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

34 | Strutture Algebriche

Per diventare formati ed educati è necessario passare attraverso la sofferenza.

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.

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.

  Definizione 1.2. Tautologia

  – **Semplice**:
  Data una formula P abbiamo che $\mathsf{P} \implies \mathsf{P}$ 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 $(\mathsf{P} \implies \mathsf{Q}) \implies (\neg\mathsf{Q} \implies \neg\mathsf{P})$ è tautologia. Per dimostrarla è necessario trovare le prove di ambo le ipotesi, dopodiché supponi le prove per $[\neg\mathsf{P} := (\mathsf{P} \implies \bot)]$ e $[\neg\mathsf{Q} := (\mathsf{Q} \implies \bot)]$.
  Supponi ora P. Da $\mathsf{P} \implies \mathsf{Q}$ traiamo Q, dalla quale possiamo trarre $\mathsf{Q} \implies \bot$, quindi $\bot$. La formula quindi vale perché dall'assurdo si può derivare qualunque cosa.

- **Principio del terzo escluso** - PEM_P:

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

  Proposizione 1.3. Principio del terzo escluso

  $$(\mathsf{P} \vee \neg\mathsf{P}).$$

- **Eliminazione della doppia negazione** DNE_P:

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

  Proposizione 1.4. Eliminazione della doppia negazione

  $$\neg\neg\mathsf{P} \implies \mathsf{P} := \neg\mathsf{P} \implies \bot := (\mathsf{P} \implies \bot) \implies \bot.$$

Da questi ultimi due assiomi logici traiamo anche le seguenti formule vere, la cui dimostrazione è lasciata per esercizio:

1. $\mathsf{PEM}_\mathsf{P} \implies \mathsf{DNE}_\mathsf{P}$.
2. $\neg\neg\mathsf{P} \implies \mathsf{P}$.
3. $(\neg\mathsf{Q} \implies \neg\mathsf{P}) \implies (\mathsf{P} \implies \mathsf{Q})$.

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 1.5. 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 1.6. 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; è sottoinsieme di tutti gli insiemi, perché di base ogni collezione di elementi contiene il vuoto, il quale verrà riempito con questi ultimi.

- **Unione**

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

  Definizione 1.7. 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:

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

  Con questa operazione ci è possibile generalizzare le coppie non ordinate come segue, dati tre insiemi arbitrari X_1, X_2, X_3:

  $$\{X_1, X_2, X_3\} = \{X_1\} \cup \{X_2\} \cup \{X_3\}.$$

  Ogni insieme può quindi essere rappresentato come l'unione di tutte le sue parti; la stessa cosa vale anche per i numeri naturali che vedremo in seguito.

- **Intersezione**

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

  Definizione 1.8. 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 1.9. 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 1.10. Differenza $A \setminus B = \{x | x \in A \land x \notin B\}$

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 1.11. 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 1.12. 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 1.13. Insieme delle parti - $P(X) := \{A | A \subseteq X\}$

Definiamo l'insieme delle parti $P(X)$ l'insieme di tutti i sottoinsiemi di X. Traiamo inoltre le seguenti conseguenze logiche:

- **Proprietà**:
  1. $A \cup A^c = X$.
  2. $A \cap A^c = \emptyset$.
  3. $(A^c)^c = A$.
  4. $X^c = \emptyset$.
  5. $\emptyset^c = X$.
  6. $A/B = A \cap B^c$
  7. $A \subseteq B \iff B^c \subseteq A^c$.
- **Proposizioni**:
  1. $\emptyset \in P(X)$.
  2. $X \in P(X)$.
  3. $A \subseteq X \iff A \in P(X)$.
  4. $x \in X \iff \{x\} \in P(X)$.

Definiamo inoltre **Complemento di un insieme** o insieme complementare A^c di A in X come la il risultato dell'operazione X/A; formalmente:

$$A^c := X/A := \{x \in X | x \notin A\}$$

Esempio. Insieme delle parti

Parola chiave "comprende OGNI sottoinsieme ricavabile dall'insieme originale". Osserva e capisci la pattern.

- Se $X = \emptyset \implies P(\emptyset) := \{\emptyset\}$.

- Se $X = 1 := \{0\} \implies P(\{0\}) := \{\emptyset, \{0\}\}$.
- Se $X = 2 := \{0, 1\} \implies P(\{0, 1\}) := \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.

1.1.1 Leggi di De Morgan

Le leggi di De Morgan sono delle formule importanti per la teoria degli insiemi: consentono di mettere in relazione l'operazione di unione con l'operazione di intersezione. Segue definizione formale:

Definizione 1.14. Leggi di De Morgan:
Siano gli insiemi: $A \subseteq X, B \subseteq X, A^c \subseteq X, B^c \subseteq X$. Valgono le seguenti ipotesi:

1. $(A \cup B)^c = A^c \cap B^c$.
2. $(A \cap B)^c = A^c \cup B^c$.

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

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

Lavorando con le corrispondenze possiamo trovare i seguenti casi base:

- 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.

A partire da queste nozioni ci è possibile definire i seguenti casi notevoli:

- **Relazione inversa**

  Definizione 1.16. 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:

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

[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.

Traiamo inoltre la seguente proprietà:

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

- **Composizione delle operazioni**

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

  Definizione 1.17. 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:

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

  E ne traiamo le seguenti conclusioni, date le relazioni $R \subseteq X \times Y$, $S \subseteq Y \times Z$ e $T \subseteq Z \times W$:

  - $Diag(Y) \circ R = R$.
  - $R \circ Diag(X) = R$.
  - $T \circ (S \circ R) = (T \circ S) \circ R$.

