▼ 3.0 - Teoria assiomatica degli insiemi

▼ **3.1 - Teoria degli insiemi naive**

Nella **teoria degli insiemi naive** tutto viene trattato come un insieme, dunque numeri, figure geometriche, funzioni rappresentano insiemi particolari. Questo permette di avere principalmente un vantaggio e uno svantaggio:

- Permette di introdurre e comprendere concetti come i limiti.
- Causa la perdita di alcuni aspetti computazionali (Es. le funzioni come insiemi non si calcolano).

In questa teoria gli insiemi non devono per forza essere omogenei (possono possedere un mix di qualunque cosa, in quanto tutto è considerato come un insieme) e le ripetizioni e l'ordine non contano (Es. {1, 2, 3} = {1, 3, 3, 2, 1}).

I diagrammi di Venn non riescono a rappresentare molto bene la teoria degli insiemi e vanno utilizzati con cautela.

Appartenenza $\in$

Il primo insieme deve essere esattamente contenuto nel secondo, non basta che i suoi insiemi siano contenuti.

- {1, 2} $\notin$ {1, 2, 3}
- 1 $\in$ {1, 2, 3}
- 1 $\notin$ {{1, 2}, 3}
- {1, 2} $\in$ {{1, 2}, 3}
- $\varnothing$ $\notin$ {1, 2, 3}
- $\varnothing$ $\in$ {$\varnothing$, 1}

Inclusione $\subseteq$

Il primo insieme deve essere allo stesso livello del secondo insieme ma può avere meno insiemi al suo interno.

- {1, 3} $\nsubseteq$ {{1, 3}, 2}
- {1, 3} $\subseteq$ {1, 2, 3}
- 1 $\nsubseteq$ {1, 2, 3}
- {1} $\subseteq$ {1, 2, 3}
- {1} $\nsubseteq$ 1
- 1 $\subseteq$ 1

▼ **3.2 - Teoria assiomatica degli insiemi**

La teoria assiomatica degli insiemi nasce dal fatto che la teoria degli insiemi naive porta a dei paradossi, occorre:

- Eliminare l'assioma di comprensione (per qualunque proprietà P è possibile formare un insieme $\{x|P(x)\}$) il quale porta al paradosso di Russell.
- Controllare l'uso meta-linguistico (es. nel paradosso di Russell l'insieme X non può essere un insieme ma una classe in quanto altrimenti parlerebbe di sè stesso).

La teoria assiomatica degli insiemi si basa dunque su:

- La non definizione del concetto di insieme, considerato quindi come un elemento primitivo.

- L'utilizzo di assiomi per permettere di creare insiemi di partenza dai quali gli altri insiemi possono essere creati.

Esistono numerose teorie insiemistiche che differiscono per quanto riguarda i loro assiomi, noi utilizzeremo la **teoria di Zermelo-Fraenkel (ZF)**, la quale è la meno controversa ed è sufficiente per sviluppare gran parte della matematica. Nonostante ciò questa teoria non è mai stata dimostrata essere consistente.
Questa teoria si basa sui seguenti assiomi:

Assioma di estensionalità

Due insiemi sono uguali se e solo se hanno gli stessi elementi.

$\forall X, \forall Y, (X = Y \iff \forall Z, (Z \in X \Leftrightarrow Z \in Y))$

Definizione di essere sottoinsieme

X è sottoinsieme di Y se ogni suo elemento appartiene anche a Y.

$X \subseteq Y = \forall Z, (Z \in X \Rightarrow Z \in Y)$

Assioma di separazione

Dato un insieme, è possibile formare un suo sottoinsieme che soddisfi una certa proprietà.

$\forall X, \exists Y, \forall Z, (Z \in Y \iff Z \in X \wedge P(Z))$

Da questo assioma è poi possibile indicare Y in questo modo:
$Y = \{Z \in X | P(Z)\}$

Assioma dell'insieme vuoto

$\exists X, \forall Z, Z \notin X$

X viene indicato così: $\emptyset$

Definizione di intersezione binaria

$X \in A \cap B \iff X \in A \wedge X \in B$

Intersezione n-aria

$A_1 \cap ... \cap A_n = ((A_1 \cap A_2) \cap ... \cap A_n)$

Tuttavia l'assioma di intersezione binaria non consente di intersecare un numero infinito di insiemi.

