Appunti di Logica e Fondamenti di Matematica

Francesco Lucibello

17 gennaio 2025

Indice

Premessa

Questi appunti sono relativi al corso di *Logica e Fondamenti di Matematica* del primo semestre dell'anno accademico 2021/22 tenuto dalla professoressa Giuseppina Terzo presso l'università Federico II di Napoli.

Gli appunti riportano tutti gli argomenti trattati durante il corso con diversi livelli di dettaglio, sono anche presenti aggiunte e approfondimenti, osservazioni e dubbi personali che forse risulteranno utili.
I testi consigliati per seguire il corso sono:

- [Dal08]: Logic and Structure di Van Dalen
- [End77]: Elements of Set Theory di Enderton
- [AF14]: Logica di Tortora e Abrusci

Consiglio. Ricorda che molti dei testi pubblicati da Springer possono essere ottenuti gratuitamente in formato PDF se sei studente della Federico II, è sufficiente scaricarli dal sito ufficiale mediante proxy unina.

Capitolo 1

Teoria ZF

Esistono vari sistemi di assiomi che permettono di descrivere la matematica, uno di questi è la Teoria degli insiemi di Zermelo-Fraenkel ed è quello utilizzato in questo corso.

1.1 Linguaggio di ZF

Il linguaggio utilizzato nella teoria ZF è un linguaggio del prim'ordine

1. Infinità numerabile di variabili proposizionali
$$p_1, p_2, \dots$$
2. Connettivi logici
$$\neg, \wedge, \vee, \rightarrow, \longleftrightarrow$$
3. Quantificatori
$$\forall, \exists$$
4. Parentesi
$$(,)$$
servono ad evitare ambiguità
5. Simboli di relazioni binarie
$$\in, =$$

1.2 Assiomi di ZF

Il seguente è l'elenco completo degli assiomi della teoria ZF (non sono tutti indipendenti fra loro, infatti per costruire la teoria non sono tutti necessari).

1. Assioma di estensionalità
2. Assioma dell'insieme vuoto
3. Assioma della coppia non ordinata
4. Assioma dell'unione
5. Assioma dell'insieme delle parti
6. Assioma di separazione
7. Assioma dell'infinito
8. Assioma di rimpiazzamento
9. Assioma di fondazione

Ci sono altri due assiomi "aggiuntivi", che non fanno parte della teoria ZF, sono l'assioma della scelta e l'ipotesi del continuo. Se oltre agli assiomi di ZF si assume anche l'assioma della scelta, la teoria costruita si dice teoria ZFC.
Descriviamo tali assiomi singolarmente (alcuni verranno introdotti in seguito).

Assioma 1.1 (Assioma di estensionalità)**.** *Se due insiemi hanno gli stessi elementi, allora coincidono.*

$$\forall x \forall y (\forall t (t \in x \longleftrightarrow t \in y) \rightarrow x = y)$$

Assioma 1.2 (Assioma dell'insieme vuoto)**.** *Esiste un insieme privo di elementi.*

$$\exists x (\forall y (y \notin x))$$

Osservazione 1.1. L'assioma dell'insieme vuoto garantisce l'esiste di un insieme vuoto (cioè privo di elementi), mentre l'unicità è garantita dall'assioma di estensionalità, quindi è possibile definire *l'insieme vuoto* e denotarlo col simbolo $\varnothing$.

Assioma 1.3 (Assioma della coppia non ordinata)**.** *Dati due insiemi x e y esiste un insieme i cui elementi sono x e y.*

$$\forall x \forall y \exists z (\forall t (t \in z \longleftrightarrow (t = x \vee t = y)))$$

Osservazione 1.2. Dati due insiemi x e y, l'esistenza di un insieme che abbia per elementi x e y è garantito da questo assioma, mentre l'unicità è garantita dall'assioma di estensionalità, quindi è possibile definire l'insieme della *coppia non ordinata* e denotarlo col simbolo $\{x, y\}$.

Assioma 1.4 (Assioma dell'unione - Forma provvisoria)**.** *Dati due insiemi x e y esiste un insieme i cui elementi sono gli elementi di x e di y.*

$$\forall x \forall y \exists z (\forall t (t \in z \longleftrightarrow (t \in x \vee t \in y)))$$

Osservazione 1.3. Puoi definire l'unione ecc col simbolo $x \cup y$

Definizione 1.1 (Inclusione fra insiemi)**.** Siano x e y, si dice che *x è incluso in y* e si scrive $x \subseteq y$ se

$$\forall t (t \in x \rightarrow t \in y)$$

Assioma 1.5 (Assioma dell'insieme delle parti)**.** *Per ogni insieme x esiste un insieme i cui elementi sono i sottoinsiemi di x.*

$$\forall x \exists y (\forall t (t \in y \longleftrightarrow t \subseteq x))$$

Osservazione 1.4. Puoi definire l'insieme delle parti $\mathcal{P}(x)$ ...

Assioma 1.6 (Schema di assiomi di separazione (o assioma di separazione))**.** *Sia P una proprietà, allora per ogni insieme x esiste un insieme i cui elementi sono gli elementi di x che soddisfano P* [1].

$$\forall x \exists y (\forall t (t \in y \longleftrightarrow (t \in x \wedge P(t))))$$

o equivalentemente

Osservazione 1.5. Questo non è realmente un assioma ma uno schema di assiomi (perché abbiamo infinite proprietà P), grazie ad esso, possiamo definire l'insieme $\{t \in x : P(t)\}$

Osservazione 1.6. "L'insieme" del paradosso di Russell non è realmente un insieme secondo questa definizione (infatti nella teoria naive di Cantor era possibile ottenere un insieme data una qualsiasi proprietà, mentre per come abbia scritto l'assioma di separazione abbiamo bisogno sia di una proprietà che di un insieme e quindi l'insieme "naive" $\{x : x \notin X\}$ del paradosso non lo possiamo definire).

Teorema 1.1 (Inesistenza dell'insieme degli insiemi)**.** *Non esiste l'insieme degli insiemi.*

$$\nexists x (\forall y (y \in x))$$

Dimostrazione. Prendiamo un qualsiasi insieme A e dimostriamo che esiste un insieme B che non vi appartiene, di consegeunza non può esistere l'insieme degli insiemi. Sia A un insieme e sia $B = \{x \in A : x \notin x\}$, sia per assurdo che $B \in A$, allora se $B \in B \implies B \notin B$, se $B \notin B \implies B \in B$, un assurdo in entrambi i casi, quindi $B \notin B$. □

[1] Una "proprietà" in ZF è un modo diverso per dire "formula", il concetto di "formula soddisfacibile", verrà introdotto molto più avanti, quindi per adesso pensala intuitivamente, però sappi che c'è una giustificazione formale di tutto questo

Definizione 1.2 (Intersezione fra insiemi)**.** Siano x e y insiemi, si definisce

$$x \cap y \coloneqq \{t \in x \cup y : t \in x \wedge t \in y\} = \{t \in x : t \in y\} = \{t \in y : t \in x\}$$

Definizione 1.3 (Sottrazione tra insiemi)**.** Siano x e y insiemi, si definisce

$$x \backslash y \coloneqq \{t \in x : t \notin y\}$$

Assioma 1.7 (Assioma dell'unione - Forma definitiva)**.** *Dato un insieme x, esiste un insieme y i cui elementi sono gli elementi degli elementi di x.*

$$\forall x \exists y (\forall t (t \in y \longleftrightarrow \exists z (z \in x \wedge t \in z)))$$

Definizione 1.4 (Unione di un insieme)**.** Sia a un insieme, si definisce la sua unione l'insieme i cui elementi sono gli elementi degli elementi di x e si denota $\cup a$.

Osservazione 1.7. Informalmente puoi scrivere che

$$\bigcup a = \{x : \exists t (t \in a \wedge x \in t)\}$$

ma per come scritto non è un insieme, quello che garantisce l'esistenza e unicità sono gli assiomi dell'unione e di estensionalità (si potrebbe anche esplicitare, sul libro ci sta ma non è difficile).

Definizione 1.5 (Intersezione di un insieme)**.** Sia a un insieme, si definisce la sua intersezione

$$\bigcap a \coloneqq \left\{x \in \bigcup a : \forall t (t \in a \to x \in t)\right\}$$

Definizione 1.6 (Coppia ordinata)**.** Siano a e b insiemi, si definisce la coppia ordinata

$$\langle a, b \rangle \coloneqq \{\{a\}, \{a, b\}\}$$

Osservazione 1.8. Si potrebbe pensare ad una definizione più intuitiva del tipo $\{a, \{a, b\}\}$ ma questa fallisce per $\langle \varnothing, \{\varnothing\} \rangle$ e $\langle \{\{\varnothing\}\}, \varnothing \rangle$

Teorema 1.2 (Uguaglianza fra coppie ordinate)**.** *Siano u, v, x, y insiemi, si ha*

$$\langle u, v \rangle = \langle x, y \rangle \iff u = x \wedge v = y$$

Definizione 1.7 (Prodotto cartesiano)**.** Siano A e B insiemi, si definisce il *prodotto cartesiano di A e B*

$$A \times B \coloneqq \{w \in \mathcal{P}(\mathcal{P}(A \cup B)) : \exists x \exists y (x \in A \wedge y \in B \wedge w = \langle x, y \rangle)\} = \{\langle x, y \rangle \in \mathcal{P}(\mathcal{P}(A \cup B)) : x \in A \wedge y \in B\}$$

La seconda scrittura è leggermente meno formale della prima, ma è di più semplice lettura.

1.3 Relazioni

Definizione 1.8 (Relazione)**.** Un insieme di coppie ordinate si dice *relazione*.

La prof definisce così una relazione binaria (il libro invece fa una distinzione [End77, p. 40, 42]).

Osservazione 1.9. Uno si può chiedere (e si deve chiedere, altrimenti la definizione non è ben posta), se dato un insieme so dire se è una relazione o no, in altre parole, so dire se i suoi elementi sono coppie ordinate? Io credo che un insieme può essere sempre considerato una relazione, infatti se ho un insieme x, puoi dimostrare (CREDO) che $x \subseteq \mathcal{P}(\mathcal{P}(\bigcup \bigcup x))$, questo significa che ogni elemento di x è una coppia ordinata dell'insieme $\bigcup \bigcup x$. Forse mi sto sbagliando perché dopo c'è (Proprietà 1.4), pensaci.

Definizione 1.9 (Elementi in relazione)**.** Sia R una relazione e siano x, y insiemi tali che $\langle x, y \rangle \in R$, allora si dice che *$x$ è in relazione con y* e si scrive xRy

Lemma 1.3. *Siano A, x, y insiemi tali che $\langle x, y \rangle \in A$, allora $x, y \in \bigcup \bigcup A$.*

Definizione 1.10 (Dominio di un insieme)**.** Sia R un insieme si dice *dominio di R* l'insieme

$$\operatorname{dom} R \coloneqq \left\{x \in \bigcup \bigcup R : \exists y (\langle x, y \rangle \in R)\right\}$$

Definizione 1.11 (Rango di un insieme)**.** Sia R un insieme si dice *rango di R* l'insieme

$$\operatorname{ran} R \coloneqq \left\{x \in \bigcup \bigcup R : \exists y (\langle y, x \rangle \in R)\right\}$$

Definizione 1.12 (Campo di un insieme)**.** Sia R un insieme si dice *campo di R* l'insieme

$$\operatorname{fld} R := \operatorname{dom} R \cup \operatorname{ran} R$$

Definizione 1.13 (n-upla)**.** Definiamo per ricorrenza

$$\langle x_1, \dots, x_n \rangle = \langle \langle x_1, \dots, x_{n-1} \rangle, x_n \rangle$$

Proprietà 1.4 (Caratterizzazione relazione)**.** *Sia A un insieme, allora A è una relazione sse* $A \subseteq \operatorname{dom} A \times \operatorname{ran} A$

Definizione 1.14 (Relazione binaria su un insieme)**.** Sia A un insieme, un sottoinsieme di $A \times A$ si dice *relazione binaria su A*.