  INSERISCI ESEMPIO CON LA DIAGONALE.

1.3 Principi di dimostrazione

Il processo di dimostrazione matematica è un algoritmo deduttivo utilizzato per provare la verità o falsità di ipotesi arbitrarie basandosi sul ragionamento logico. Il processo si effettua formalizzando i concetti espressi nell'enunciato e consideriamo l'esercizio concluso quando si è riusciti a dimostrare tutto. Esistono inoltre più metodi per arrivare a una stessa soluzione:

- **Dimostrazione per prova diretta**

  Molto semplicemente si prende l'enunciato e si prova a dimostrare quanto richiesto, senza fare magheggi di alcun tipo.

  Esempio. Dimostrazione per prova diretta

  INSERISCI ESEMPIO.

- **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.

1.4 Domande di teoria

Teorema 1.18. Here goes a theorem.

Dimostrazione. Here goes the proof □

Corollario 1.19. Here goes a collorary

Esempio. Here goes an example

Nota. Here goes a note

Lemma 1.20. Here goes a lemma

Proposizione 1.21. Here goes a proposition

Definizione 1.22. 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** - $\mathtt{Diag}(X) := \{(x, x) | x \in X\}$

  La funzione diagonale o identità, denotata con $\mathtt{id}_X(x) = x$ per ogni $x \in X$, restituisce lo stesso valore che le è stato assegnato. Se vuoi scriverla, fai appello alla scrittura dell'insieme delle parti, solo saranno considerati parte dell'insieme le coppie con ambo i numeri uguali.

- **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** - $qu := \{(x, x^2) | x \in \mathbb{R}\}$

  Più comunemente conosciuta come la parabola fra le funzioni elementari. Hai che $qu(x) = x^2$.

  INSERIRE IMMAGINE.

- **Funzione di Dirichlet** - $Dir = \{(x, 0) | x \in Q\} \cup \{(x, 1) | x \in R/Q\}$.

  Curiosa funzione dalla difficile integrazione. Always bet on Lebesgue. Si definisce con:

$$Dir(x) = \begin{cases} 1 & , x \in \mathbb{Q} \\ 0 & , x \notin \mathbb{Q} \end{cases}$$

La possibilità di ottenere risultati tramite applicazioni implica l'esistenza di immagini; infatti definiamo formalmente:

Definizione 2.2. Immagine e Controimmagine:
Sia $f : X \to Y$ un'applicazione. Se $A \subseteq X$, diremo che l'immagine di A secondo f è il seguente insieme:

$$f(A) := \{f(x) | x \in A\} = \{y \in Y | \exists x \in A(f(x) = y)\}$$

L'immagine di tutto il dominio è poi detta immagine dell'applicazione f ed è l'insieme $f(X) := \{f(x) | x \in X\}$.

Se invece abbiamo $B \subseteq Y$, definiamo controimmagine di B secondo f l'insieme:

$$f^{-1}(B) := \{x \in X | f(x) \in B\}.$$

CONTINUA DA PAGINA 31 DOCUMENTO PAGINA 33 EFFETTIVA.

- 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 $\mathsf{Succ}(n)$, 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 $\mathsf{IND}_{\mathbb{N}}$. 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, i quali renderanno più semplice la risoluzione degli esercizi:

Proposizione 3.1. Assiomi di Peano

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

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

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 $\mathsf{IND}_{<}$.

Esempio. Dimostrazione con $\text{IND}_{\mathbb{N}^*}$
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.

Esempio. Dimostrazione con $\text{IND}_{<}$
INSERISCI ESEMPIO.

3.2 Principali operazioni ed elementi

Dove è sempre possibile utilizzare l'induzione per la dimostrazione dei teoremi, risulta particolarmente comodo provare determinate relazioni e operazioni per **Ricorsione**. Anch'essa è composta di due casi:

1. Caso base, da dove inizia la dimostrazione.
2. Caso ricorsivo, il quale avanza tenendo conto dei valori precedentemente ottenuti.

L'esempio più semplice, spesso usato anche nella programmazione, è la formalizzazione del concetto di fattoriale.

Esempio. Dimostrazione con ricorsione

- 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:

$$0! = (0-1)! \times 1 = 1$$
$$1! = (1-1)! \times 1 = 1 \times 1 = 1$$
$$2! = (2-1)! \times 2 = 1 \times 2 = 2$$
$$3! = (3-2)! \times 3 = 2 \times 3 = 6$$
$$4! = (4-3)! \times 4 = 6 \times 4 = 24$$

Adesso è ora di distruggere tutto ciò che è stato insegnato alle scuole elementari sulla matematica; definiamo tutte le operazioni elementari:

- **Funzione Successore**

  La funzione più semplice ma anche la più importante, che consente di poter ragionare induttivamente sull'insieme dei naturali.

  Definizione 3.2. Funzione numero successore

  Supponiamo la formula: $\forall n \in \mathbb{N}.\{1 + n = succ(n)\}$

  Diciamo quindi che $[1 + n = succ(n)] = \phi(n)$.

  – Caso base
  $\phi(0) \iff 1 + 0 = succ(0) \iff 1 + 0 = 1$, vero.
  – Passo induttivo
  $\phi(n) \implies \phi(n+1) = \phi(succ(n)) \iff 1 + succ(n) = succ(succ(n))$
  $1 + succ(n) = succ(n+1) = succ(succ(n))$ per definizione.

  Formula dimostrata.