Definizione di intersezione

Dato un insieme di insiemi, esiste un insieme che ne è l'intersezione, il quale viene definito in questo modo:

$\bigcap F = \{X \in A | \forall Y, (Y \in F \Rightarrow X \in Y)\}$ dove $A \in F$

> Preso un qualunque insieme appartenente ad $\bigcap F$, ogni suo elemento appartiene ad ogni altro insieme presente all'interno dell'insieme F.

F non è l'insieme intersezione, ma l'insieme di tutti gli insiemi da intersecare, mentre l'insieme intersezione viene indicato come $\bigcap_{Y \in F} Y$ per esempio con $\bigcap_{Y \in \{A,B,C\}} Y = A \cap B \cap C$.

Assioma dell'unione

$\forall F, \exists X, \forall Z, (Z \in X \iff \exists Y, (Y \in F \wedge Z \in Y))$

L'insieme X viene indicato con $\bigcup F$ o $\bigcup_{Y \in F} Y$.

> Preso un qualunque insieme F di insiemi da unire, esiste un insieme unione X tale per cui per ogni elemento qualsiasi Z, Z appartiene all'insieme unione X se e solo se

> esiste almeno un insieme Y appartenente a F nel quale Z è contenuto

Teorema dell'unione binaria

$\forall A, \forall B, \exists X, \forall Z, (Z \in X \iff Z \in A \vee Z \in B)$

> Per ogni insieme A e B casuali, esiste un insieme X unione dei due insiemi tale per cui per ogni Z, Z appartiene ad A o Z appartiene a B.

Assioma del singoletto

Un **singoletto** è un insieme contenente un unico elemento.

$\forall X, \exists Y, \forall Z, (Z \in Y \iff Z = X)$

> Per ogni insieme X, esiste un insieme singoletto Y che lo contiene tale per cui, per ogni suo elemento Z, Z = X (esiste un solo elemento Z = X).

Abuso di notazione per indicare un insieme

Per indicare un insieme solitamente viene utilizzata la seguente forma:
$\{A_1, ..., A_n\}$

per indicare:

$\{A_1\} \cup ... \cup \{A_n\}$, il quale esiste per i teoremi del singoletti e dell'unione.

Costruzione dei numeri naturali

Per costruire i numeri naturali ci serviamo degli insiemi, definendo l'insieme vuoto come 0 e poi creando i numeri successivi come l'unione tra il numero precedente e l'insieme contenente il numero precedente:

$N + 1 = N \cup \{N\}$

Esempio:

$0 = \emptyset$

$1 = \{\emptyset\}$

$2 = \{\emptyset, \{\emptyset\}\}$

$3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

...

Assioma dell'infinito

$\exists Y, (\emptyset \in Y \wedge \forall N, (N \in Y \wedge N \cup \{N\} \in Y))$

> Esiste un insieme infinito Y il quale contiene l'insieme vuoto e, preso un qualsiasi insieme N, N appartiene a Y e N + 1 appartiene a Y

Assioma dell'insieme potenza

Assioma che asserisce l'esistenza dell'insieme dei sottoinsiemi di un insieme dato.

$\forall X, \exists Y, \forall Z, (Z \in Y \iff Z \subseteq X)$

> Per ogni insieme X esiste un insieme Y dei sottoinsiemi di X tale che, per ogni elemento casuale Z, Z appartiene a Y se e solo se Z è contenuto in X.

Y viene indicato come 2^X oppure $P(X)$ (**insieme potenza** o **insieme delle parti**).

Esempio:

$2^{\{1,2\}} = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$

Assioma di regolarità

Ogni insieme non vuoto possiede almeno un elemento dal quale è disgiunto (due insiemi disgiunti sono due insiemi che non hanno nessun elemento in comune).

Una delle conseguenze di questo assioma è che nessun insieme contiene sè stesso.

Assioma di rimpiazzamento

L'immagine di un insieme rispetto ad una formula che descrive una funzione è sempre un insieme.