Definizione 1.15 (Funzione)**.** Sia F una relazione tale che per ogni $x \in \operatorname{dom} F$ esiste un unico y tale che $\langle x, y \rangle \in F$, allora F si dice *funzione*.

$$\forall x \forall y \forall y' ((\langle x, y \rangle \in F \wedge \langle x, y' \rangle \in F) \to y = y')$$

Definizione 1.16 (Funzione da un insieme ad un altro)**.** Sia F una funzione e siano A, B insiemi tali che $\operatorname{dom} F = A$ e $\operatorname{ran} F \subseteq B$, allora si dice che F va da A in B e si scrive $F : A \to B$.

Definizione 1.17 (Immagine di un elemento mediante una funzione)**.** Sia F una funzione e sia $x \in \operatorname{dom} F$, allora l'unico elemento y tale che xFy, si dice *immagine di x mediante F* e si denota $F(x)$.

Definizione 1.18 (Funzione iniettiva)**.** Sia F una funzione, se per ogni $x \in \operatorname{ran} F$ esiste un unico y tale che $F(y) = x$, allora la funzione F si dice *iniettiva*.

$$\forall x \forall y \forall y' ((yFx \wedge y'Fx) \to y = y')$$

Definizione 1.19 (Funzione suriettiva)**.** Siano A e B insiemi e $F : A \to B$ una funzione, se per ogni $x \in B$ esiste y tale che yFx, allora la funzione F si dice *suriettva*.

$$\forall x (x \in B \to \exists y (yFx))$$

Equivalentemente $\operatorname{ran} F = B$.

Definizione 1.20 (Funzione biettiva)**.** Siano A e B insiemi e $F : A \to B$ una funzione, se F è sia iniettiva che biettiva, allora F si dice *biettiva*.

Le seguenti definizione vengono date per un qualsiasi insieme ma solitamente vengono utilizzate per le funzioni.

Definizione 1.21 (Inverso di un insieme)**.** Sia F un insieme, si dice *inverso di F*, l'insieme

$$F^{-1} := \left\{ \langle y, x \rangle \in \mathcal{P}\left(\mathcal{P}\left(\bigcup\bigcup F\right)\right) : xFy \right\} = \{ \langle y, x \rangle \in \operatorname{ran} A \times \operatorname{dom} A : \langle x, y \rangle \in F \}$$

Osservazione 1.10. L'esistenza ed unicità sono garantite rispettivamente dagli assiomi di separazione e di estensionalità.

Osservazione 1.11. Nota che se F è una relazione, allora F^{-1} è la relazione inversa e che se F è una funzione iniettiva allora F^{-1} è una funzione iniettiva.

Definizione 1.22 (Composizione di insiemi)**.** Siano F e G insiemi, si definisce la composizione di F e G come l'insieme

$$F \circ G := \{ \langle x, z \rangle \in \operatorname{dom} G \times \operatorname{ran} F : \exists y (xGy \wedge yFz) \}$$

Definizione 1.23 (Restrizione di insieme ad un altro)**.** Siano F e A insiemi, si definisce la restrizione di F ad A l'insieme

$$F|_A := \{ \langle x, y \rangle \in \operatorname{dom} F \times \operatorname{ran} F : xFy \wedge x \in A \} = \{ \langle x, y \rangle \in A \times \operatorname{ran} F : xFy \}$$

Osservazione 1.12. Nel caso in cui F è una relazione puoi scrivere più brevemente

$$F|_A = \{ \langle x, y \rangle \in F : x \in A \}$$

Definizione 1.24 (Immagine di un insieme mediante un altro)**.** Siano F e A insiemi, si definisce *l'immagine di A mediante F* l'insieme

$$F[A] := \operatorname{ran} F|_A = \{ x \in \bigcup\bigcup F|_A : \exists y (yFx) \} = \{ x \in \bigcup\bigcup F : x \in A \wedge \exists y (yFx) \}$$

Definizione 1.25 (Relazione riflessiva)**.** Sia R una relazione, si dice che R *è riflessiva* se

$$\forall x(x \in \operatorname{fld} R \to xRx)\,,$$

cioè

$$\operatorname{diag} A \subseteq R$$

Definizione 1.26 (Relazione riflessiva su un insieme)**.** Siano A un insieme e R una relazione, si dice che R *è riflessiva su* A se

$$\forall x(x \in A \to xRx)\,,$$

cioè

$$\operatorname{diag} A \subseteq R$$

Definizione 1.27 (Relazione simmetrica)**.** Sia R una relazione, se per ogni x, y tali che xRy si ha che yRx, allora R si dice *simmetrica*.

$$\forall x \forall y(xRy \to yRx)$$

Definizione 1.28 (Relazione transitiva)**.** Sia R una relazione, se per ogni x, y, z tali che xRy e yRz si ha che xRz, allora R si dice *transitiva*.

$$\forall x \forall y \forall z((xRy \wedge yRz) \to xRz)$$

Definizione 1.29 (Relazione di equivalenza)**.** Sia R una relazione, se R è riflessiva, simmetrica e transitiva, allora R si dice *relazione di equivalenza*.

Definizione 1.30 (Relazione di equivalenza su un insieme)**.** Sia A un insieme e sia R una relazione binaria su A, se R è riflessiva su A, simmetrica e transitiva, allora R si dice *relazione di equivalenza su* A.

Esempio 1.1 (Esempio di relazione di equivalenza che non è una relazione di equivalenza su un insieme). L'insieme vuoto è una relazione di equivalenza ma non è una relazione di equivalenza su qualsiasi insieme non vuoto.

Lemma 1.5. *Sia R una relazione, allora R è una relazione binaria su* $\operatorname{fld} R$.

Proprietà 1.6. *Sia R una relazione, allora* $R \subseteq \operatorname{dom} R \times \operatorname{ran} R \subseteq \operatorname{fld} R \times \operatorname{fld} R$.

Proprietà 1.7. *Siano A un insieme e sia R una relazione binaria su A, allora* $\operatorname{fld} R \subseteq A$.

Teorema 1.8. *Sia R una relazione simmetrica e transitiva, allora R è una relazione di equivalenza su* $\operatorname{fld} R$.

Osservazione 1.13. Nota che se hai che R è una relazione binaria su A tale che R è simmetrica e transitiva, non è detto che R sia una relazione di equivalenza su A, perché abbiamo osservato (Proprietà 1.7) che in generale $\operatorname{fld} R \neq A$.

Proprietà 1.9. *Sia R una relazione simmetrica, allora* $\operatorname{dom} R = \operatorname{ran} R = \operatorname{fld} R$.

Dimostrazione. Sia $x \in \operatorname{dom} R$, allora esiste y tale che xRy, ma per la simmetria si ha yRx, allora $x \in \operatorname{ran} R$, quindi $\operatorname{dom} R \subseteq \operatorname{ran} R$. Analogamente si vede che $\operatorname{ran} R \subseteq \operatorname{dom} R$, per cui $\operatorname{dom} R = \operatorname{ran} R = \operatorname{fld} R$. □

Proprietà 1.10. *Siano A un insieme e sia R una relazione riflessiva su A, allora* $A = \operatorname{fld} R$.

Dimostrazione. Per (Proprietà 1.7), si ha che $\operatorname{fld} R \subseteq A$. Sia $a \in A$, allora aRa e $a \in \operatorname{dom} R \cap \operatorname{ran} R \subseteq \operatorname{dom} R \subseteq \operatorname{fld} R$, quindi $A \subseteq \operatorname{fld} R$. □

Proprietà 1.11. *Sia R una relazione, allora*

$$R = \varnothing \iff \operatorname{dom} R = \varnothing \iff \operatorname{ran} R = \varnothing$$

Dimostrazione. Sia $R = \varnothing$, se per assurdo $\operatorname{dom} R \neq \varnothing$, allora esiste $x \in \operatorname{dom} R$ e y tali che $\langle x, y\rangle \in R = \varnothing$ ↯.

Sia $\operatorname{dom} R = \varnothing$, se fosse per assurdo $R \neq \varnothing$, allora esiste $\langle x, y\rangle \in R$ e $x \in \operatorname{dom} R = \varnothing$ ↯. □

Corollario 1.11.1. *Siano A un insieme e sia R una relazione riflessiva su A, allora*

$$A = \varnothing \iff R = \varnothing$$

Dimostrazione. Se $A = \varnothing$, allora, per le proprietà precedenti, $\operatorname{dom} R \subseteq \operatorname{fld} R \subseteq A = \varnothing$, allora $R = \varnothing$.

Sia $R = \varnothing$, allora $\operatorname{dom} R = \operatorname{ran} R = \varnothing$ e $\operatorname{fld} R = \varnothing$, ma per (Proprietà 1.10) $A = \operatorname{fld} R = \varnothing$. □

Definizione 1.31 (Classe di equivalenza)**.** Sia R una relazione di equivalenza, per ogni $x \in \operatorname{fld} R$ si dice *classe di equivalenza di x modulo R* l'insieme

$$[x]_R \coloneqq \{y \in \operatorname{fld} R : xRy\}$$

Osservazione 1.14. Nota che vale anche

$$[x]_R = \{y \in \operatorname{dom} R : yRx\} = \{y \in \operatorname{ran} R : xRy\}$$

Osservazione 1.15. Nota che se A è non vuoto, per ogni $a \in A$ si ha aRa, quindi $a \in [a]_R \neq \varnothing$.

Lemma 1.12. *Siano A un insieme e R una relazione di equivalenza su A, siano $x, y \in A$, allora*

$$xRy \iff [x]_R = [y]_R$$

Definizione 1.32 (Partizione di un insieme)**.** Sia A un insieme e sia Π un insieme di insiemi non vuoti tale che l'unione dei suoi elementi sia A e che suoi elementi distinti siano disgiunti.

$$\forall x(x \in \Pi \to x \neq \varnothing) \wedge \bigcup \Pi = A \wedge \forall x \forall y((x \in \Pi \wedge y \in \Pi) \to (x = y \vee x \cap y = \varnothing))$$

Osservazione 1.16. Nota che l'unica partizione del vuoto è il vuoto.

Definizione 1.33 (Insieme quoziente)**.** Siano A un insieme e R una relazione di equivalenza su A, allora si dice *insieme quoziente di A modulo R* l'insieme

$$A/R \coloneqq \{[x]_R \in \mathcal{P}(A) : x \in A\}$$

Lemma 1.13. *Siano A un insieme e R una relazione di equivalenza su A, allora l'insieme quoziente A/R è una partizione di A.*

Definizione 1.34 (Applicazione canonica)**.** Siano A un insieme e R una relazione di equivalenza su A, l'applicazione $\varphi : A \to A/R$ tale che $a \mapsto [a]_R$ è una funzione chiamata *applicazione canonica*.

Osservazione 1.17. Puoi scrivere anche

$$\varphi = \{\langle x, y\rangle \in A \times \mathcal{P}(A) : y = [x]_R\}$$

Definizione 1.35 (Relazione antiriflessiva su un insieme)**.** Siano A un insieme e sia R una relazione binaria su A tale che per ogni $x \in A$ si ha $x \not R x$ allora R si dice *relazione antiriflessiva su A*.

Definizione 1.36 (Relazione asimmetrica)**.** Sia R una relazione, se per ogni x e y tali che xRy e yRx si ha $x = y$, allora R si dice *relazione asimmetrica*.

$$\forall x \forall y((xRy \wedge yRx) \to x = y)$$

Definizione 1.37 (Relazione d'ordine stretto su un insieme)**.** Siano A un insieme e sia R una relazione binaria su A tale che R è antiriflessiva su A e transitiva, allora R si dice *relazione di ordine stretto su A*.

Definizione 1.38 (Relazione d'ordine largo su un insieme)**.** Siano A un insieme e sia R una relazione binaria su A tale che R è riflessiva su A, asimmetrica e transitiva, allora R si dice *relazione d'ordine largo su A*.