  Questa prova ci consente di ampliare il nostro arsenale con le operazioni elementari, in quanto esse sono basate su di essa e ogni numero naturale di può scrivere come la somma di 1_n.

- **Addizione**

  L'operazione elementare di base usa la definizione di funzione successore. Viene definita ricorsivamente come:

  Definizione 3.3. Addizione fra due numeri m, n

  – **Passo base**
  $m + 0 = m$
  – **Passo ricorsivo**
  $m + succ(n) = succ(m + n)$

Esempio. Dimostrare che $2+3=5$

Molto semplicemente utilizziamo i casi della definizione per andare avanti:

- $2+3=2+succ(2)=succ(2+2)$
- $succ(2+2)=succ(2+succ(1))=succ(succ(2+1))$
- $succ(succ(2+1))=succ(succ(2+succ(0)))=succ(succ(succ(2)))=5$.

L'addizione porta necessariamente con sé le sue proprietà, che sono:

1. $0+m=m$, $m+0=m$

   Dimostrazione. $\phi_0(m) := 0+m=m \in \mathbb{N}$

   - $\phi_0(0) \iff 0+0=0$, vale.
   - $\phi_0(m) \implies \phi_0(succ(m)) \iff 0+succ(m)=succ(m)$
     $0+succ(m)=succ(m+0)=succ(m)$ per definizione.

   CVD. □

2. $succ(m)=m+1=1+m$
   Dimostrata nella definizione 3.2

3. $m+succ(n)=succ(m)+n$

   Dimostrazione. $\forall n \in N, \forall m \in N.[(m+succ(n)=succ(m)+n]$

   Diciamo innanzitutto che $\forall m \in N.[(n+succ(n)=succ(m)+n]=\phi(n)$

   - $\phi(0) \iff \forall m \in \mathbb{N}.[m+succ(0)=succ(0)+m]$
     $m+succ(0)=succ(m+0)=succ(m)=succ(m)+0$. Vale.
   - $\phi(n) \implies \phi(succ(n)) \iff \forall m \in \mathbb{N}.[m+succ(succ(n))=succ(m)+succ(n)]$.
     Sia ora $m \in \mathbb{N}.succ(m)+succ(n)=succ(m+n)=succ(m+succ(n))=m+succ(succ(n))$.

   La formula vale per definizione della funzione successore. CVD. □

4. $(m+n)+l=m+(n+l)$

   Dimostrazione. INSERIRE DIMOSTRAZIONE □

5. $m+n=n+m$

   Dimostrazione. $\forall m, [\forall n \in \mathbb{N}.(m+n=n+m)]$, $[]=\phi(m)$

   - $\phi(0) \iff 0+n=n+0$. Vale per definizione della proprietà n.1.
   - $\phi(m) \implies \phi(succ(m)) \iff \forall n \in \mathbb{N}.[succ(m)+n=n+succ(m)]$, dove $[]=\theta(m)$.

   Effettuiamo una seconda induzione sulla formula $\theta(n)$:

   - $\theta(0) \iff succ(m)+0=0+succ(m)$, formula vera.

– $\theta(n) \implies \theta(succ(n)) \iff succ(m) + succ(n) = succ(n) + succ(m) =$
  1. $= succ(succ(m) + n)$
  2. $= succ(m + succ(n))$
  3. $= succ(succ(n) + m)$
  4. $= succ(n + succ(m))$

Formula dimostrata. CVD. □

6. $m + n = 0 \implies m = 0 \wedge n = 0$

Dimostrazione. $\forall m \in N.[\forall n \in N.(m + n = 0 \implies m = 0 = n)], [] = \phi(m)$

– $\phi(0) \iff \forall n \in N.(0 + n = 0 \implies 0 = n)$, vale per definizione.
– $\phi(m) \implies \phi(succ(m)) \iff \forall n \in N.[succ(m) + n = 0 \implies succ(m) = 0 = n]$.

A questo punto ragioniamo. La formula $succ(m) + n = 0$ non potrà mai essere vera poiché viola l'assioma di Peano 1. Raggiungiamo quindi un'assurdità e la formula risulta falsa.

Tuttavia, la formula $\phi(m)$ è della forma $P \implies Q$. Noi abbiamo provato che P è falsa, di conseguenza Q risulta vera grazie al connettivo. Abbiamo quindi dimostrato la formula. □

7. $m + n = l + n \implies m = l$

Dimostrazione. $m, l \in \mathbb{N}.\forall n \in N.[(m + n = l + n \implies m = l)], [] = \phi(n)$.

– $\phi(0) \iff m + 0 = l + 0 \implies m = l$, vale.
– $\phi(n) \implies \phi(succ(n)) \iff m + succ(n) = l + succ(n) \implies succ(m + n) = succ(l + n) \implies m + n = l + n$

Formula dimostrata in quanto abbiamo raggiunto l'ipotesi induttiva $m + n = l + n \implies m = l$. □

8. $m + n = n \implies m = 0$

Dimostrazione. $\forall n \in \mathbb{N}.[m + n = n \implies m = 0], [] = \phi(m)$.

– $\phi(0) \iff 0 + n = n$, vale per definizione.
– $\phi(m) \implies \phi(succ(m)) \iff succ(m) + n = 0$, impossibile per Peano 1.