In parole povere: tutti gli elementi immagine ricavati tramite una formula che descrive una funzione a partire da un insieme (chiamato in questo caso dominio in quanto parliamo di funzioni) formano sempre un insieme.

▼ **3.3 - Dimostrazioni in teoria assiomatica degli insiemi**

Per ogni ($\forall$)

$\forall$ introduzione

Scopo: per dimostrare $\forall x.P(x)$.

Linguaggio naturale: sia x un insieme fissato; [dimostrazione di P(x)]

Matita: **assume x: set. [dimostrazione di $P(x)$]**.

$\forall$ eliminazione

Scopo: da un'ipotesi o un risultato intermedio $\forall x.P(x)$ possiamo concludere che P valga per una x a nostra scelta.

Matita: **by [NOME_IPOTESI] we proved [CONCLUSIONE] ([NOME_RISULTATO_OTTENUTO])**.

Esiste ($\exists$)

$\exists$ introduzione

Scopo: per dimostrare $\exists x.P(x)$.

Linguaggio naturale: scelgo x e dimostro $P(x)$: [dimostrazione di $P(x)$]

Matita: **by ex_intro, [NOME_IPOTESI_$P(e)$] we proved $\exists x.P(x)$** ($P(e)$ è una sottoprova che dimostra $P(x)$ scegliendo come x un valore e).

$\exists$ eliminazione

Scopo: da un'ipotesi o un risultato intermedio $\exists x.P(x)$ è possibile procedere nella prova utilizzando la x che soddisfa $P(x)$.

Linguaggio naturale: sia x tale che $P(x)$.

Matita: **by [NOME_IPOTESI_$\exists x.P(x)$] let x: set such that $P(x)$ ([NOME_IPOTESI])**.

Implicazione ($\implies$)

$\implies$ introduzione

Scopo: dimostrare $P \implies Q$

Linguaggio naturale: assumo P ([NOME_IPOTESI]). [dimostrazione di Q]

Matita: **suppose P ([NOME_IPOTESI]). [dimostrazione di Q]**.

$\implies$ eliminazione

Scopo: da un ipotesi o un risultato intermedio $P \implies Q$ e da un ipotesi o un risultato intermedio P è possibile concludere che Q vale.

Matita: **by [NOME_IPOTESI_PQ], [NOME_IPOTESI_P] we proved [Q] ([NOME_RISULTATO_OTTENUTO])**.

$\implies$ eliminazione (variante)

Scopo: da un ipotesi o un risultato intermedio $P \implies Q$, per dimostrare Q mi posso ridurre a dimostrare P.

Linguaggio naturale: per $P \implies Q$, per dimostrare Q mi posso ridurre a dimostrare P.

Matita: **we need to prove P ([NOME_IPOTESI_P]). [dimostrazione di P]. by [NOME_IPOTESI_PQ], [NOME_IPOTESI_P] done**.

Se e solo se ($\iff$)

$\iff$ introduzione

Scopo: per dimostrare $P \iff Q$ si dimostra sia $P \implies Q$ che $Q \implies P$.

$\iff$ eliminazione

Scopo: l'ipotesi $P \iff Q$ può essere utilizzata sia come ipotesi $P \implies Q$ che come ipotesi $Q \implies P$.

And ($\wedge$)

$\wedge$ introduzione

Scopo: per dimostrare $P \wedge Q$ si dimostrano sia P che Q.

Matita: **by conj, P, Q we proved $P \wedge Q$ ([NOME_RISULTATO_OTTENUTO])**.

$\wedge$ eliminazione

Scopo: un'ipotesi o un risultato intermedio $P \wedge Q$ può essere usato sia come P che come Q.

Matita: **by [NOME_IPOTESI_$P \wedge Q$] we proved P ([NOME_IPOTESI_P]) and Q ([NOME_IPOTESI_Q])**.

Or ($\vee$)

$\vee$ introduzione

Scopo: per dimostrare $P \vee Q$ basta dimostrare P o Q.

Matita: **by or_introl, [NOME_IPOTESI_P] we proved $P \vee Q$. by or_intror, [NOME_IPOTESI_Q] we proved $P \vee Q$**.