Definizione 1.39 (Diagonale di un insieme)**.** Sia A un insieme si definisce la *diagonale di A* l'insieme

$$\operatorname{diag} A \coloneqq \{\langle x, y\rangle \in A \times A : x = y\}$$

Proposizione 1.14. *Siano A un insieme e sia R una relazione d'ordine stretto, allora $R' = R \cup \operatorname{diag} A$ è una relazione di ordine largo.*

Definizione 1.40 (Relazione di ordine totale, relazione di ordine parziale)**.** Siano A un insieme e $<$ una relazione d'ordine su A, allora $<$ si dice anche una *relazione d'ordine parziale*. Se per ogni $x, y \in A$ si ha $x < y \vee y < x \vee x = y$, allora $<$ si dice *relazione d'ordine totale*.

$$\forall x \forall y((x \in A \wedge y \in A) \to (x = y \vee x < y \vee y < x))$$

Definizione 1.41 (Insieme ordinato)**.** Sia A un insieme e $<_A$ una relazione d'ordine su A, allora la coppia ordinata $\langle A, <_A\rangle$ si dice *insieme ordinato* o *struttura d'ordine*.

Definizione 1.42 (Insieme totalmente/parzialmente ordinato)**.** Sia $\langle A, <\rangle$ un insieme ordinato, se $<$ è una relazione d'ordine totale su A si dice che $\langle A, <\rangle$ è un *insieme totalmente ordinato*, se $<$ è una relazione d'ordine parziale, allora $\langle A, <\rangle$ si dice *insieme parzialmente ordinato*.

Notazione 1.43 (Abbreviazione insieme ordinato)**.** Sia A un insieme, dire che A è un insieme ordinato, è un'abbreviazione per indicare che esiste una relazione d'ordine (che implicitamente denotiamo con $<$) su A.

Definizione 1.44 (Elemento minimale, elemento massimale)**.** Sia A un insieme ordinato e sia $x \in A$, se

$$\forall y(y \in A \rightarrow (y < x \rightarrow y = x))$$

allora x si dice *elemento minimale* di A. Se invece

$$\forall y(y \in A \rightarrow (x < y \rightarrow y = x))$$

allora x si dice *elemento massimale* di A.

Definizione 1.45 (Elemento minimo, elemento massimo)**.** Sia A un insieme ordinato e sia $x \in A$, se

$$\forall y(y \in A \rightarrow (y = x \vee x < y))$$

allora x si dice *minimo* di A.

Se invece

$$\forall y(y \in A \rightarrow (y = x \vee y < x))$$

allora x si dice *massimo* di A.

Osservazione 1.18. Se esiste il minimo o il massimo esso è unico.

Definizione 1.46 (Relazione d'ordine indotta)**.** Sia $\langle A, <_A\rangle$ un insieme ordinato e sia $B \subseteq A$, si dice *relazione d'ordine indotta da A su B*, la relazione d'ordine $<_B = <_A \cap B \times B$.

Osservazione 1.19. Devi dimostrare che $<_B$ è una relazione d'ordine su B.

Proprietà 1.15. *Si può definire il minimo di un sottoinsieme B di un insieme ordinato $\langle A, <_A\rangle$, mediante la relazione relazione d'ordine indotta da A su B.*

Definizione 1.47 (Minorante/maggiorante per un sottoinsieme)**.** Siano A un insieme ordinato e $B \subseteq A$ e sia $x \in A$, se

$$\forall y(y \in B \rightarrow (x = y \vee x < y))$$

allora si dice che *x è minorante per B*.

Se invece

$$\forall y(y \in B \rightarrow (x = y \vee y < x))$$

allora si dice che *x è maggiorante per B*.

Definizione 1.48 (Insieme inferiormente limitato, insieme superiormente limitato)**.** Siano A un insieme ordinato e $B \subseteq A$, se esistono dei minoranti/maggioranti per B, allora B si dice inferiormente/superiormente limitato.

Definizione 1.49 (Estremo superiore, estremo inferiore)**.** Siano A un insieme ordinato e $B \subseteq A$ se esistono, si dicono *estremo superiore di B* il minimo dei maggioranti di B e *estremo inferiore di B* il massimo dei minoranti di B.

Definizione 1.50 (Segmento iniziale di un insieme, segmento finale di un insieme)**.** Sia A un insieme ordinato, un sottoinsieme $S \subseteq A$ di A si dice segmento iniziale di A se

$$\forall x \forall y((x \in S \wedge y \in A) \rightarrow (y < x \rightarrow y \in S))$$

Osservazione 1.20. In parole povere puoi dire che S è segmento iniziale di A se per ogni $x \in S$ S contiene tutti gli elementi di A più piccoli di x. Nota che in generale la relazione d'ordine è parziale, quindi ci potrebbero essere elementi non confrontabili (e quindi per definizione S non deve per forza contenerli).

Osservazione 1.21. Per ogni insieme A esistono sempre i segmenti iniziali e finali di A banali $\varnothing, A$.

Definizione 1.51 (Segmento iniziale proprio)**.** Sia A un insieme ordinato, un segmento iniziale di A strettamente contenuto in A si dice *segmento iniziale proprio di A*.

Definizione 1.52 (Segmento iniziale aperto/chiuso determinato da un elemento di un insieme ordinato)**.** Sia A un insieme ordinato e sia $a \in A$, si dice *segmento iniziale aperto di A determinato da a* l'insieme

$$S_a(A) = \{y \in A : y \neq a \wedge y < a\}$$

e si dice *segmento iniziale chiuso di A determinato da a* l'insieme

$$S_a(A) = \{y \in A : y = a \vee y < a\}$$

Si denoterà con *segmento iniziale determinato da a* il segmento iniziale aperto determinato da a.

Osservazione 1.22. Nota che per le definizioni che abbiamo dato sia il segmento iniziale aperto determinato da un elemento che quello chiuso sono segmenti iniziali, ma in generale si ha che quello aperto è sempre proprio e quello chiuso è sempre non vuoto.

Esempio 1.2 (Segmento iniziale non determinato da nessun elemento). Un segmento iniziale proprio di un insieme non è necessariamente determinato da un elemento di quell'insieme.

Basta considerare $\{x \in \mathbb{Q} : x < \sqrt{2}\}$ che è un sottoinsieme di $\mathbb{Q}$ non determinato da nessun elemento.

Definizione 1.53 (Relazione di buon ordine)**.** Una relazione d'ordine su A si dice di buon ordine se per ogni sottoinsieme non vuoto di A esiste minimo (mediante relazione d'ordine indotta).

Definizione 1.54 (Insieme ben ordinato)**.** Ogni sottoinsieme non vuoto di A possiede minimo

Osservazione 1.23. Se A è un insieme ben ordinato e se B è un suo sottoinsieme, allora anche B è ben ordinato.

Proprietà 1.16. *Ogni relazione di buon ordine su un insieme è una relazione di ordine totale su quell'insieme. ma non è vero il viceversa. Ad esempio $(\mathbb{R}, <)$ non è ben ordinato ma è ordinato totalmente.*

Definizione 1.55 (Similitudine, insiemi simili)**.** Siano $\langle A, <_A\rangle, \langle B, <_B\rangle$ due insiemi ordinati, un'applicazione $\varphi : A \to B$ si dice *similitudine* se è biunivoca e tale che

$$x <_A y \iff \varphi(x) <_B \varphi(y), \quad \forall\, x, y \in A$$

Osservazione 1.24. Osserva che la similitudine induce una relazione di equivalenza fra insiemi, come l'equipotenza. Infatti un insieme è simile a sé stesso, se un insieme è simile ad un altro basta considerare la "similitudine inversa" e ho che il secondo insieme è simile al primo e poi vale anche la proprietà transitiva. Sì però nota che questa non è una relazione di equivalenza su un insieme (perché non esiste l'insieme degli insiemi in ZF), però è comunque una relazione di equivalenza (ma non l'abbiamo definita).

Teorema 1.17 (Segmenti iniziali propri di un insieme ben ordinato)**.** *I segmenti iniziali propri di un insieme ben ordinato sono tutti e soli i segmenti iniziali determinati da un elemento dell'insieme.*

Definizione 1.56 (Insieme dei segmenti propri iniziali di un insieme)**.** Sia A insieme ordinato si definisce

$$S_A \coloneqq \{S_x(A) \in \mathcal{P}(A) : x \in A\}$$

Definizione 1.57 (Relazione d'ordine su S_A)**.** Sia $\langle A, <\rangle$ un insieme ordinato, allora si può definire la relazione d'ordine su S_A

$$R = \{\langle x, y\rangle \in S_A \times S_A : x \subset y\}$$

Denotiamo l'insieme ordinato $\langle S_A, R\rangle$ più semplicemente con $\langle S_A, \subset\rangle$.

Lemma 1.18. *Sia $\langle A, <\rangle$ un insieme totalmente ordinato, allora per ogni $x, y \in A$ si ha*

$$S_x(A) \subset S_y(A) \iff x < y$$

e quindi la relazione d'ordine su S_A coincide con

$$\{\langle x, y\rangle \in S_A \times S_A : x \subset y\} = \{\langle S_x(A), S_y(A)\rangle \in S_A \times S_A : x < y\}$$

Teorema 1.19 (Un insieme bene ordinato è simile all'insieme dei segmenti iniziali determinati dai suoi elementi)**.** *Sia A un insieme bene ordinato, gli insiemi ordinati $\langle A, <_A\rangle, \langle S_A, \subset_A\rangle$ sono simili e la similitudine è*

$$\varphi : x \in A \mapsto S_x(A) \in S_A$$

è ben definita perché è sottoinsieme di $A \times S_A$.

Osservazione 1.25. Basta solo che l'insieme sia totalmente ordinato, però la prof lo enuncia così.

Capitolo 2

Calcolo proposizionale

Il calcolo proposizionale, anche detto logica di ordine zero, si interessa delle proposizioni a cui si può dare una risposta "vero" o "falso", quindi ci sono delle proposizioni a cui il calcolo proposizionale non sa rispondere, ad esempio

$$x \cdot y \text{ è pari}$$

che ne so io chi sono x e y? Devono essere determinati affinché si possa dare una risposta.

2.1 Linguaggio del calcolo proposizionale

Il calcolo proposizionale utilizza i seguenti simboli

1. Infinità numerabile di variabili proposizionali

   $$p_1, p_2, \dots$$

2. Connettivi logici

   $$\neg, \wedge, \vee, \rightarrow, \longleftrightarrow$$

3. Parentesi

   $$(,)$$

   servono a spiegare meglio il concetto

4. Formule ben formate

   Sia $\mathcal{F}$ il più piccolo insieme di formule tale che

   (a) Ogni variabile proposizionale è una formula

   (b) Due formule legate da connettivi logici sono una formula
   Siano $\alpha, \beta \in \mathcal{F}$, allora

   $$(\neg\alpha), (\neg\beta), (\alpha \wedge \beta), (\alpha \vee \beta), (\alpha \rightarrow \beta), (\alpha \longleftrightarrow \beta) \in \mathcal{F}$$

   E' la chiusura dell'insieme delle variabili proposizionali per connettivi logici.

Definizione 2.1 (Formula)**.** Una sequenza finita di simboli del linguaggio chiusa per connettivi logici.

Osservazione 2.1. Non tutte le sequenze finite di simboli sono formule, infatti:

$$p_3 \neg\neg p_1 \rightarrow$$

non è una formula.

Esempio 2.1 (Utilizzo delle parentesi). Siano p_1, p_2, p_3, p_4 variabili proposizionali e consideriamo le seguenti formule

$$\begin{aligned} (p_1 \wedge p_2) \vee p_3 &\neq p_1 \wedge (p_2 \vee p_3) \\ (\neg p_1) \wedge p_2 &\neq \neg(p_1 \wedge p_2) \\ (p_1 \wedge p_2) \rightarrow (p_3 \wedge p_4) &\neq p_1 \wedge (p_2 \rightarrow p_3) \wedge p_4 \end{aligned}$$

da cui risulta chiara l'importanza delle parentesi, anche se, nei casi in cui non sono presenti ambiguità, le parentesi possono essere omesse.