Formula dimostrata poiché $P \implies Q$, dove $P = 0$, $Q = 1$. □

- **Ordinamento, concetto di minimo**

Partiamo dal presupposto che per parlare di ordinamento abbiamo bisogno di definire cosa rende un numero maggiore o minore di un altro. Assorbito tal concetto, diciamo che ogni sottoinsieme non vuoto di $\mathbb{N}$ ha necessariamente un elemento minimo, formalmente:

$$\exists n \in N, \text{ dove } n \in A, \forall \alpha \in A.(n \leq \alpha).$$

Dimostrazione. Concetto di minimo MIN

Iniziamo supponendo un insieme A non vuoto ed un elemento $n \in A$. Diciamo che:

- $0 \in A$, se non lo è, passa al numero successivo, altrimenti hai trovato il minimo.
- $1 \in A$, se non lo è, passa ancora al successivo, altrimenti hai trovato il minimo. Ripeti il processo fin quando non trovi il numero.

□

Tuttavia, attenzione: il concetto di minimo non vale per i sovrainsiemi numerici di $\mathbb{N}$, a meno che non venga preso un insieme proprio. Puoi inoltre usare lo stesso ragionamento per trovare il valore massimo in un insieme i cui estremi sono definiti.

Un'altra particolarità del principio di minimo è che implica la validità del principio del terzo escluso nei numeri naturali:

Teorema 3.4. $\text{MIN} \implies \text{PEM}_P$

Dimostrazione. Ricorsione

Sia una formula P, dimostriamo che vale il principio del terzo escluso, ovvero $(P \vee \neg P)$.

$$A_P = \{1\} \cup \{x \in \mathbb{N} | x = 0 \wedge P\}$$

$1 \in A_P$, quindi A_P non è vuoto.

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

Possiamo ottenere uno stesso risultato anche induttivamente, effettuando il seguente ragionamento:

Dimostrazione. $\text{IND}_{\mathbb{N}}$

Sia ora $n = min(A_P)$, abbiamo che $[n = 0 \vee \exists m \in \mathbb{N}.(n = succ(m))]$.

Chiamiamo il minimo P e dimostriamo che vale $(P \vee \neg P)$:

$$0 \in A_P \implies P$$

Se il minimo è 1, P non è valida, di conseguenza vale $\neg P$, quindi:

$$P_A.(0 = 0) \implies (0 \in A_P) \implies 0 = minA_P.$$

Qui hai trovato l'assurdo ricavando che il minimo è 0.

CVD, vale $(P \vee \neg P)$. □

- **Moltiplicazione**

La moltiplicazione è la seconda operazione elementare che consente di esprimere ogni singolo numero naturale. Viene definita ricorsivamente come segue:

Definizione 3.5. Moltiplicazione - $m, n \in N$

- $m \times 0 = 0$

– $m \times succ(n) = m \times n + m$

Seguono esempi pratici per miglior comprensione:

Esempio. Dimostrare che $2 \times 3 = 6$

Il senso dei passaggi è che, in base alla definizione ricorsiva della moltiplicazione e a quella della funzione successivo, puoi ridurre tutti i numeri nella formula al minimo ed arrivare a una somma.

$$2 \times 3 = 2 \times succ(2) = 2 \times 2 + 2 = 2 \times succ(1) + 2 =$$
$$2 \times 1 + 2 + 2 = 2 \times succ(0) + 2 + 2 = 2 \times 0 + 2 + 2 + 2 =$$
$$0 + 2 + 2 + 2 = 6.$$

Questo procedimento può tranquillamente valere anche per numeri incogniti. Infatti, se vogliamo dimostrare che $m \times 1 = m$, opereremo allo stesso modo:

$$m \times 1 = m \times succ(0) = m \times 0 + m = 0 + m = m$$

– **Proprietà distributiva**
La moltiplicazione ha giustamente la sua proprietà distributiva, ovvero rende possibile "distribuire" l'operazione a più valori se ambo devono essere moltiplicati.

Proposizione 3.6. La proprietà distributiva viene definita ricorsivamente e ha i seguenti casi:

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

Dimostrazione. La proprietà è definita tramite induzione come segue:

Supponiamo che $\forall m \in N.[\forall n \in N.(m * n = 0 \implies m = 0 \vee n = 0]$

* Il caso base vale per identità. Bella fortuna.
  $\phi(0) \iff \forall n \in N.(0 \times n = 0 \implies 0 = 0 \vee n = 0)$.
* Passo induttivo
  $\phi(n) \implies \phi(succ(n)) \iff$
  $\forall n \in N.[(succ(n) \times n = 0) \implies succ(m) = 0 \vee n = 0], [] = \theta(n)$
* Abbiamo ottenuto la formula $\theta(n)$, sulla quale possiamo operare:
  $\theta(n) \iff succ(m) \times n = 0 \implies succ(m) = 0 \vee n = 0)$.
* Il suo caso base vale fortunatamente per identità:
  $\theta(0) \iff succ(m) \times 0 = 0 \implies succ(m) = 0 \vee 0 = 0$.
* Passo induttivo.
  $\theta(n) \implies \theta(succ(n)) \iff$

$$succ(n) = 0 \implies succ(m = 0 \vee succ(n)) = 0.$$

∗ Proviamo a verificare la proprietà
$succ(m) \times succ(n) = 0 \iff succ(m) \times n + succ(m) = 0 \implies$
$succ(m) \times n = 0 \wedge succ(m) = 0.$
Questa formula risulta falsa per l'assioma di Peano 1, infatti il successore di 0 è 1, non 0.

La formula qui è in ogni caso dimostrata grazie al funzionamento del connettivo $\implies$. Il falso implica il vero. CVD □

- **Elevamento a potenza**

  Contrariamente a quello che si può pensare, l'elevamento a potenza è un'operazione fattibile nell'insieme $\mathbb{N}$ e anche questa viene definita ricorsivamente:

Definizione 3.7. Elevamento a potenza

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

Vediamo un semplice esempio usando la definizione.

