb{R} \implies \mathbb{R}$, possiamo associare a questa funzione un numero all'interno dell'insieme per ottenere la sua corrispondenza nello stesso.

Fin qua tutto chiaro, ma la presenza di n numeri corrisposti implica l'esistenza di un insieme che li contenga tutti. Questo si chiama **Insieme Immagine**. Andando più nello specifico, possiamo dire che il singolo elemento $f(x)$ è chiamato **immagine** di x sotto f. Inoltre chiameremo l'insieme di partenza X il **Dominio** e quello della corrispondenza Y il **Codominio**.

Per definizione di funzione non è possibile che ad un elemento $f(x)$ corrispondano più elementi nell'insieme Y, tuttavia è possibile che più elementi di X abbiano una stessa immagine. Seguono alcuni casi notevoli:

- **Funzione costante** - $f_{y_0} := \{(x, y_0) | x \in X\}$

  Si tratta di una funzione definita dalla regola $f_{y_0}(x) = y_0$, la quale vale per ogni $x \in X$.

  INSERISCI IMMAGINE.

- **Funzione identità** - $Diag(X) := \{(x, x) | x \in X\}$

  La funzione diagonale o identità, denotata con $id_X(x) = x$ per ogni $x \in X$, restituisce lo stesso valore che le è stato assegnato.

- **Funzione valore assoluto** - $|.| := \{(x, x) | x \; 0\} \cup \{(x, -x) | x < 0\}$

  Definita unicamente su intervalli positivi, possiamo dire che "specchia" ogni valore che si sarebbe trovato negli intervalli negativi. Si definisce con la seguente regola:

  $$|x| = \begin{cases} x & , x \geq 0 \\ -x & , x < 0 \end{cases}$$

INSERIRE IMMAGINE.

- **Funzione quadratica** -
- **Funzione di Dirichlet** -

CONTINUA DA 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 Principio di induzione sui naturali

L'insieme dei numeri naturali $\mathbb{N}$ è il più importante di tutta la matematica e la sua dinamica si basa su due principi:

- Un numero dato, spesso 0, dal quale partire.
- Una funzione successore $Succ(n)$, che permette di ottenere il numero conseguente.

Conosci già gli elementi di $\mathbb{N}$; si tratta di un intervallo che comprende i numeri da $[0, +\infty)$, ne consegue che è possibile dimostrare una proprietà $\phi(n)$ per tutti i numeri naturali usando l'induzione, che in questo caso chiameremo $\text{IND}_{\mathbb{N}}$. Il suo funzionamento non differisce da una classica induzione:

1. Parti da un caso base $\phi(0)$ e provalo vero.
2. Supponi un $n \in \mathbb{N}$ e prova l'ipotesi $\phi(n + 1)$.
3. Concludi che $\forall n \in \mathbb{N}$ vale $\phi(n)$.

Per i nostri scopi useremo inoltre i seguenti assiomi:

Proposizione 3.1. Assiomi di Peano

- $0 \notin \mathbb{N}$, quindi la funzione $Succ(n)$ non è suriettiva.
- $Succ(m) = Succ(m) \implies m = n \forall m, n \in \mathbb{N}$, quindi la funzione $Succ(n)$ è iniettiva.
- Sia $\phi(n)$ una formula sui numeri naturali, allora vale:
  $[\phi(0) \land \forall n \in \mathbb{N}.(\phi(n) \implies \phi(Succ(n))] \implies \forall n \in \mathbb{N}.(\phi(n))$

Proviamo adesso ad effettuare una prima $\text{IND}_{\mathbb{N}}$ dimostrando la validità della seguente formula

Esempio. Dimostrazione per $\text{IND}_{\mathbb{N}}$ della formula $\forall n \in \mathbb{N}.[(1+2024)^n \geq 1+n \times 2024]$
INSERISCI ESEMPIO.

Considera che è possibile operare anche in un insieme dei naturali dove non fa parte lo zero, formalmente definito come $\mathbb{N}^* = \mathbb{N}/\{0\}$. Il procedimento per le dimostrazioni non cambia, semplicemente il passo base sarà con il numero 1.

Abbiamo inoltre un algoritmo equivalente a quanto visto denominato $\text{IND}_{<}$ INSERISCI ESEMPIO.