Nota che questi esempi sono più "evidenti", ma vale anche

$$(p_1 \wedge p_2) \wedge p_3 \neq p_1 \wedge (p_2 \wedge p_3),$$

cosa significa questo? Che non vale la proprietà associativa di $\wedge$? Per come l'abbiamo sempre intesa "intutivamente" vale, ma non nel calcolo proposizionale, cioè come ho scritto quelle due formule sono diverse ma non il loro "significato". Cioè noi dimostremo che quelle due formule sono "logicamente equivalenti" (che vuol dire che hanno lo stesso "significato"), però formalmente restano due cose diverse. Da cui deriva l'importanza delle parentesi, anche dopo quando parleremo di sottoformule, nota che $p_1 \wedge p_2$ è una sottoformula della prima formula ma non della seconda!

Definizione 2.2 (Sottoformula)**.** Sia α una formula e sia β una formula tale che $\alpha = \beta$ o α si può ottenere da β mediante altre formule e connettivi logici, allora β si dice *sottoformula di* α.

Poiché sappiamo che le formule sono una sequenza finita, tale definizione è ben posta, inoltre una formula α può essere vista come un "diagramma ad albero", dove sono presenti tutte le sottoformule di α che, legate per connettivi logici, seguendo il diagramma, formano α.

Definizione 2.3 (Complessità di una formula (definizione intuitiva))**.** Ad ogni formula è associabile un numero naturale che è detto complessità della formula, essa corrisponde "al numero di sottoformule in cui si può decomporre", se pensi al diagramma descritto prima, corrisponde alla sua "profondità".

In calcolo proposizionale, data una una formula e, scelta una valutazione, si associa ad essa un unico valore fra i due possibili: vero o falso. Esistono altre "logiche" che associano più valori.

Definizione 2.4 (Funzione valutazione)**.** Sia $v : P \to \{0,1\}$ una funzione, allora si dice *funzione valutazione* o *valutazione*.

Dove P è l'insieme delle variabili proposizionali (sì però non l'abbiamo definito).

Proprietà 2.1 (Estensione di una funzione valutazione)**.** *Una funzione di valutazione si può estendere a tutte le formule come*

$$\overline{v} : \mathcal{F} \to \{0,1\}$$

che è tale che $\overline{v}(p) = v(p)\ \forall\, p \in P$ *e* $\forall\, \varphi, \psi \in \mathcal{F}$ *si ha*

1. $$\overline{v}(\neg\varphi) = \begin{cases} 1, & \text{se } \overline{v}(\varphi) = 0 \\ 0, & \text{altrimenti} \end{cases}$$

2. $$\overline{v}(\varphi \wedge \psi) = \begin{cases} 1, & \text{se } \overline{v}(\varphi) = 1 \wedge \overline{v}(\psi) = 1 \\ 0, & \text{altrimenti} \end{cases}$$

3. $$\overline{v}(\varphi \vee \psi) = \begin{cases} 1, & \text{se } \overline{v}(\varphi) = 1 \vee \overline{v}(\psi) = 1 \\ 0, & \text{altrimenti} \end{cases}$$

4. $$\overline{v}(\varphi \to \psi) = \begin{cases} 1, & \text{se } \overline{v}(\varphi) = 0 \vee \overline{v}(\varphi) = 1 \wedge \overline{v}(\psi) = 1 \\ 0, & \text{altrimenti} \end{cases}$$

5. $$\overline{v}(\varphi \longleftrightarrow \psi) = \begin{cases} 1, & \text{se } \overline{v}(\varphi) = \overline{v}(\psi) \\ 0, & \text{altrimenti} \end{cases}$$

Osservazione 2.2. Nota che $\overline{v}(\varphi \longleftrightarrow \psi) = \overline{v}((\varphi \to \psi) \wedge (\psi \to \varphi))$.

Proprietà 2.2 (Identificazione di una funzione di valutazione con una sua estensione)**.** *Data una valutazione* v *esiste un'unica valutazione* $\overline{v}$*, quindi si posso identificare*

Definizione 2.5 (Formula soddisfacibile)**.** Una formula α si dice *soddisfacibile* se esiste una valutazione v tale che $v(\alpha) = 1$.

Definizione 2.6 (Funzione di verità)**.** Sia $\alpha = \alpha(p_1, \ldots, p_n)$ una formula che dipende da n variabili proposizionale, per ogni $x = (x_1, \ldots, x_n) \in \{0,1\}^n$ sia v valutazione tale che $v(p_i) = x_i \ \forall i \in \{1, \ldots, n\}$, allora si definisce la *funzione di verità di* α $f_\alpha : \{0,1\}^n \to \{0,1\}$

$$f_\alpha(x) = v(\alpha)\,.$$

Tale definizione è ben posta per la definizione iterativa di valutazione, in quanto due valutazioni che coincidono su n variabili proposizionali coincidono su qualsiasi formula con quelle variabili proposizionali.

Proprietà 2.3 (Determinabilità della soddisfacibilità di una formula)**.** *E' possibile determinare se una formula di n variabili proposizionali è soddisfacibile in un numero finito di passi.*

Dimostrazione. Una formula $\alpha = \alpha(p_1, \ldots, p_n)$ che dipende da n variabili proposizionali è soddisfacibile se e solo se esiste $x \in \{0,1\}^n$ tale che $f_\alpha(x) = 1$ e, poiché esistono 2^n combinazioni possibili dei valori di verità delle proposizioni (combinazioni di 0 e 1) e α essendo una formula è una sequenza finita di variabili proposizionali e connettivi logici, è possibile calcolare in un numero finito di passi $f_\alpha(x) \ \forall\, x \in \{0,1\}^n$, da cui si determina la soddisfacibilità di α. □

Osservazione 2.3. Nota che la tavola di verità è solo una rappresentazione della funzione di verità.

Consiglio. Può essere utile esercitarsi con il calcolo della tavola di verità di una data proposizione.

Definizione 2.7 (Tautologia o formula logicamente valida)**.** Una formula f si dice *tautologia* o *formula logicamente valida* se per ogni valutazione v si ha $v(f) = 1$

Definizione 2.8 (Contraddizione)**.** Una formula f si dice *contraddizione* se $\neg f$ è una tautologia.

Notazione 2.9. Sia v una valutazione e α una formula, allora la notazione

$$v \models \alpha$$

significa

$$v(\alpha) = 1$$

Notazione 2.10 (Tautologia)**.** Sia α una formula, la notazione

$$\models \alpha$$

significa che α è una tautologia.

Esempio 2.2 (Tautologie e contraddizioni). Esempi di tautologie sono

$$p \vee \neg p$$

$$p \implies p$$

$$(p \implies q) \vee (q \implies p)$$

e di contraddizione

$$p \wedge \neg p$$

$$p \nrightarrow p$$

Definizione 2.11 (Formule logicamente equivalenti)**.** Siano α e β formule, se $f_\alpha = f_\beta$ allora α e β si dicono *logicamente equivalenti*.

Proprietà 2.4 (Caratterizzazione formule logicamente equivalenti)**.** *Due formule α e β sono logicamente equivalenti se e solo se la formula $\alpha \longleftrightarrow \beta$ è una tautologia.*

Notazione 2.12 (Formule logicamente equivalenti)**.** Siano α e β due formule, per denotare che sono logicamente equivalenti si scrive

$$\alpha \equiv \beta$$

Proposizione 2.5 (Relazione di logica di equivalenza)**.** *Siano α, β formule, introdotta la relazione*

$$\alpha \sim \beta \iff \alpha \text{ e } \beta \text{ sono logicamente equivalenti}$$

essa risulta una relazione di equivalenza sull'insieme delle formule $\mathcal{F}$.

Esempio 2.3. Alcune formule logicamente equivalenti sono

$$\alpha \implies \beta \equiv (\neg\alpha) \vee \beta$$
$$\neg(\alpha \wedge \beta) \equiv (\neg\alpha) \vee (\neg\beta)$$
$$\neg(\alpha \vee \beta) \equiv (\neg\alpha) \wedge (\neg\beta)$$
$$\alpha \iff \beta \equiv (\alpha \implies \beta) \wedge (\beta \implies \alpha)$$

E altre sulla associatività e distributività di $\wedge$ e $\vee$.

Osservazione 2.4. La prof osserva che se consideri una funzione che ad ogni formula associa la corrispondente funzione di verità, allora questa funzione non è iniettiva perché per ogni formula α esiste una classi di equivalenza $[\alpha]_\sim$ di formule logicamente equivalenti che hanno tutte la stessa funzione di verità. E' possibile però definire una funzione nell'insieme quoziente e quindi tale che ad ogni classe di equivalenza di formule logicamente equivalenti associa la funzione di verità di un elemento qualsiasi della classe (sono tutte uguali quindi è ben posta la definizione) e questa funzione risulta iniettiva. A questo punto ci chiediamo se la funzione risulta anche suriettiva (cioè per ogni funzione di verità esiste una formula con quella funzione di verità).

Definizione 2.13 (Formula ottenuta per sostituizione di variabili proposizionali)**.** Sia $\alpha(p_1, \ldots, p_n)$ una formula dipendente da n variabili proposizionali $p_1, \ldots, p_n$, allora se "sostituiamo" le variabili proposizionali con le formule $\gamma_1, \ldots, \gamma_n$ otteniamo la formula

$$\tilde{\alpha}(p_1/\gamma_1, \ldots, p_n/\gamma_n)\,,$$

che è una formula differente con complessità differente.

Teorema 2.6 (Teorema di sostituzione)**.** *Sia β una sottoformula di α e sia β logicamente equivalente ad una formula γ, allora la formula ottenuta sostituendo β con γ nella formula α si scrive*

$$\tilde{a}(\beta/\gamma)$$

ed si ha

$$\tilde{a} \equiv \alpha$$

Definizione 2.14 (Insieme soddisfacibile)**.** Sia S un insieme di formule, se esiste una valutazione $v : S \to \{0, 1\}$ tale che

$$v(\alpha) = 1, \quad \forall\, \alpha \in S$$

allora S si dice soddisfacibile.

Notazione 2.15 (Insieme di formule soddisfacibile)**.** Sia S un insieme di formule, per indicare che una valutazione $v : S \to \{0, 1\}$ rende soddisfacibile l'insieme S nel senso della definizione, scriviamo

$$v \models S\,.$$

Se non mi sbaglio si dice anche che "v soddisfa S".

Definizione 2.16 (Conseguenza logica di un insieme di formule)**.** Sia Γ un insieme di formule e sia φ una formula, se per ogni valutazione $v : \Gamma \to \{0, 1\}$ tale che $v \models \Gamma$ si ha che $v \models \varphi$ allora si dice che φ è conseguenza logica di Γ.

Notazione 2.17 (Conseguenza logica di un insieme di formule)**.** Sia Γ un insieme di formule e sia φ una formula, per denotare che φ è conseguenza logica di Γ si scrive

$$\Gamma \models \varphi\,.$$

Inoltre, siano $\varphi_1, \ldots \varphi_n$ formule, per indicare che φ è conseguenza logica di $\{\varphi_1, \ldots, \varphi_n\}$ si scrive più semplicemente

$$\varphi_1, \ldots, \varphi_n \models \varphi$$

Osservazione 2.5. Esistono insiemi di formule tali che ogni formula è loro conseguenza logica, ad esempio un insieme non soddisfacibile. Se invece fissiamo una formula φ e consideriamo una formula ψ, si ha che $\varphi \wedge \psi \models \varphi$.

Proprietà 2.7 (Caratterizzazione conseguenza logica di una formula)**.** *Siano α e β formule, allora*

$$\alpha \models \beta \iff \alpha \to \beta \text{ è una tautologia}$$

Corollario 2.7.1 (Caratterizzazione formule logicamente equivalenti)**.** *Siano α e β formule, allora α e β sono logicamente equivalenti se e solo se $\alpha \models \beta \wedge \beta \models \alpha$.*

Dimostrazione. Qui l'ho messo come corollario (ed è facilissimo da dimostrare), però puoi tranquillamente dimostrarlo dalla definizione. □

Teorema 2.8 (Caratterizzazione conseguenza logica di un insieme di formule)**.** *Siano Σ un insieme di formule e α una formula, allora*

$$\Sigma \models \alpha \iff \Sigma \cup \{\neg\alpha\} \text{ è un insieme non soddisfacibile}$$

Esercizi
Riprendendo la (Osservazione 2.4), intrudicamo la seguente definizione che sarà seguita da un teorema.