Esempio. Dimostrare che $2^3 = 8$

Come visto nella moltiplicazione, anche qui è necessario vedere i numeri sotto la lente della funzione successivo, per poi usare la definizione di moltiplicazione e ottenere il risultato.

$$2^3 = 2^{succ(2)} = 2^2 \times 2 = 2^{succ(1)} \times 2 = 2^1 \times 2 \times 2 = 2^{succ(0)} \times 2 \times 2 = 2^0 \times 2 \times 2 \times 2 =$$

$$1 \times 2 \times 2 \times 2 = 8. \text{ CVD}$$

3.3 Costruzione di interi e razionali

Finora ci siamo concentrati sull'insieme numerico dei numeri naturali $\mathbb{N}$, ma come è possibile definire gli altri sovrainsiemi che compongono la matematica? Partiamo dal basso per ora e cerchiamo di definire i **Numeri interi**, appartenenti all'insieme $\mathbb{Z}$:

Definizione 3.8. Insieme dei numeri interi relativi $\mathbb{Z}$
Fondamentalmente l'unione dell'insieme dei naturali con quello dei loro opposti, formalmente:

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \mathbb{N}^-$$

Dove i rispettivi insiemi sono:

- $\mathbb{N} = \{0, 1, 2, ..., n\}$.
- $\mathbb{N}^- = \{-1, -2, ..., -n\}$.

Il ragionamento vale pure per l'insieme dei naturali senza 0, $\mathbb{N}^*$. Importante ricordare che siccome stai unendo due opposti, se provi a trovare un'intersezione fra i due, otterrai un insieme vuoto.

$$N^* \sim N_*, N^* \cap N_* = \emptyset$$

Abbiamo aggiunto all'equazione dello studio i numeri negativi: come possiamo rappresentarli? Ebbene, serviranno due numeri.

Esempio. Rappresentazione dei numeri negativi.

$$-1 = 0 - 1 = 1 - 2$$
$$-2 = 0 - 2 = 1 - 3$$
e così via.

Questa scrittura vale anche con 0, 1, 2 e altri. Tutti i numeri si possono infatti rappresentare mediante una relazione di sottrazione. Ci consente di rendere due coppie scritte in modo diverso uguali grazie alla definizione di funzione.

Adesso approfondiamo un simbolo raramente utilizzato negli studi della matematica alle scuole dell'obbligo: $\sim$, indicante l'equivalenza. Ci permette di identificare gli oggetti disuguali che però sono equivalenti. Diamone una definizione formale:

Definizione 3.9. Equivalenza
Una relazione si dice equivalente quando rispetta questi tre criteri:

1. La relazione è riflessiva.
2. La relazione è simmetrica.
3. La relazione è transitiva.

Supponiamo ora le coppie $(m, n) \sim (m', n')$. Se queste sono equivalenti, come indicato dalla tilde, sarà possibile utilizzare i classici criteri di equivalenza per le equazioni. Varranno quindi le seguenti scritture *equivalenti*:

$$m - n = m' - n' \sim m + n' = m' + n$$

Diremo inoltre che $\sim$ è un'equivalenza su $\mathbb{N} \times \mathbb{N}$.

Dimostrazione. Relazione di equivalenza

- La relazione è riflessiva.
  $(m, n) \sim (m, n) \iff m + n = m + n$.
- La relazione è simmetrica.
  $(m, n) \sim (m', n') \implies (m', n') \sim (m, n) \implies m + n' = m' + n \implies$
  $m' + n = m + n'$.

- La relazione è transitiva.
  $(m,n) \sim (m',n') \iff m+n' = m'+n \wedge (m',n') \sim (m'',n'') \iff$
  $m'+n'' = m''+n' \wedge (m,n) \sim (m'',n'') \iff m+n'' = m''+n$
  Abbiamo ora che:
  $m'+n'' = m''+n' \implies m'+n+n'' = m''+n'+n$
  $\implies m'+n'+n'' = m''+n'+n$
  $\implies m+n'' = m''+n$. Un termine vale l'altro. Transitività dimostrata.

□

Sapendo tutto ciò, ci è possibile dare una definizione rigorosa dell'insieme dei relativi:

Definizione 3.10. Definizione rigorosa dell'insieme $\mathbb{Z}$
Definiamo $\mathbb{Z}$ l'insieme delle classi di equivalenza $\mathbb{Z} := (\mathbb{N}\times\mathbb{N})/\sim$, ovvero:

$$\mathbb{Z} = \{[(m,n)]_\sim | (m,n) \in \mathbb{N}\times\mathbb{N}\} = \left\{\{(m',n') \in \mathbb{N}\times\mathbb{N} | (m',n') \sim (m,n)\} | (m,n) \in \mathbb{N}\times\mathbb{N}\right\}.$$

Come visto prima, ci è possibile definire ogni numero tramite sottrazioni. Vedi queste coppie come se fossero una funzione di sottrazione e avrai capito tutto.

- $0_\mathbb{Z} = [(0,0)]_\sim$
- $1_\mathbb{Z} = [(1,0)]_\sim$
- $-1_\mathbb{Z} = [(0,1)]_\sim$
- $2_\mathbb{Z} = [(2,0)]_\sim$
- $-2_\mathbb{Z} = [(0,2)]_\sim$

Puoi potenzialmente andare avanti ad infinitum con questa scrittura.