3.2 Principali operazioni ed elementi

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

3.8 Appunti

Per il principio del minimo MIN, ogni insieme ha un elemento minimo e non è vuoto. Quindi esisterà $\exists n \in N$, dove $n \in A, \forall \alpha \in A.(n <= \alpha)$. Nei precedenti appunti è stata confutata la tesi (Non tutti gli insiemi hanno un minimo) indirettamente.
Un'altra prova per MIN:

$$A \neq \emptyset, \text{ sia } n \in A.$$
$$0 \in A \vee 0 \notin A, \text{ continua ad andare avanti finché non trovi il minimo dell'insieme.}$$

Teorema 3.2. Il principio MIN implica il principio del terzo escluso PEM

Dimostrazione. Sia P una formula, dimostriamo che vale $(P \vee \neg P)$.

$$A_P = \{1\} \cup \{x \in \mathbb{N} | x = 0 \wedge P\}$$
$$1 \in A_P, \text{ quindi } A_P \text{ non è vuoto.}$$

Non essendo un insieme vuoto, avrà per forza un minimo. □

Sia $n = min(A_P)$, abbiamo che $n = 0 \vee \exists m \in \mathbb{N}.(n = succ(m))$. Con questa formula troviamo il minimo per induzione, che chiamiamo P. Dimostriamo quindi che vale $P \vee \neg P$.

$$0 \in A_P \implies P$$
$$\text{Se il minimo è 1, P non è valida, quindi vale } \neg P\text{, quindi:}$$
$$P_A.0 = 0 \implies 0 \in A_P \implies 0 = minA_P. \text{ Hai trovato l'assurdo.}$$

$$\text{Hai provato che vale } P \vee \neg P.$$

- Moltiplicazione in $\mathbb{N}$

Definizione 3.3. $m, n \in N$
Definizione ricorsiva:

- $m0 = 0$
- $m\mathrm{succ}(n) = m * n + m$

Esempio. $2 \times 3 = 2 \times \mathrm{succ}(2) = 2 \times 2 + 2 = 2 \times \mathrm{succ}(1) + 2 = 2 * 1 + 2 + 2 = 2 \times \mathrm{succ}(o) + 2 + 2 = 2 * 0 + 2 + 2 + 2 = 0 + 2 + 2 + 2 = 6.$

Esempio. $1 \times 1 = 1$
$1 * 1 = 1 * \mathrm{succ}(0) = 1 * 0 + 1 = 0 + 1 = 1$

Esempio. $m * 1 = m$
$m * 1 = m * \mathrm{succ}(0) = m * 0 + m = 0 + m = m$

Esempio. $1 * m = m$
$\forall m \in N.(1 * m = m)$
$\phi 0 = 1 * 0 = 0$
$\phi(m) \implies \phi(\mathrm{succ}(m)) \iff 1 * \mathrm{succ}(m) = \mathrm{succ}(m)$
$1 * \mathrm{succ}(m) = 1 * m + 1 = m + 1 = \mathrm{succ}(m)$
$\phi(m) \iff *m = m.$

Esempio. $0 * m = 0$
$\forall m \in N(0 * m = 0)$
$\phi(0) \iff 0 * 0 = 0$ Per definizione
$\phi(\mathrm{succ}(m)) \iff 0 * \mathrm{succ}(m) = 0$
$0 * \mathrm{succ}(m) = 0 * m + 0 = 0 + 0 = 0$

La moltiplicazione è distributiva rispetto all'addizione.

Definizione 3.4. Proprietà distributiva

1. $m(l + n) = m * l + m * n$
2. $m(l * n) = (m * l)n$
3. $m * n = n * m$
4. $m * n = 0 \implies m = 0 \vee n = 0$

Dimostrazione. $\forall m \in N.[\forall n \in N.(m * n = 0 \implies m = 0 \vee n = 0]$
$\phi(0) \iff \forall n \in N.(0 * n = 0 \implies 0 = 0 \vee n = 0$ Vale banalmente per identità
$\phi(n) \implies \phi(succ(n)), \phi(succ(n)) \iff \forall n \in N.(succ(n) * n = 0 \implies succ(m) = 0 \vee n = 0$

$\theta(n) \iff succ(m) * n = 0 \implies succ(m) = 0 \vee n = 0)$
$\theta(0) \iff succ(m) * 0 = 0 \implies succ(m) = 0 \vee 0 = 0$ vale banalmente per identità.
$\theta(n) \implies \theta(succ(n)), \theta(succ(n)) \iff succ(n = 0 \implies succ(m = 0 \vee succ(n) = 0$
$succ(m) * succ(n) = 0 \iff succ(m) * n + succ(m) = 0 \implies succ(m) * n = 0 \wedge succ(m) = 0$ Questa è falsa per peano 1. Il successore di 0 è 1.
La formula è dimostrata per il funzionamento del connettivo implica 0->1. □

Esempio. Dimostrare $m < n$, tenendo conto della definizione ricorsiva della moltiplicazione.