Definizione 2.18 (Letterale)**.** Sia α una variabile proposizionale o una negazione di una variabile proposizionale, allora α si dice *letterale*.

Definizione 2.19 (Forma normale disgiuntiva di una formula)**.** Sia α una formula, si dice che α è in *forma normale disgiuntiva (DNF)* se

$$\alpha = D_1 \vee \cdots \vee D_n$$

dove $D_i = \bigwedge_{j=1}^{n_i} \lambda_{ij}$
dove λ_{ij} sono letterali.

Definizione 2.20 (Forma normale congiuntiva di una formula)**.** Sia α una formula, si dice che α è in *forma normale congiuntiva (CNF)* se

$$\alpha = D_1 \wedge \cdots \wedge D_n$$

dove $D_i = \bigvee_{j=1}^{n_i} \lambda_{ij}$
dove λ_{ij} sono letterali.

Proprietà 2.9.

$$\alpha \implies \beta \equiv (\neg\alpha) \vee \beta$$

Esercizio 2.1.

$$p \implies (\neg q) \equiv (\neg p) \vee (\neg q)$$

si può scrivere in forma normale congiuntiva facilmente...

Teorema 2.10. *Sia $f : \{0,1\}^n \to \{0,1\}$, allora esiste una formula α la cui funzione di verità $f_\alpha = f$.*

Dimostrazione. L'ordine di $\{0,1\}^n$ è 2^n e siano $\{0,1\}^n = \{x_1, \ldots, x_{2^n}\}$ e k tali che $f(x_i) = 1 \; \forall\, i \in \{1, \ldots, k\}$ e $f(x_i) = 0 \; \forall\, i \in \{k+1, \ldots, 2^n\}$. Poiché per ogni $i \in \{1, \ldots, 2^n\}$ $x_i = (x_{i1}, \ldots, x_{in})$, posso definire per ogni $i \in \{1, \ldots, 2^n\}$ e $j \in \{1, \ldots, n\}$

$$\lambda_{ij} = \begin{cases} p_j & \text{se } x_{ij} = 1 \\ \neg p_j & \text{se } x_{ij} = 0 \end{cases},$$

dove p_j è una variabile proposizionale. Questi saranno i letterali che compariranno nella forma normale disgiuntiva finale.

A questo punto definiamo i "disgiunti" $D_i = D_i(p_1, \ldots, p_n)$

$$D_i = \lambda_{i1} \wedge \cdots \wedge \lambda_{in}\,.$$

Si verifica facilmente che per ogni valutazione v

$$v(\lambda_{ij}) = 1 \iff v(p_j) = x_{ij}\,,$$

ne segue che

$$v(D_i) = 1 \iff v(\lambda_{i1}) = \cdots = v(\lambda_{in}) = 1 \iff (v(p_1), \ldots, v(p_n)) = x_i$$

Infine definiamo la formula $\alpha = \alpha(p_1, \ldots, p_n)$

$$\alpha = D_1 \vee \cdots \vee D_k$$

e vogliamo dimostrare che $f = f_\alpha$, notiamo anche che α è in forma normale disgiuntiva.

Sia $x_i \in \{0,1\}^n$ e v una valutazione tale che $(v(p_1), \ldots, v(p_n)) = x_i$, se $i \in \{1, \ldots, k\}$ allora

$$f_\alpha(x_i) = v(\alpha) = 1 \iff \exists\, j \in \{1, \ldots, k\} : v(D_j) = 1 \iff \exists\, j \in \{1, \ldots, k\} : (v(p_1), \ldots, v(p_n)) = x_j$$

e questo è vero perché esiste i con quest'ultima proprietà per come abbiamo scelto v (nota che questa scelta non è arbitraria, v va scelto così affinché si possa considerare $f_\alpha(x_i)$, per definizione di f_α). Quindi si ha $f_\alpha(x_i) = 1 = f(x_i)$.

Se ora $i \in \{k+1, \ldots, 2^n\}$ e v come prima, allora

$$f_\alpha(x_i) = v(\alpha) = 0 \iff \forall\, j \in \{1, \ldots, k\}\ v(D_j) = 0 \iff \forall\, j \in \{1, \ldots, k\} : (v(p_1), \ldots, v(p_n)) \neq x_j$$

e questo è vero perché $(v(p_1), \ldots, v(p_n)) = x_i \neq x_j\ \forall\, j \neq i$ e in particolare $x_i \neq x_j\ \forall\, j \in \{1, \ldots, k\}$. Quindi di ha $f_\alpha(x_i) = 0 = f_\alpha(x_i)$ e abbiamo dimostrato che $f = f_\alpha$. □

Esempio 2.4 (Esempio di applicazione del teorema precedente). Consideriamo la funzione $f : \{0,1\}^2 \to \{0,1\}$ e tale che ... determiniamo α tale che $f_\alpha = f$.

Corollario 2.10.1. *Sia α una formula, allora esistono due formule α^c, α^d rispettivamente in forma normale congiuntiva e disgiuntiva che sono logicamente equivalenti ad α.*

Dimostrazione. Sia α una formula, allora posso considerare f_α che è una funzione di verità, per il teorema precedente, esiste una formula a^d in forma normale disgiuntiva tale che $f_\alpha = f_{\{a^d\}}$ e quindi α e α^d sono logicamente equivalenti; inoltre è possibile passare da una formula in forma normale disgiuntiva ad una in forma normale congiuntiva logicamente equivalante. E' possibile seguire anche un altro tipo di dimostrazione più "manuale": data una formula, "iterando sulla complessità" si possono trasformare i connettivi logici delle sottoformule della formula iniziale in espressioni che coinvolgono solo $\neg$, $\wedge$ e $\vee$, da cui si può ottenere una formula in forma normale disgiuntiva logicamente equivalente. □

Definizione 2.21 (Insieme adeguato di connettivi)**.** Un insieme di connettivi logici si dice *insieme adeguato di connettivi* se genera tutte le funzioni di verità e non esistono suoi sottoinsiemi propri che generano tutte le funzioni di verità.

Esempio 2.5 (Esempio insieme adeguato di connettivi). $\{\neg, \wedge, \vee\}$ è un insieme che genera tutte le funzioni di verità, in quanto una funzione di verità possiede sempre una formula in forma normale disgiuntiva o congiuntiva che ha la funzione di verità coincidente con quella data, quindi in certo senso usando solo questo insieme (sono gli unici connettivi che appaiono in DNF e in CNF) si può ottenere qualsiasi funzione di verità, in questo senso le funzioni di verità sono "generate". In realtà si ha che anche $\{\neg, \wedge\}$ e $\{\neg, \vee\}$ sono generano tutte le funzioni di verità perché $\wedge$ si può riscrivere in termini di $\neg$ e $\vee$, e $\vee$ di può riscrivere in termini di $\neg$ e $\wedge$, ma nessun loro sottoinsieme proprio fa lo stesso, quindi sono insiemi adeguati.

Definizione 2.22 (Catena)**.** Sia $\langle X, \subseteq \rangle$ un insieme parzialmente ordinato, una sua catena è un sottoinsieme non vuoto di X totalmente ordinato.

Definizione 2.23 (Insieme induttivo)**.** Un insieme parzialmente ordinato $\langle X, \subseteq \rangle$ tale che ogni catena di X ammette maggiorante si dice *induttivo*.

Lemma 2.11 (Lemma di Zorn)**.** *Sia $\langle X, \subseteq \rangle$ un insieme non vuoto parzialmente ordinato, se X è induttivo, allora X possiede un elemento massimale.*

Definizione 2.24 (Insieme di formule finitamente soddisfacibile)**.** Sia Σ un insieme di formule, se ogni sottoinsieme finito di Σ è soddisfacibile allora Σ si dice *finitamente soddisfacibile*.

Teorema 2.12 (Teorema di compattezza (calcolo proposizionale))**.** *Sia Σ un insieme di formule, allora Σ è soddisfacibile $\iff$ Σ è finitamente soddisfacibile.*

Dimostrazione. $\Longrightarrow$) Poiché Σ è soddisfacibile, esiste v valutazione tale che $v(s) = 1 \ \forall \ s \in \Sigma$ allora per qualsiasi sottoinsieme $\Gamma \subseteq \Sigma$ finito si ha $v(s) = 1 \ \forall \ s \in \Gamma$.

$\Longleftarrow$) Si procede in tre passi.

1° passo: Definiamo un insieme ordinato Ω induttivo, applichiamo il lemma di Zorn e otteniamo un insieme di formule Σ^* come elemento massimale di Ω tale che $\Sigma \subseteq \Sigma^*$.

Definiamo

$$\Omega = \{\Gamma \in \mathcal{P}(\mathcal{F}) : \Gamma \text{ è finitamente soddisfacibile e } \Sigma \subseteq \Gamma\},$$

esso è un insieme ordinato rispetto all'inclusione $\subseteq$ e si ha che $\Sigma \in \Omega$, quindi $\Omega \neq \varnothing$. Sia C una catena di Ω, allora $\bigcup_{X \in C} X \in \Omega$ (devi dimostrare che $\bigcup_{X \in C} X$ è finitamente soddisfacibile e che Σ vi è contenuto, l'ultima cosa è ovvia) è un maggiorante di C in Ω, ne segue che Ω è un insieme induttivo. Ω è un insieme ordinato non vuoto e induttivo, quindi per il lemma di Zorn Ω ammette un elemento massimale Σ^*.

2° passo: studiamo le proprietà di Σ^*

Poiché $\Sigma^* \in \Omega$, allora Σ^* è finitamente soddisfacibile e $\Sigma \subseteq \Sigma^*$, inoltre sappiamo che Σ^* è massimale in Ω. Ora sia α una formula, dimostriamo che $\alpha \in \Sigma^*$ o $\neg\alpha \in \Sigma^*$. Supponiamo per assurdo che $\alpha, \neg\alpha \notin \Sigma^*$, cioè $\Sigma^* \subset \Sigma^* \cup \{\alpha\}, \Sigma^* \cup \{\neg\alpha\}$. Poiché Σ^* è massimale in Ω, e $\Sigma \subseteq \Sigma^* \subset \Sigma^* \cup \{\alpha\}, \Sigma^* \cup \{\neg\alpha\}$, non può succedere che $\Sigma^* \cup \{\alpha\}, \Sigma^* \cup \{\neg\alpha\} \in \Omega$ e quindi $\Sigma^* \cup \{\alpha\}, \Sigma^* \cup \{\neg\alpha\}$ non sono finitamente soddisfacibili. Allora esistono $A_0 \cup \{\alpha\} \subseteq \Sigma^* \cup \{\alpha\}, B_0 \cup \{\neg\alpha\} \subseteq \Sigma^* \cup \{\neg\alpha\}$ insiemi finiti non soddisfacibili (si possono scrivere sempre in questa forma perché non può succedere che un sottoinsieme $A \subseteq \Sigma^* \cup \{\alpha\}$ finito non soddisfacibile che non contenga α, perché significherebbe che $A \subseteq \Sigma^*$ e quindi Σ^* sarebbe non soddisfacibile, lo stesso vale per $\Sigma^* \cup \{\neg\alpha\}$), quindi, per (Teorema 2.8), si ha $A_0 \models \alpha$ e $B_0 \models \neg\alpha$. Di conseguenza $A_0 \cup B_0 \models \alpha \wedge \neg\alpha$ e quindi $A_0 \cup B_0$ è non soddisfacibile, ma è un sottoinsieme finito di Σ^* e questo è assurdo, quindi si ha $\alpha \in \Sigma^*$ o $\neg\alpha \in \Sigma^*$.