A partire da questa definizione ci è possibile ragionare induttivamente per eseguire utili dimostrazioni, come nel seguente esempio:

Esempio. Dimostrare che: $[(m,n)]_\sim := \{(m',n') \in NxN | (m',n') \sim (m,n)\}$
Per avere un'equivalenza da un punto di vista di valore con numeri effettivi, bisogna trovare due operazioni che ritornino lo stesso numero. Ora ragionando induttivamente:

- $0_Z. = [(0,0)]_\sim = [(1,1)]_\sim \iff (0,0) \sim (1,1)$, vera perché $0-0=0$, $1-1=0$.
- $1_Z := [(1,0)]_\sim = [(2,1)]_\sim \iff (1,0) \sim (2,1)$, vera perché $1-0=1$, $2-1=1$.

La dimostrazione vale perché abbiamo dimostrato precedentemente che si può andare avanti all'infinito.

Proposizione 3.11. Osserviamo inoltre che l'insieme $\mathbb{N}$ è incorporato in $\mathbb{Z}$.
Definiamo quindi la funzione $i : \mathbb{N} \to \mathbb{Z}$ dalla regola:

$$m \to i(m) := m_{\mathbb{Z}} := [(m, 0)]_{\sim} := \{m', n' \in \mathbb{N} \times \mathbb{N} | m' = m + n'\}.$$

Nel caso in cui valga $m = l$, avremo il seguente sviluppo:

- $i(m) = i(l) \iff [(m, 0)]_{\sim} = [(l, 0)]_{\sim}$
- $\iff (m, 0) \sim (l, 0)$
- $\iff m + 0 = l + 0$
- $\iff m = l.$

Puoi osservare che la funzione i è iniettiva perché $\mathbb{N}$ si può identificare in $i(\mathbb{N})$ in quanto scritture equivalenti, ed in questo senso, otteniamo che $\mathbb{N} \subseteq \mathbb{Z}$.

3.4 Fattorizzazione e teorema fondamentale dell'aritmetica

3.5 Congruenze

3.6 Domande di teoria

3.7 Esercizi

1. Dimostrare la funzione $\mathtt{pred}(n) : \mathbb{N} \to \mathbb{N}$

   Dimostrazione. Definiamo la funzione predecessore nei naturali ricorsivamente con i seguenti casi:

   - $\mathtt{pred}(0) = 0$
   - $\mathtt{pred}(\mathtt{succ}(n)) = n$

   Data la particolarità del caso 0, lavoreremo su $\mathbb{N}^*$. Supponiamo la seguente formula:

   $$\forall n \in \mathbb{N}^*.[(\mathtt{succ}(\mathtt{pred}(n))] = n, [] = \theta(n)$$

   - $\theta(1) \iff \mathtt{succ}(\mathtt{pred}(\mathtt{succ}(0)) = \mathtt{succ}(0)$
   - $\theta(n) \implies \theta(\mathtt{succ}(n)) \iff \mathtt{succ}(\mathtt{pred}(\mathtt{succ}(n))) = \mathtt{succ}(n).$

   Per definizione abbiamo che $\mathtt{pred}(\mathtt{succ}(n)) = n$. Quindi la formula è dimostrata. □

2. Dimostrare che $1 \times 1 = 1$.

Dimostrazione. Banalmente sostituisci i termini nella definizione di moltiplicazione e vedi i numeri come i successori del loro valore precedente

$$1 \times 1 = 1 \times succ(0) = 1 \times 0 + 1 = 1$$

□

3. Dimostrare che $1 \times m = m$.

Dimostrazione. Questa volta ragioniamo per induzione

Supponiamo innanzitutto che $\forall m \in N.(1 \times m = m)$

- Il caso base vale banalmente per definizione di moltiplicazione
  $\phi(0) = 1 \times 0 = 0$.
- Per gli assiomi di Peano, diciamo che:
  $\phi(m) \implies \phi(succ(m)) \iff 1 \times succ(m) = succ(m)$.
- Mentre per la definizione del caso ricorsivo della moltiplicazione abbiamo:
  $1 \times succ(m) = 1 \times m + 1 = m + 1 = succ(m)$.
- Avendo dimostrato il passo induttivo, possiamo dire che vale anche per m:
  $\phi(m) \iff 1 \times m = m$. CVD

□

4. Dimostrare che $0 \times m = 0$.

Dimostrazione. Anche qui risulta comodo ragionare per induzione

Supponiamo che $\forall m \in N(0 \times m = 0)$.

- Abbiamo che il caso base vale per definizione:
  $\phi(0) \iff 0 \times 0 = 0$.
- Usiamo ancora gli assiomi di Peano per implicare la funzione successiva.
  $\phi(m) \implies \phi(succ(m)) \iff 0 \times succ(m) = 0$.
- Usiamo la definizione di moltiplicazione e sostituiamo i termini:
  $0 \times succ(m) = 0 \times m + 0 = 0 + 0 = 0$. CVD

□

5. Dimostrare induttivamente e ricorsivamente che $m < n$.

   Per entrambe le dimostrazioni valgono le seguenti supposizioni:

   (a) $m < n \implies m * l < n * l$, dove $l >= 1$

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

Dimostrazione. Per induzione

AGGIUSTA

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

□

Dimostrazione. Per ricorsione

AGGIUSTA

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

□

6. Dimostrare che $m <= m * n$, dove $n >= 1$.

Dimostrazione. AGGIUSTA - Per lavorare su questa dimostrazione risulta utile fissare un m. Detto ciò:

Supponiamo la formula: $m <= n \iff \exists k \in N.(n = m + k), k >= 0$.