$m < n \implies m * l < n * l$, dove $l >= 1$
$m < n \iff \exists k \in N^*(n = m + k), k >= 1$

Per ricorsione:
$n = m + k, k <= 1$
$m * l < n * l$
$n * l = (m + k)l = m * l + k * l, k * l >= 1$
$k >= 1, l >= 1, k * l >= 1$
$k = 1 + \sigma$, $l = 1 + \sigma'$
$k * l = (1 + \sigma)(1 + \sigma') = 1 + \sigma' + \sigma + \sigma * \sigma' >= 1$

Per induzione:
$\forall l \in N^*[(m * l < n * l)]$, $m, n.m < n$, $\phi(l) = []$
$\phi(1) \iff m * l < n * l \iff m < n$ vale
$\phi(l) \implies \phi(succ(l))$
$\phi(succ(l)) \iff m * succ(l) < n * succ(l)$
$m * succ(l) = m * l + m$
$n * succ(l) = n * l + n$
$m * l < n * l = m < n$

Esempio. Dimostrare che $m <= m * n, n >= 1$
$m <= n \iff \exists k \in N.(n = m + k), k >= 0$

Per m fissato:
$\forall n \in N^*.[(m <= m * n)], \theta(n) = []$
$\theta(1) \iff m <= m * 1 = m$ vale
$\theta(n) \implies \theta(succ(n)) \iff m <= m * succ(n) \iff m <= m(n + 1) = m * n + m$
$\theta(n) \iff m <= m * n <= m * n + n = n * succ(m)$

Per ogni numero naturale definiamo:

Definizione 3.5. Potenza

- $m^0 = 1$
- $m^{succ(n)} := m^n * m$

$2^3 = 2^{succ(2)} = 2^2*2 = 2^{succ(1)}*2 = 2^1*2*2 = 2^{succ(0)}*2*2 = 2^0*2*2*2 = 1*2*2*2 = 8.$

- Costruzione dei numeri interi

Come definire gli interi? $\mathbb{N} \cup \{0\} \cup \mathbb{N}$

$N^* tilde N_*, N^* \cap N_* = void.$

Esempio. Proviamo a rappresentare -1 con i numeri naturali. Ne serviranno due:

$$\begin{aligned} -1 &= 0 - 1 \\ &= 1 - 2 \text{ e così via.} \end{aligned}$$

Puoi provare a farlo anche con 0, 1, 2 e altri. Questo per dire che tutti i numeri si possono rappresentare mediante una relazione di sottrazione. Ci consente di rendere due coppie scritte in modo diverso uguali grazie alla definizione di funzione.

Supponiamo le coppie $(m, n) tilde (m', n')$, le quali devono essere appunto equivalenti, avremo di conseguenza che $m - n = m' - n'$. Possiamo spostare i termini coi criteri di equivalenza, varrà quindi: $m + n' = m' + n$.

Proposizione 3.6. tilde è un'equivalenza su NxN.

Dimostrazione. Equivalenza
$(m, n) tilde (m, n) \iff m + n = m + n$. La relazione è riflessiva.
$(m, n) tilde (m', n') \implies (m', n') tilde (m, n) \implies m+n' = m'+n \implies m'+n = m+n'$. La relazione è simmetrica.
$(m, n) tilde (m', n') \iff m+n' = m'+n!(m', n') tilde (m'', n'') \iff m'+n'' = m''+n'$
$(m, n) tilde (m'', n'') \iff m + n'' = m'' + n$.
$B = m' + n'' = m'' + n' \implies m' + n'' + n = m'' + n' + n$
Quanto ottenuto fa ottenere $A = m + n' + n'' = m'' + n' + n \iff m + n'' = m'' + n$. La relazione è quindi transitiva.

□

Definizione 3.7. $\mathbb{Z} := \mathbb{N} \times \mathbb{N}/tilde, (m, n) tilde (m', n') \iff m + n' = m' + n$
$Z = \{[(m, n)]_{tilde} | (m, n) \in NxN$
$[(m, n)]_\sim := \{(m', n') \in NxN | (m', n') tilde (m, n)\}$
$0_Z. = [(0, 0)]_{tilde} = [(1, 1)]_{tilde} \iff (0, 0) tilde (1, 1)$
$1_Z := [(1, 0)]_{tilde} = [(2, 1)]_{tilde}, (1, 0) tilde (2, 1)$

Proposizione 3.8. Definiamo $i : N- > Z$ definito da $n|- > i(n) := [(n, 0)]_{tilde}$
La funzione è iniettiva.
$i(n) = i(m) \implies n = m, \forall n, m \in N$
$i(n) = i(m) \iff [(n, 0)]_{tilde} = [(m, 0)]_{\sim} \iff (n, 0) \sim (m, 0) \iff n + 0 = m + 0 \iff n = m$.

Cardinalità

4.1 Insiemi finiti e infiniti

4.2 Equipotenza

4.3 Ordinamento delle cardinalità

4.4 Teorema di Cantor

4.5 Non numerabilità dei reali

4.6 Domande di teoria

4.7 Esercizi

Strutture Algebriche

5.1 Monodi

5.2 Gruppi

5.3 Anelli

5.4 Reticoli

5.5 Domande di teoria

5.6 Esercizi