3° passo: costruiamo la valutazione v che soddisfa Σ

Sia v una valutazione tale che per ogni $p \in P$, $v(p) = 1 \iff p \in \Sigma^*$, ora la vogliamo estendere a tutte le formule, poiché $\{\neg, \vee\}$ è un insieme adeguato, basta estenderla considerando questi connettivi. Vogliamo dimostrare che $v(\alpha) = 1 \iff \alpha \in \Sigma^*$, procediamo per induzione sulla complessità della formula, sia $\alpha \in P$, allora $v(\alpha)$ è già definita. Sia $\alpha = \neg\beta$, allora $v(\alpha) = 1 \iff v(\beta) = 0$, poiché β ha complessità minore di 1 rispetto ad α, per ipotesi induttiva $v(\beta) = 0 \iff \beta \notin \Sigma^*$, ma per quanto dimostrato sopra si ha $\beta \in \Sigma^*$ o $\neg\beta \in \Sigma^*$, quindi si ha $v(\alpha) = 1 \iff \alpha \in \Sigma^*$. Sia $\alpha = \beta \vee \gamma$, allora $v(\alpha) = 1 \iff v(\beta) = 1 \vee v(\gamma) = 1$, per ipotesi induttiva si ha $v(\beta) = 1 \vee v(\gamma) = 1 \iff \beta \in \Sigma^* \vee \gamma \in \Sigma^*$.

A questo punto vogliamo far vedere che $\beta \in \Sigma^* \vee \gamma \in \Sigma^* \iff \beta \vee \gamma \in \Sigma^*$. Sia $\beta \in \Sigma^* \vee \gamma \in \Sigma^*$ e supponiamo per assurdo $\beta \vee \gamma \notin \Sigma^*$, allora, per la proprietà dimostrata precedentemente, $\neg(\beta \vee \gamma) \in \Sigma^*$. Si ha che $\{\beta, \neg(\beta \vee \gamma)\} \subseteq \Sigma^*$ o $\{\gamma, \neg(\beta \vee \gamma)\} \subseteq \Sigma^*$, ma entrambi gli insiemi sono finiti e non soddisfacibili e ciò assurdo, allora $\beta \vee \gamma \in \Sigma^*$. Sia $\beta \vee \gamma \in \Sigma^*$ e supponiamo per assurdo $\beta, \gamma \notin \Sigma^*$, allora, sempre per le proprietà di Σ^*, $\neg\beta, \neg\gamma \in \Sigma^*$ e quindi l'insieme finito $\{\neg\beta, \neg\gamma, \beta \vee \gamma\} \subseteq \Sigma^*$, ma questo è non soddisfacibile e ciò è assurdo, quindi $\beta \in \Sigma^* \vee \gamma \in \Sigma^*$.

In conclusione ho determinato una valutazione v tale che $v(\alpha) = 1 \ \forall \alpha \in \Sigma^*$, ma allora $v(\alpha) = 1 \ \forall \alpha \in \Sigma$, poiché $\Sigma \subseteq \Sigma^*$, cioè Σ è soddisfacibile. □

Osservazione 2.6. La dimostrazione richiede l'utilizzo dell'assioma della scelta (nella forma di Lemma di Zorn) ed è possibile dimostrare che questo stesso teorema è equivalente all'assioma della scelta.

Corollario 2.12.1. *Siano Σ un insieme di formule e α una formula, se $\Sigma \models \alpha$ allora esiste $\Sigma_0 \subseteq \Sigma$ sottoinsieme finito di Σ tale che $\Sigma_0 \models \alpha$.*

Dimostrazione. Se Σ è non soddisfacibile, allora per (Teorema 2.12) esiste $\Sigma_0 \subseteq \Sigma$ finito e non soddisfacibile, allora $\Sigma_0 \models \alpha$. Per (Teorema 2.8) e (Teorema 2.12) si ha $\Sigma \models \alpha \iff \Sigma \cup \{\neg\alpha\}$ è non soddisfacibile $\iff$ $\exists\, \Sigma' \subseteq \Sigma \cup \{\neg\alpha\}$ insieme finito non soddisfacibile. Sia $\Sigma_0 = \Sigma' \setminus \{\neg\alpha\} \subseteq \Sigma$ insieme finito, allora $\Sigma_0 \models \alpha \iff \Sigma' = \Sigma_0 \cup \{\neg\alpha\}$ è non soddisfacibile e questo è vero, da cui l'asserto. □

Notazione 2.25 (Simbolo del falso)**.** $\perp$ è il simbolo per indicare il falso ed corrisponde ad un espressione del tipo $p \wedge (\neg p)$, con p variabile proposizionale.

Esempio 2.6. $\{\rightarrow, \perp\}$ è un insieme adeguato.

Capitolo 3

Calcolo dei predicati

Il calcolo dei predicati è anche detto logica del prim'ordine ed estende in un certo senso il calcolo proposizionale, infatti esso ha un linguaggio più vasto che comprende anche i quantificatori e le relazioni binarie. Su di esso si basano i "linguaggi del prim'ordine" come quello della teoria ZF.

3.1 Linguaggio del calcolo dei predicati

Questa sezione l'ho creata io perché secondo me è mancante... In quanto nel calcolo dei predicati si usano più simboli di quelli del calcolo proposizionale (ci sono gli operatori binari e i quantificatori).

In realtà i linguaggi sono infiniti perché descrivono "tutta la matematica" (vedi ho scritto anche altro da un'alrta parte).

Comunque forse ho capito (vedi [Dal08, p.60]), nel calcolo dei predicati consideriamo un numero infinito (numerabile) di simboli di variabili, i connettivi $\{\vee, \wedge, \to, \neg, \longleftrightarrow, \bot, \forall, \exists\}$ e le parentesi e la virgola, INOLTRE ogni volta fissiamo un linguaggio (a seconda del contesto) che contiene: simboli di predicati (relazioni), simboli di funzioni e simboli di costanti.

3.2 Regole di deduzione naturale

La logica può essere sviluppata da un punto di vista "semantico" (si usa il concetto di "verità") o da un punto di vista della "deduzione logica" (si usa il concetto di "derivazione"), fin'ora abbiamo seguito il primo approccio, cioè abbiamo considerato delle valutazioni e "come vengono valutate le formule" (cosa succede se sostituisco ad una formula un'altra, se ci sono formule logicamente equivalenti, ecc) e quindi ci siamo chiesti quando una proposizione (cioè una formula) è "vera" o "falsa", ci siamo quindi basati sul concetto di "verità". Ora invece introduciamo un metodo per trarre delle conclusioni "logiche" (nel senso che seguono un ragionamento obiettivamente corretto, fissate delle regole) da un insieme di "premesse" (le nostre ipotesi), cioè introduciamo delle *regole di deduzione naturale*. La deduzione naturale è un metodo di ragionamento che permette di dimostrare enunciati (o "passare da enunciati veri a enunciati veri", direbbe così la prof?), esso possiede una sua notazione e delle sue regole formali. La deduzione naturale non è esclusiva del calcolo dei predicati, può essere utilizzata in calcolo proposizionale ma con delle "limitazioni" (perché in calcolo dei predicati sono presenti più simboli e quindi anche più regole di deduzione).

Quindi il calcolo proposizionale gode solo di pochi simboli che indicano una relazione fra gli oggetti che si stanno considerando: i connettivi logici, ad ogni modo la deduzione naturale può essere applicata, la debolezza di questo approccio è che non può trattare di "tutta la matematica" (cioè di tutti i tipi di proposizioni che ci servono), questo è dovuto alla mancanza di altri simboli che stabiliscono ulteriori relazioni fra gli oggetti di studio: quantificatori, operatori binari, ecc che invece sono presenti nel calcolo dei predicati; inoltre nel calcolo dei predicati non è presente un unico linguaggio ma un'infinità di linguaggi (studieremo le $\mathcal{L}$-strutture).

Notazione I passaggi logici della deduzione naturale vengono schematizzati in una simile tabella

$$\frac{\text{(PREMESSE)}}{\text{(CONCLUSIONI)}}\ \text{(REGOLA DI DERIVAZIONE)}$$

Le dimostrazioni sono una sequenza finita di formule che si ottiene a partire da un insieme di formule Σ o dalla sequenza di formule già dimostrate. Nella notazione che usiamo le PREMESSE sono le formule di

Σ o quelle già dimostrate e attraverso una REGOLA DI DERIVAZIONE otteniamo un'altra formula o più formule, che sono le nostre CONCLUSIONI[1].

Nella pratica delle dimostrazioni, esistono due tipi di ipotesi: *ipotesi "reali"* e *ipotesi fittizie o provvisorie*, entrambe sono un insieme di formule ma vengono usate in modo diverso. Le prime sono ipotesi che prendiamo nell'insieme di formule Σ, per fare un'analogia con le dimostrazioni "classiche" (cioè prima di studiare Logica) sono proprietà che già conosciamo (ad esempio un lemma prima di un teorema che vogliamo dimostrare), oppure sono assiomi o semplicemente delle formule che includiamo nell'enunciato nella forma di "Sia ..." (dopo farò un esempio che chiarisce questo concetto). Le seconde invece sono formule utilizzate per dimostrare altre formule ma originariamente non erano presenti in Σ e nemmeno erano state dimostrate precedentemente, quindi compaiono necessariamente solo nella dimostrazione, cosa significa questo? Che possiamo prendere formule a casaccio? No, semplicemente che, secondo le regole di derivazione, in alcuni casi è possibile prendere delle formule siffatte che permettono comunque di dimostrarne altre (nelle regole di derivazione vengono denotate esplicitamente con la notazione $[\varphi]$, dove φ è una formula), per fare un'analogia con le "dimostrazioni classiche", sono quelle che compaiono negli enunciati nella forma di "Se ... allora ...", ma anche quando consideriamo i diversi casi possibili o facciamo una dimostrazione per assurdo. Prima ho detto che le ipotesi fittizie compaiono solo nella dimostrazione e ora ho detto che compaiono anche nell'enunciato, il motivo è che a volte, per come sono scritti gli enunciati, stiamo preannunciando "una parte di dimostrazione" (ancora una volta rimando all'esempio successivo). Un'altra differenza importante fra ipotesi "vere" e "fittizie" è che queste ultime vanno "cancellate", cioè non devono apparire alla fine della dimostrazione, questo termine viene utilizzato nella pratica delle dimostrazioni mediante regole di deduzione naturale e significa semplicemente applicare una delle regole che permette di usare le ipotesi fittizie, infatti se le regole vengono correttamente applicate, l'ipotesi fittizia fatta "viene cancellata", nel senso che "abbiamo fatto finta che ci fosse prima" (per questo "fittizia") ma poi la regola ci dice che "possiamo smettere di considerarla (e quindi cancellarla) e tenerci il risultato", si dice anche che "le ipotesi fittizie vengono inglobate nel risultato".

Vederemo che se abbiamo un insieme di formule Σ da cui dimostriamo una formula α, scriviamo $\Sigma \vdash \alpha$, qui compaiono palesemente le "ipotesi vere" (che sarebbero le formule di Σ), ma non quelle fittizie, perché, ancora una volta, divengono "visibili" solo nella dimostrazione, inoltre una dimostrazione non è mai unica e per una singola dimostrazione potrebbero esistere delle ipotesi fittizie diverse che uno utilizza per ottenere lo stesso risultato, anche per questo non compaiono, perché dipendono dalla "scelta" di chi dimostra.

In alcuni casi la differenza principale fra le ipotesi fittizie e quelle "vere" è solo formale, cioè due enunciati che hanno lo stesso "significato" possono essere dimostrati in due modi formalmente diversi, anche se intuitivamente sono molto simili. A breve seguirà un esempio.