$\vee$ eliminazione

Scopo: per utilizzare un'ipotesi o un risultato intermedio $P \vee Q$, occorre proseguire per casi nella dimostrazione, una volta assumendo che P valga e una volta che Q valga.

Linguaggio naturale: procedo per casi:

- caso in cui valga P (H): [dimostrazione]
- caso in cui valga Q (H): [dimostrazione]

Matita: we proceed by cases on [NOME_IPOTESI_$P \vee Q$] to prove [CONCLUSIONE]:

case or_introl

suppose P (H)

[dimostrazione di [CONCLUSIONE] sotto l'ipotesi H:P]

case or_intror

suppose Q (H)

[dimostrazione di [CONCLUSIONE] sotto l'ipotesi H:Q]

Not (¬)

¬ introduzione

Scopo: per dimostrare $\neg P$ occorre dimostrare $P \implies$ assurdo.

Inoltre, data un ipotesi $\neg P$ e un'altra ipotesi o un risultato intermedio P si conclude l'assurdo.

Assurdo eliminazione

Scopo: se ho dimostrato l'assurdo posso concludere qualsiasi cosa.

Matita: **using (ABSURDUM [NOME_ASSURDO]) done**

Tips

- Tutte le variabili di un enunciato che non sono introdotte da un per ogni o da un esiste si considerano introdotte da dei per ogni (es. l'enunciato n + m = m + n abbrevia ∀n, m. n + m = m + n).
- Tutti gli assiomi sono sempre utilizzabili come prove in qualunque momento.
- A volte occorre esplicitare la conclusione corrente (cosa resta da dimostrare) attraverso "**the thesis becomes** P".
- Per indicare che il lettore è in grado di ricostruire la prova per conto suo combinando le ipotesi si utilizza "**done**".
- $\forall x \in A, P(x)$ viene utilizzato per indicare $\forall x, (x \in A \implies P(x))$.
- $\exists x \in A, P(x)$ viene utilizzato per indicare $\exists x, (x \in A \wedge P(x))$.