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

□

3.8 Appunti

- 21-11-24

Es 28. Sia $n \in N$, dimostriamoche$\exists k \in N.(n < k < succ(n)) \implies \perp$Dimostraquindichenonc'
laformulaappenascritta.

Supponiamo $\exists k \in N.(n < k < succ(n))$

- $n < k \iff \exists l \in N*.(k = n + l) l > 0 \iff l >= 1 \iff l = 1 + \sigma, \sigma >= 0.k = n + 1 +$

$k < succ(n) \iff \exists m \in N*.(succ(n) = k + m), m >= 1$

- $Succ(n) = n + 1 + \sigma) + m \iff n + 1 = (n + 1) + \sigma + m \iff \sigma + m = 0 \implies \sigma = 0 = m$

Siccome abbiamo trovato che m >= 1, siamo incappati in un'assurdità provando che $\sigma = 0 =$
m.Laformulaquindifalsaeabbiamoprovatol'assurdo.Inoltre, n+1statosemplificatograzieaicrit

Prop. 1 Siano m, n, m', n' $\in N$

- $m = m' \wedge n = n' \wedge m <= n \implies m' <= n' - m = 0 \vee m > 0 - l = 1 \vee l > 1, \forall l \in N* - n <$
$succ(n) - n < m \implies succ(n) <= m - m < n \vee m = n \vee n < m - m <= n \iff m =$
$n \vee m < n - m < n \iff m <= n \wedge m! = n - \neg(n < n) - m < n \implies m! = n - m! =$
$nm < n \vee n < m - m > 1 \implies pred(m) >= 1$

- Il principio di numero minimo - Siano un relazione d'ordine (x, <=) . $x_0 \in X, A \subseteq$
$Xx_0unelementominimodiA \iff -x_0 \in A - \forall \alpha \in A.(x_0 <= \alpha)$

X = 0,1,2 . 0 è un elemento minimo di X perché 0 è in X e $\forall x \in Xx >= 0$.

Decidere un elemento minimo dipende dal sottoinsieme. Ogni altro elemento deve essergli maggiore o uguale.

Prop. (X, <=) X insieme parzialmente ordinato, dove $x_0, y_0 \in X, A \subseteq XSex_0, y_0$sonoelementiminimidiA
y_0.Questoperchesistesolamenteunminimo.

Dim. $x_0 \iff \forall a \in A, a >= x_0 y_0 \iff \forall a \in A, a >= y_0$

Transitività? if $a >= x_0 \wedge a >= y_0 \implies x_0 = y_0$.

Definizione, minimo MIN Ogni sottoinsieme non vuoto di N ha un elemento minimo.

Dim. per induzione $IND_< - \phi(0)[(0) \wedge \phi(1) ... \wedge (\phi(n) \implies \phi(n+1)] \implies \forall n \in N.(\phi(n))$

!= $A \subseteq X$

- $\phi(n) \iff n \notin A$SupponiamocheAnonabbiaunminimoeproviamoadimostrarel'assurditdiques

- $\phi(0) \iff 0 \notin A$valeperchse$0 \in a$allora0Min(A). $- 0 \notin A \wedge 1 \notin A \wedge ... \wedge n \notin A \implies$
$n + 1 \notin A \iff \neg(n + 1 \in A)$;Se$n + 1 \in A$, alloran + 1 = min(A)

Guarda la foto da telefono.

C'è una prova più semplice, che segue: Supponi A insieme non vuoto e che $n \in A$.

- $0 \in A$.Se0noninA, passaalsuccessivo, altrimentiilminimo$-1 \in A$.Se1noninA, passaalsuccessivo

Il principio del minimo non regge per l'insieme R, a meno che non venga preso un insieme proprio.

- 05-12-24

Ex 29. $\in N.[(, \in N.(m(n + l) = mn + ml))][] = \phi(m)$

$\phi(0) \iff \in N, \in N.(0(n + l) = 0 * n + 0 * l)$vale$\phi(m) \implies \phi(succ(m)) \iff \forall n \in N, \forall l \in$
$N.(succ(m)(n + l) = succ(m)n + succ(m)l)$

Lemma: $\in N.(succ(m) * n = m * n + n)m + 0 = 0m + succ(n) = succ(m + n)m * 0 = 0m * succ(n) = m$

$\theta(0) \iff succ(m) * 0 = m * 0 + 0 vale \theta(n) \implies \theta(succ(n)) \iff succ(m) * succ(n) = m * succ(n) + succ(n) succ(m) * succ(n) = succ(m) * n + succ(m) = (m * n + n) + succ(m) = m * n + m + succ(m)$

n+succ(m) = n+m+1 m+succ(n) = m+n+1

m*n + m + succ(m) = m*n+m+succ(n)

Per il lemma, succ(n)(n+l) = m(n+l)+n+l = mn+ml+nl = (m*n+l)+(m*l+l) = succ(n)*n + succ(m)*l La formula $\phi(n) vale.$

Ex. 30 $\forall m \in N, \forall n \in N.[(m * n = n * m)][] = \phi(m)$

$\phi(0) \iff \in N.(0 * n = n * 0) la formula vale \phi(m) \implies \phi(succ(m)) \iff \forall n \in N.[(succ(m) * n = n * succ(m))]$

for n $\in n : succ(m) * n = m * n + n. Questo ultimo risultato uguale all'ultima ipotesi ottenuta fra le que$ $n = n * m periporesi induttiva$

Formula dimostrata.