Esempio 3.1 (Significato di "$\vdash$" negli enunciati). Qui chiarisco il senso di "$\vdash$", voglio dimostrare le seguenti cose:

1. $$\varphi \wedge \psi \vdash \psi$$

   Dimostrazione.
   $$\frac{\varphi \wedge \psi}{\psi}\,\mathrm{E}\wedge$$
   □

2. $$\vdash \varphi \wedge \psi \to \psi$$

   Dimostrazione.
   $$\frac{\frac{[\varphi \wedge \psi]}{\psi}\,\mathrm{E}\wedge}{\varphi \wedge \psi \to \psi}\,\mathrm{I}\to$$
   □

Come vedi il significato degli enunciato è lo stesso ma le dimostrazioni sono leggermente diverse, quello che cambia è che in un caso abbiamo dovuto "cancellare" l'ipotesi fittizia con l'introduzione dell'implicazione e nell'altro caso no.

[1] Quando daremo la definizione formale di dimostrazione, si vedrà che non è esattamente così, perché diremo che le regole di derivazione si applicano solo a formule già dimostrate e non alle formule di Σ, d'altra parte però ogni formula di Σ "dimostra se stessa" ($\varphi \vdash \varphi$), cioè le possiamo sempre considerare; inoltre per "iniziare la dimostrazione" alcune formule devono essere necessariamente prese da Σ (se no non potrei dimostrare niente), quindi è solo una questione di notazione.

Ma allora qual è il vantaggio di avere ipotesi "vere"? Se io ho già dimostrato in precedenza un risultato, allora lo posso considerare "vero" e non c'è bisogno di considerare tale risultato un'ipotesi "fittizia" (cioè non devo dire nel teorema "Se [questo] è vero, allora [quest'altro] è vero" (perché io ho già so che "[questo]" è vero), anzi un'espressione simile è caratteristica delle ipotesi fittizie in cui si utilizza l'introduzione dell'implicazione), ecco un esempio per distinguerle.

Esempio 3.2 (Distinzione fra ipotesi "reali" e "fittizie"). Considera il seguente enunciato (è il migliore che mi è venuto in mente)

Sia $f : [a, b] \to \mathbb{R}$ *una funzione continua. Se* f *è monotona, allora la sua inversa è monotona.*

In questo enunciato stiamo supponendo di avere una funzione continua e monotona e ne deduciamo che la sua inversa è anch'essa monotona, ma chi ci dice che la sua inversa esiste? E' un'ipotesi aggiuntiva? No, semplicemente l'abbiamo dimostrato in precedenza, quindi l'esistenza dell'inversa di f è una "ipotesi reale", mentre le ipotesi che sia continua e monotona sono "ipotesi fittizie" e si nota facilmente che vengono introdotte col "se", mentre le ipotesi "reali" vengono introdotte come vere e proprie affermazioni certe.

Si potrebbe fare un esempio in cui viene utilizzata la riduzione all'assurdo.

Consiglio. Ora introdurrò le regole di deduzione naturale, per averne un'idea intuitiva, devi immaginare che le ipotesi nelle PREMESSE siano "vere" e le CONCLUSIONI sono quelle che puoi ottenere come hai sempre fatto nelle dimostrazioni, qui sono semplicemente scritte in modo più formale, prova a leggere "Ho Σ", dove Σ sono formule che rappresentano le PREMESSE, e poi "Allora Σ'", dove Σ' sono le formule che rappresentano le CONCLUSIONI.

1. Regole di introduzione
   - Introduzione della congiunzione
   $$\frac{\varphi \qquad \psi}{\varphi \wedge \psi}\, \mathrm{I}\wedge$$
   - Introduzione dell'implicazione
   $$\begin{array}{c} [\varphi] \\ \vdots \\ \psi \end{array} \over \varphi \to \psi\, \mathrm{I}\to$$
   Se da un ipotesi fittizia $[\varphi]$ riesco ad ottenere ψ, allora è vero che $\varphi \to \psi$.
   Cerchiamo di spiegarne il significato intuitivo. La regola sta dicendo che "se ottengo una formula ψ da un'altra formula sotto forma di ipotesi $[\varphi]$ allora la seconda implica la prima", cioè ho trasformato la mia ipotesi $[\varphi]$ e il risultato ottenuto ψ nella mia tesi $\varphi \to \psi$ e quindi la mia ipotesi fittizia è stata "inglobata" nella tesi! E' il ragionamento classico del tipo "Se a allora b", con la semplice precisazione che io inizialmente non avevo "preso in considerazione a" (se invece l'avessi fatto avrei dovuto dire "Io ho a, allora ottengo b").
   - Introduzione del per ogni (o dell'universale) Se ho ottenuto una derivazione di $\varphi(x)$ da ipotesi in cui la x non compariva come variabile libera (ovvero era vincolata), allora vale
   $$\frac{\varphi(x)}{\forall x \varphi(x)}\, \mathrm{I}\forall$$
   Sono riuscito a fare un esempio per capire il senso della regola, sta sul quaderno cancellabile.
   - Introduzione dell'esistenziale
   Sia $\alpha(x)$ una formula e sia t termine libero per x in $\alpha(x)$, allora vale
   $$\frac{\alpha(t)}{\exists x \alpha(x)}\, \mathrm{I}\exists$$
2. Regole di eliminazione
   - Eliminazione della congiunzione
   $$\frac{\varphi \wedge \psi}{\varphi}\, \mathrm{E}\wedge$$
   $$\frac{\varphi \wedge \psi}{\psi}\, \mathrm{E}\wedge$$

- Eliminazione dell'implicazione

$$\frac{\varphi \qquad \varphi \to \psi}{\psi} \, \mathrm{E}\to$$

- Eliminazione del per ogni (o dell'universale)
  Data una formula $\forall x\varphi(x)$ è possibile ottenere $\varphi(t)$, con t termine libero per x in φ (cioè in φ non compaiono quantificatori che "agiscono" sulle variabili di t), mediante la seguente derivazione

$$\frac{\forall x\varphi(x)}{\varphi(t)} \, \mathrm{E}\forall$$

- Eliminazione dell'esistenziale
  Se x non compare libera in β (e ho "un qualsiasi z"), allora

$$\begin{array}{c} [\alpha(z)] \\ \vdots \\ \beta \quad \exists x\alpha(x) \end{array} \, \mathrm{E}\exists$$

3. Altre regole

- Regola falsum o regola del falso

$$\frac{\bot}{\varphi} \, \bot$$

  Il falso implica tutto

- Riduzione all'assurdo

$$\begin{array}{c} [\neg\varphi] \\ \vdots \\ \bot \end{array} \, \mathrm{RAA}$$

  Data un ipotesi fittizia $[\neg\varphi]$, se riesco ad ottenere una dimostrazione del falso da tale ipotesi fittizia, allora ho dimostrato φ.

Osservazione 3.1. Le regole di deduzione non vengono introdotte tutte "contemporaneamente", infatti le regole del "per ogni" e "dell'esistenziale" vengono introdotte molto più avanti, quindo vengono trattate $\mathcal{L}$-strutture, variabili libere e vincolate, ecc, mentre tutte le altre possono essere introdotte fin dall'inizio (perché sono quelle che vanno bene anche per il calcolo proposizionale), molte delle interpretazione scritte fin'ora valgono (con certezza) solo per queste ultime. Inoltre ho commesso un errore di notazione, nella parte di spiegazione intuitiva ho scritto più volte di pensare alle formule nelle premesse come "vere" e questo da un punto di vista intuitivo va bene, ma nasce un problema perché successivamente si da' una definizione formale di "formula vera".

3.3 Formalizzazione teoremi, dimostrazioni, ecc

Definizione 3.1 (Insieme delle derivazioni o delle dimostrazioni)**.** Confronta [Dal08, p. 34]
L'insieme delle dimostrazioni o delle dimostrazioni è il più piccolo insieme X tale che

1. $\alpha \in X$ per ogni variabile proposizionale α
2. Se io ho una dimostrazione di $\frac{D}{\alpha}$ e una dimostrazione di $\frac{D}{\alpha'}$, cioè $\frac{D}{\alpha}, \frac{D}{\alpha'} \in X$ allora

$$\frac{\frac{D}{\alpha} \qquad \frac{D}{\alpha}}{\alpha \wedge \alpha'} \in X$$

3. Se $\frac{D}{\alpha\wedge\alpha'} \in X$, allora $\frac{\alpha\wedge\alpha'}{\alpha}, \frac{\alpha\wedge\alpha'}{\alpha'} \in X$

4. $\frac{\overset{\varphi}{D}}{\psi} \in X$ allora $\frac{\overset{[\varphi]}{\psi}}{\varphi \to \psi} \in X$

5. $\overset{D}{\varphi}, \varphi \overset{D'}{\to} \psi \in X$ allora $\frac{\overset{D}{\varphi} \qquad \overset{D'}{\varphi \to \psi}}{\psi} \in X$

6. Se $\overset{D}{\perp}$, allora $\frac{\overset{D}{\perp}}{\alpha} \in X$ per ogni formula α

7. Se $\frac{\overset{\varphi}{D}}{\perp} \in X$, allora $\frac{\perp}{\varphi} \in X$

8. Se x non compare libera nelle formule di D

   - se $\frac{D}{\alpha(x)} \in X$ allora $\frac{\overset{D}{\alpha(x)}}{\forall x \alpha(x)} \in X$
   - se $\frac{D}{\forall x \alpha(x)} \in X$ allora $\frac{\overset{D}{\forall x \alpha(x)}}{\alpha(t)} \in X$, con t libero per x in $\alpha(x)$

Riassumendo X è il più piccolo insieme tale che

1. Contiene tutte le formule
2. E' chiuso per le regole di derivazione naturale (sia quelle dei connettivi che quelle dei quantificatori)

Definizione 3.2 (Dimostrazione di una formula a partire da un insieme di formule)**.** Siano Γ un insieme di formule e α una formula, sia $\alpha_0, \ldots, \alpha_n$ una sequenza finita di formule tale che $\alpha_n = \alpha$ e per ogni $i \in \{1, \ldots, n\}$ $\alpha_i \in \Gamma$ o α_i è ottenuto per le regole di deduzione naturale dall'insieme $\{\alpha_j : j < i\}$, allora si dice che la sequenza $\alpha_0, \ldots, \alpha_n$ è una *dimostrazione di α a partire da* Γ.

Osservazione 3.2. Nota che da questa definizione si ha che una dimostrazione è una sequenza finita di formule ottenute per dall'applicazione di regole che coinvolgono un numero finito di formule.

Definizione 3.3 (Formula dimostrabile a partire da un insieme di formule)**.** Sia Γ un insieme di formule. una formula α si dice *dimostrabile a partire da* Γ se esiste una dimostrazione con conclusione α e ipotesi "non cancellabili" (non fittizie) su Γ.

Notazione 3.4 (Formula dimostrabile a partire da un insieme di formule)**.** Siano Γ un insieme di formule e α una formula se α è dimostrabile a partire da Γ si scrive

$$\Gamma \vdash \alpha$$

Definizione 3.5 (Teorema)**.** Sia α una formula tale che $\varnothing \vdash \alpha$, allora α si dice *teorema*.

Notazione 3.6 (Teorema)**.** Sia α una formula, se α è un teorema si scrive

$$\vdash \alpha$$

Esercizio 3.1. Sia $\Gamma = \{\varphi, \varphi \to \psi, \varphi \to \gamma\}$, determina una dimostrazione di $\psi \wedge \gamma$ a partire da Γ.