▼ **3.4 - Esercizi di dimostrazioni in teoria assiomatica degli insiemi**

```
(* Exercise 1 *)
theorem reflexivity_inclusion: ∀A. A ⊆ A.
 assume A:set
 we need to prove (∀Z. Z ∈ A → Z ∈ A) (ZAtoZA)
  assume Z:set
  suppose (Z ∈ A) (ZA)
  by ZA (* Quale ipotesi serve? Osservate cosa bisogna dimostrare *)
 done
 by ax_inclusion2, ZAtoZA (* Quale ipotesi devo combinare con l'assioma? *)
done
qed.

(* Exercise 2 *)
theorem transitivity_inclusion: ∀A,B,C. A ⊆ B → B ⊆ C → A ⊆ C.
 assume A:set
 assume B:set
 assume C:set
 suppose (A ⊆ B) (AB)
 suppose (B ⊆ C) (BC)
 we need to prove (∀Z. Z ∈ A → Z ∈ C) (ZAtoZC)
  assume Z:set
  suppose (Z ∈ A) (ZA)
  by AB, ax_inclusion1, ZA we proved (Z ∈ B) (ZB)
  by BC, ax_inclusion1, ZB we proved (Z ∈ C) (ZC)(* Osservate bene cosa deve essere dimostrato *)
 done
 by ax_inclusion2, ZAtoZC
done
qed.

(* Exercise 3 *)
theorem antisymmetry_inclusion: ∀A,B. A ⊆ B → B ⊆ A → A = B.
 assume A:set
 assume B:set
 suppose (A ⊆ B) (AB)
 suppose (B ⊆ A) (BA)
 we need to prove (∀Z. Z ∈ A ⇔ Z ∈ B) (P)
  assume Z:set
  by AB, ax_inclusion1 we proved (Z ∈ A → Z ∈ B) (AB')
  by BA, ax_inclusion1 we proved (Z ∈ B → Z ∈ A) (BA')
  by conj, AB', BA'
 done
 by ax_extensionality, P  (* Quale assioma devo utilizzare? *)
```

```
done
qed.

(* Exercise 4 *)
theorem intersection_idempotent_1: ∀A. A ⊆ A ∩ A.
 assume A:set
 we need to prove (∀Z. Z ∈ A → Z ∈ (A ∩ A)) (AinAA)
  assume Z:set
  suppose (Z ∈ A) (ZA)
  we need to prove (Z ∈ A ∧ Z ∈ A) (ZAZA)
   by conj, ZA (* Il teorema conj serve per dimostrare una congiunzione (un "and" ∧) *)
  done
  by ax_intersect2, ZAZA (* Cosa stiamo dimostrando? Che assioma serve? *)
 done
 by ax_inclusion2, AinAA
done
qed.

(* Exercise 5*)
theorem intersect_monotone_l: ∀A,A',B. A ⊆ A' → A ∩ B ⊆ A' ∩ B.
 assume A:set
 assume A':set
 assume B:set
 suppose (A ⊆ A') (AA')
 we need to prove (∀Z. Z ∈ A ∩ B → Z ∈ A' ∩ B) (P)
  assume Z:set
  suppose (Z ∈ A ∩ B) (F)
  by ax_intersect1, F we proved (Z ∈ A ∧ Z ∈ B) (ZAZB)
  by ZAZB we have (Z ∈ A) (ZA) and (Z ∈ B) (ZB) (* Da un'ipotesi congiunzione si ricavano due ipotesi distinte *)
  by ax_inclusion1, AA' we proved (Z ∈ A') (ZA')
  by conj  we proved (Z ∈ A' ∧ Z ∈ B) (ZAZB')
  by ax_intersect2 (* Cosa stiamo dimostrando? Che assioma serve? *)
 done
by ax_inclusion2, P
done
qed.

(* Exercise 6*)
theorem intersect_monotone_r: ∀A,B,B'. B ⊆ B' → A ∩ B ⊆ A ∩ B'.
 assume A:set
 assume B:set
 assume B':set
 suppose (B ⊆ B') (BB')
 we need to prove (∀Z. Z ∈ A ∩ B → Z ∈ A ∩ B') (P)
  assume Z:set
  suppose (Z ∈ A ∩ B) (F)
  by ax_intersect1, F we proved (Z ∈ A ∧ Z ∈ B) (ZAZB)
  by ZAZB we have (Z ∈ A) (ZA) and (Z ∈ B) (ZB)
  by ax_inclusion1, BB' we proved (Z ∈ B') (ZB')
  by conj we proved (Z ∈ A ∧ Z ∈ B') (ZAZB')
  by ax_intersect2
 done
by ax_inclusion2, P
done
qed.
```

```
(* Exercise 7 *)
theorem union_inclusion: ∀A, B. A ⊆ A ∪ B.
  assume A: set
  assume B: set
  we need to prove (∀Z. Z ∈ A → Z ∈ A ∪ B) (I)
    assume Z: set
    suppose (Z∈A) (ZA)
    we need to prove (Z ∈ A ∨ Z ∈ B) (I1)
      by ZA,or_introl
    done
    by ax_union2, I1
  done
  by ax_inclusion2, I done
qed.

(* Exercise 8 *)
theorem union_idempotent: ∀A. A ∪ A = A.
 assume A: set