Ex. 30i for m $\in$ N, $\in$ N, $\forall l \in N.](m * n) * l = m * (n * l)][] = \phi(n)$

- $\phi(0) \iff \forall l \in N.[(m * n) * l = m(0 * l)] Il caso base vale - \phi(n) \implies \phi(succ(n)) \iff \forall l \in N.[(m * succ(n)) * l = m(succ(n) * l)] Fissiamo l \in N.$

(m*succ(n))*l = (m*n+m)l per definizione. Essendo poi la moltiplicazione commutativa = l(m*n+m), che per distributività diventa = (m*n)l + m*l = m(n*l+l) = m(succ(n)*l)

Formula dimostrata.

Ex.31-1 m*l = n*l $\implies m = n, m, n, l \in N$

Per prop già vista 2.6.4 abbimo che m<n $\implies m * l < n * l. Supponiamo quindi m < n \forall l \in N. Quindi abbiamo che m * l < n * l; tuttavia questa un' assurdit, quindi m < n falsa e quindi m <= n.$

Rimangono ora solo m=n $\vee m > n, quindi m >= n. Allo stesso modo, se n < m avremo un risultato ugu$

Varrà solo l'istanza m=n. Abbiamo infatti che m<=n<=m $\implies m = n. La relazione antisimmetrica.$

Ex.31-2 m<n $\wedge m' < n' - - - - - - - - - - - - - - - - - m * m' < n * n'$

m<n $\implies m * m' < n * m' Per ipotesi m' < n' \implies m' * n < n' * n m < n \implies m * l < n * l$

m*m' < n*m' = m'*n < n*m = n*n'. Abbiamo quindi dimostrato l'ipotesi sotto la barra. [m*m' < n*n'].

Ex.32-1 $m^0 = m^{succ(0))} = m^0 * m = 1 * m = m.$

fissiamo m,n $\in$ N e dimostriamo che $\forall l \in N.[(m^{n+l} = m^n * m^l)][] = \phi(l)$

- $\phi(0) \iff m^{n+0} = m^n * m^0 = m^n * 1, che vale. - \phi(l) \implies \phi(succ(l)) \iff m^{n+succ(l)} = m^n * m^{succ(l)}$

$m^{n+succ(l)} = m^{succ(n+l)} per definizione. Or a usiamo la definizione di addizione. = m^{n+l} * m. Per ipotesi i$ $(m^n * m^l)m = m^n * (m^l * m) = m^n * m^{succ(l)}, quindi \phi(succ(l)) vale.$

Definita una relazione $0 \sim m. N x N(m, n) \sin(k, l) \iff m + l =_N k + l * m.$

Z è l'insieme delle classi di equivalenza (definizione già data) se n $\in$ N abbiamo plus potenza i. i* N $\to$ Z Abbiamo infatti che $i(m) := [(m, 0)]_\sim (m - 0) = m.$

Esercizio da esame: Dimostrare che $0_Z! = 1_Z == 0_Z = 1_Z \implies \perp$

$0_Z = [(0,0)]_\sim 1_Z = [(1,0)]_\sim$

Stiamo dimostrando che una cosa è falsa e in questo caso non uguale ad un'altra. Quindi andiamo di equivalenza. $0_Z = 1_Z \iff [(0,0)]_\sim = [(1,0)]_\sim \iff (0,0) \sim (1,0) \iff 0+0 = 1+0 \iff 0 = 1.0 = 1 \implies \perp perassiomadipeano1.Formuladimostrata.$

Dimostrare l'addizione in Z $[(m,n)]_\sim + [(k,l)]_\sim = [(m+k, n+l)]_\sim MOLTOIMPORTANTESTAFormulaPerch$
$n + k - l = (m + k) - (k + l)$

Esempio pratico: $3_Z + (-5)_Z = [(3,0)] + [(0,5)] = 3+0+0-5 = 3-5 = [(3,5)] = -2 = [(0,2)].$

(m,n) $\sim (m', n') \wedge (k,l) \sim (k', l') \implies [(m,n)]_\sim + [(k,l)]_\sim = [(m', n')]_\sim + [(k', l')]_\sim = [(m + k, n + l)]_\sim = [(m' + k', n' + l')]_\sim = (m + k, n + l) \sim (m' + k', n' + l') \iff [m + k + n' + l' = m' + k' + n + l] Dimostrare[] eledueipotesiiniziali.$

(m+n') + (k+l') = (m'+n)+(k'+l) Formula dimostrata nonostante l'ordine dei termini grazie alla commutatività dell'addizione.

Provare ora che i:Nim|->i(m) := $[(m,0]_\sim rispettal'addizionecomei(m + l) = i(m) + i(l)$

I(m+l) = [(m+l, 0)] i(m) = [(m,0)] i(l) = [(l,0)]

[m,0] + [l,0] = [m+l,0+0]

Provare che $z+0_z = 0_z + z = z, dovez \in Z$

z = [(m,n)] 0_Z = [(0, 0)]

[m,n] + [0,0] = [m,n], la seconda parte vale per commutatività.

Dimostrare che z + z' = z' + z, dove z, z' $\in Z$

z = [m,n] z' = [m',n']

[m,n] + [m',n'] = [m',n'] + [m,n] = [m+m', n+n'] = [m'+m, n'+n] vale per commutatività. = [m',n'] + [m,n], addizione vale su Z, dimostrata per definizione.

Cardinalità

Strutture Algebriche

5.1 Monodi

5.2 Gruppi

5.3 Anelli

5.4 Reticoli

5.5 Domande di teoria

5.6 Esercizi