 we need to prove (∀Z. Z ∈ A ∪ A ⇔ Z ∈ A) (II)
 assume Z: set
  we need to prove (Z ∈ A ∪ A → Z ∈ A) (I1)
```

```
    suspect (Z ∈ A ∪ A)(Zu)
    by ax_union1, Zu we proved (Z ∈ A ∨ Z ∈ A) (Zor)
    we proceed by cases on Zor to prove (Z ∈ A)
     case or_introl
        suppose (Z∈A) (H)
        by H
     done
     case or_intror
        suppose (Z∈A) (H)
        by H
     done
   we need to prove (Z ∈ A → Z ∈ A ∪ A) (I2)
   suppose (Z∈A) (ZA)
    by ZA, or_introl we proved (Z ∈ A ∨ Z ∈ A) (Zor)
    by ax_union2, Zor
   done
   by conj, I1, I2
  done
  by II,ax_extensionality
done
qed.

(* Exercize 9 *)
theorem empty_absurd: ∀X, A. X ∈ ∅ → X ∈ A.
 assume X: set
 assume A: set
 suppose (X ∈ ∅) (XE)
 by ax_empty we proved False (bottom)
 using (ABSURDUM bottom)
done
qed.

(* Exercise 10 *)
theorem intersect_empty: ∀A. A ∩ ∅ = ∅.
 assume A: set
 we need to prove (∀Z. Z ∈ A ∩ ∅ ⇔ Z ∈ ∅) (II)
   assume Z: set
   we need to prove (Z ∈ A ∩ ∅ → Z ∈ ∅) (I1)
     suppose (Z ∈ A ∩ ∅) (Ze)
     we need to prove (Z ∈ ∅)
     by Ze, ax_intersect1 we have (Z ∈ A) (ZA) and (Z∈∅) (ZE)
     by ZE
   done
   we need to prove (Z ∈ ∅ → Z ∈ A ∩ ∅) (I2)
     suppose (Z ∈ ∅) (ZE)
     by ZE, ax_empty we proved False (bottom)
     using (ABSURDUM bottom)
   done
   by I1, I2, conj
 done
 by II, ax_extensionality
done
qed.

(* Exercise 11 *)
theorem union_empty: ∀A. A ∪ ∅ = A.
 assume A: set
 we need to prove (∀Z. Z ∈ A ∪ ∅ ⇔ Z ∈ A) (II)
   assume Z:set
   we need to prove (Z ∈ A → Z ∈ A ∪ ∅) (I1)
     suppose (Z ∈ A) (ZA)
     by or_introl, ZA we proved (Z ∈ A ∨ Z ∈ ∅) (Zor)
     by ax_union2,Zor
   done
   we need to prove (Z ∈ A ∪ ∅ → Z ∈ A) (I2)
     suppose (Z ∈ A ∪ ∅) (Zu)
     by ax_union1, Zu we proved (Z ∈ A ∨ Z ∈ ∅) (Zor)
     we proceed by cases on Zor to prove (Z ∈ A)
      case or_introl
        suppose (Z ∈ A) (H)
        by H done
      case or_intror
        suppose (Z ∈ ∅) (H)
         by ax_empty, H we proved False (bottom)
         using (ABSURDUM bottom)
      done
    by conj, I1, I2
  done
  by ax_extensionality, II
```

```
 done
qed.

(* Exercise 12 *)
theorem union_commutative: ∀A,B. A ∪ B = B ∪ A.
 assume A: set
 assume B: set
 we need to prove (∀Z. Z ∈ A ∪ B ⇔ Z ∈ B ∪ A) (II)
   assume Z: set
   we need to prove (Z ∈ A ∪ B → Z ∈ B ∪ A) (I1)
     suppose (Z ∈ A ∪ B) (ZAB)
     we need to prove (Z ∈ B ∪ A)
     we need to prove (Z ∈ B ∨ Z ∈ A) (I)
       by ZAB, ax_union1 we proved (Z∈A∨Z∈B) (Zor)
       we proceed by cases on Zor to prove (Z ∈ B ∨ Z ∈ A)
       case or_intror
         suppose (Z∈B) (H)
         by H,or_introl
       done
       case or_introl
         suppose (Z∈A) (H)
         by H, or_intror
       done
   by I,ax_union2 done
   we need to prove (Z ∈ B ∪ A → Z ∈ A ∪ B) (I2)
     suppose (Z ∈ B ∪ A) (ZBA)
     we need to prove (Z ∈ A ∪ B)
     we need to prove (Z ∈ A ∨ Z ∈ B) (I)
       by ZBA, ax_union1 we proved (Z∈B∨Z∈A) (Zor)
       we proceed by cases on Zor to prove (Z ∈ A ∨ Z ∈ B)
       case or_intror
         suppose (Z∈A) (H)
         by H,or_introl
       done
       case or_introl
         suppose (Z∈B) (H)
         by H, or_intror
       done
   by I,ax_union2 done
  by I1,I2,conj
 done
 by ax_extensionality,II
done
qed.
```