Un sacco di esercizi

Teorema 3.1. *Siano Γ e Γ' insiemi di formule*

1. *Se $\Gamma \vdash \alpha$ e $\Gamma' \vdash \beta$, allora $\Gamma \cup \Gamma' \vdash \alpha \wedge \beta$*
2. *Se $\Gamma \vdash \alpha \wedge \beta$ allora $\Gamma \vdash \alpha$ e $\Gamma \vdash \beta$*
3. *Se $\Gamma \cup \{\beta\} \vdash \alpha$ allora $\Gamma \vdash \beta \to \alpha$*
4. *Se $\Gamma \cup \{\neg\alpha\} \vdash \perp$ allora $\Gamma \vdash \alpha$*
5. *Se $\Gamma \vdash \perp$ allora $\Gamma \vdash \alpha$ per ogni formula α*
6. *Se $\Gamma \vdash \alpha$ e $\Gamma' \vdash \alpha \to \beta$ allora $\Gamma \cup \Gamma' \vdash \beta$*

Teorema 3.2 (Teorema di validità (calcolo proposizionale))**.** *Siano Σ un insieme di formule e α una formula, se $\Sigma \vdash \alpha$ allora $\Sigma \models \alpha$.*

Dimostrazione. Sia $\alpha_1, \dots, \alpha_n$ una dimostrazione di α a partire da Σ, procediamo per induzione sulla lunghezza della dimostrazione. Sia $n = 1$, allora $\alpha_1 = \alpha$ e α_1 non può essere ottenuto dalle formule precedenti poiché non ce ne sono, quindi per definizioni di dimostrazione, $\alpha \in \Sigma$ e ovviamente $\Sigma \models \alpha$. Sia $n > 1$ e supponiamo che se ho una dimostrazione di lunghezza $m < n$ di una qualsiasi formula β a partire da un insieme di formule Γ, allora $\Gamma \models \beta$. Noi sappiamo che la dimostrazione $\alpha_1, \dots, \alpha_n$ è tale che $\alpha_n \in \Sigma$ (caso ovvio) o α_n è ottenuto mediante le regole di deduzione naturale da $\{\alpha_1, \dots, \alpha_{n-1}\}$, allora esiste una regola di deduzione naturale, l'ultima applicata, da cui è stata ricavata la formula α_n, consideriamo ciascuno dei possibili casi.

Se la regola è l'introduzione della congiunzione I$\wedge$, allora esistono $\beta, \gamma \in \Sigma \cup \{\alpha_1, \dots, \alpha_{n-1}\}$ tali che $\alpha = \beta \wedge \gamma$. Se $\beta \in \Sigma$ allora ovviamente $\Sigma \models \beta$, se $\beta \in \{\alpha_1, \dots, \alpha_n\}$ allora esiste $m < n$ tali che $\beta = \alpha_m$ e $\alpha_1, \dots, \alpha_m$ è una dimostrazione di β a partire da Σ e per ipotesi induttiva si ha $\Sigma \models \beta$; analogamente in ogni caso $\Sigma \models \gamma$. Dal fatto che $\Sigma \models \beta$ e $\Sigma \models \gamma$, segue $\Sigma \models \beta \wedge \gamma = \alpha$.

Se la regola è l'eliminazione della congiunzione E$\wedge$, allora esistono β e γ formule tali che $\beta \wedge \gamma \in \Sigma \cup \{\alpha_1, \dots, \alpha_{n-1}\}$ e $\alpha = \beta$ o $\alpha = \gamma$, senza perdita di generalità, supponiamo $\alpha = \beta$. Se $\beta \wedge \gamma \in \Sigma$ ovviamente $\Sigma \models \beta \wedge \gamma$, se $\beta \wedge \gamma \in \{\alpha_1, \dots, \alpha_{n-1}\}$ per ipotesi induttiva $\Sigma \models \beta \wedge \gamma$; in ogni caso $\Sigma \models \beta = \alpha$.

Se la regola è l'introduzione dell'implicazione I$\rightarrow$, allora esistono $\beta, \gamma \in \Sigma \cup \{\alpha_1, \dots, \alpha_{n-1}\}$ tali che $\alpha = \beta \implies \gamma$. Se $\beta \in \Sigma$ allora ovviamente $\Sigma \models \beta$, se $\beta \in \{\alpha_1, \dots, \alpha_{n-1}\}$ per ipotesi induttiva $\Sigma \models \beta$; analogamente in ogni caso $\Sigma \models \gamma$. Dal fatto che $\Sigma \models \beta$ e $\Sigma \models \gamma$ si ha $\Sigma \models \beta \rightarrow \gamma = \alpha$.

Se la regola è l'eliminazione dell'implicazione E$\rightarrow$, allora esistono φ, ψ formule tali che $\varphi, \varphi \rightarrow \psi \in \Sigma \cup \{\alpha_1, \dots, \alpha_{n-1}\}$. Se [... sempre la stesa cosa]

Se la regola è la regola del falso, allora abbiamo dimostrato $\bot$ "prima" di dimostrare α_n, quindi $\bot = \alpha_i$ con $i \in \{1, \dots, n-1\}$ e per ipotesi induttiva $\Sigma \models \bot$, allora σ non è soddisfacibile, quindi $\sigma \models \alpha$.

Se la regola è la riduzione all'assurdo RAA, allora significa che se prendiamo come ipotesi fittizia $\neg\alpha$ dimostriamo il falso, cioè che $\Sigma \cup \{\neg\alpha\} \vdash \bot$, ma $\bot = \alpha_i$ con $i \in \{1, \dots, n-1\}$ in qato viene "dimostrato prima" di $\aleph_n$ e quindi per ipotesi induttiva, $\Sigma \cup \{\neg\alpha\} \models \bot$, allora $\Sigma \cup \{\neg\alpha\}$ non è soddisfacibile, per cui $\Sigma \models \alpha$.

In ogni caso si ha l'asserto. □

Esercizio 3.2. Un sacco di esercizi sulla deduzione naturale

Definizione 3.7 (Insieme di formule consistente)**.** Un insieme di formule si dice *consistente* se da Γ non è possibile dimostrare il falso, cioè

$$\Gamma \nvdash \bot .$$

Un insieme che non è consistente si dice *inconsistente*.

Proposizione 3.3 (Caratterizzazione insieme inconsistente)**.** *Le seguenti affermazioni sono equivalenti*

1. Γ *è inconsistente*
2. $\Gamma \vdash \alpha$ *per ogni formula* α
3. *Esiste una formula* φ *tale che* $\Gamma \vdash \varphi$ *e* $\Gamma \vdash \neg\varphi$

Lemma 3.4. *Sia* Γ *un insieme consistente di formule, allora*

1. *Se* $\Gamma \nvdash \varphi$ *allora* $\Gamma \cup \{\neg\varphi\}$ *è consistente*
2. *Se* $\Gamma \nvdash \neg\varphi$ *allora* $\Gamma \cup \{\varphi\}$ *è consistente*

Dimostrazione. Per la dimostrazione di entrambe ragioniamo per assurdo. La (1) si fa con la riduzione all'assurdo, mentre la (2) con l'introduzione dell'implicazione e quindi qui si può cogliere proprio la differenza fra i due approcci, che non sono la stessa cosa, ma sono collegati mediante logica equivalenza (vedi Van Dalen p.31, anzi per Van Dalen si ha $\neg\varphi = \varphi \rightarrow \bot$, mentre per la prof $\neg\varphi \equiv \varphi \rightarrow \bot$, è una questione di definizione). □

Teorema 3.5 (Caratterizzazione soddisfacibilità e consistenza di un insieme di formule)**.** *Sia* Γ *un insieme di formule, allora* Γ *è soddisfacibile se e solo se* Γ *è consistente.*

Osservazione 3.3. Nota che se avessimo già dimostrato il Teorema di validità e completezza (Teorema 3.7) allora questo teorema sarebbe un corollario, in quanto

$$\Gamma \text{ è non soddisfacibile} \iff \Gamma \models \bot \iff \Gamma \vdash \bot \iff \Gamma \text{ è inconsistente} .$$

Quindi questo ci fa capire che stiamo dimostrando "un caso particolare" del teorema di validità e completezza.

Dimostrazione. $\Longrightarrow$) Sia per assurdo che Γ è inconsistente, allora $\Gamma \vdash \bot$ e, per il teorema di validità (Teorema 3.2), si ha $\Gamma \models \bot$ cioè Γ è non soddisfacibile, assurdo.

$\Longleftarrow$) Si dimostra in 3 passi.

1° passo: Definiamo un insieme ordinato Ω induttivo, applichiamo il lemma di Zorn e otteniamo un insieme di formule Γ^* come elemento massimale di Ω tale che $\Gamma \subseteq \Gamma^*$.

Sia $\Omega = \{\Sigma : \Sigma \text{ è consistente e } \Gamma \subseteq \Sigma\}$, si ha $\Gamma \in \Omega$, mostriamo che è induttivo (aggiungi questa parte), allora, per il Lemma di Zorn, esiste un elemento massimale $\Gamma^* \in \Omega$.

2° passo: studiamo le proprietà di Γ^*

Vogliamo dimostrare che

1. Se $\Gamma^* \vdash \varphi$ allora $\varphi \in \Gamma^*$
2. Per ogni formula φ si ha $\varphi \in \Gamma^*$ o $\neg\varphi \in \Gamma^*$. VEDI LA DIMOSTRAZIONE NON MI TROVO

Sia $\Gamma^* \vdash \varphi$ e supponiamo per assurdo $\varphi \notin \Gamma^*$, allora $\Gamma^* \subset \Gamma^* \cup \{\varphi\}$, ma $\Gamma \subseteq \Gamma^* \cup \{\varphi\}$ e $\Gamma^* \cup \{\varphi\} \notin \Omega$ (altrimenti Γ^* non sarebbe massimale) allora $\Gamma^* \cup \{\varphi\} \vdash \bot$ (cioè è inconsistente), ma questo significa che se prendo come ipotesi fittizia $[\varphi]$ e introduco l'implicazione si ha $\Gamma^* \vdash \varphi \implies \bot = \neg\phi$ e quindi per (la caratterizzazione di prima) $\Gamma^* \vdash \bot$ e ciò è assurdo.

Sia φ una formula, osserviamo che non può succedere che $\varphi, \neg\varphi \notin \Gamma^*$, altrimenti $\Gamma^* \vdash \varphi \wedge \neg\varphi \implies \Gamma^* \vdash \bot$ e ciò è assurdo perché Γ^* è consistente. Sia $\varphi \notin \Gamma^*$, allora $\Gamma^* \subset \Gamma^* \cup \{\varphi\}$ e, come prima per la massimalità di Γ^*, $\Gamma^* \cup \{\varphi\} \vdash \bot$, allora, per il fatto dell'ipotesi fittizia e l'introduzione dell'implicazione, si ha $\Gamma^* \vdash \varphi \to \bot = \neg\varphi$, allora per il punto precedente $\neg\varphi \in \Gamma^*$. Se $\neg\varphi \notin \Gamma^*$, allora $\Gamma^* \subseteq \Gamma^* \cup \{\neg\varphi\}$ e, stesso ragionamento, si ha $\Gamma^* \cup \{\neg\varphi\} \vdash \bot$, quindi se prendo come ipotesi fittizia $\neg\varphi$ e uso la riduzione all'assurdo, ottengo $\Gamma^* \vdash \varphi$ e dal punto precedente $\varphi \in \Gamma^*$.

3° passo: costruiamo la valutazione v che soddisfa Γ

Sia v una valutazione tale che $v(p) = 1 \iff p \in \Gamma^*$ per ogni $p \in P$. Estendiamo v a tutte le formule e facciamo vedere che $v(\alpha) = 1 \iff \alpha \in \Gamma^*$. lavoriamo per induzione sulla complessità della formula e ricordiamo che basta considerare l'insieme adeguato $\{\neg, \wedge\}$ per ottenere tutte le formule. Sia α una formula di complessità n. Se $n = 1$, allora $\alpha = p$ e per definizione $v(\alpha) = 1\Gamma^*$. Se $n > 1$, sia $\alpha = \neg\beta$, allora la complessità di β è $n-1$ e quindi posso applicare l'ipotesi induttiva, cioè abbiamo $v(\alpha) = 1 \iff v(\beta) = 0 \iff \beta \notin \Gamma^*$, ma per la proprietà precedente abbiamo che $v(\alpha) = 1 \iff \alpha = \neg\beta \in \Gamma^*$. Sia ora $\alpha = \beta \wedge \gamma$, allora β e γ hanno complessità $n-1$, quindi per ipotesi induttiva si ha $v(\alpha) = 1 \iff v(\beta) = 1 \wedge v(\gamma) = 1 \iff \beta \in \Gamma^* \wedge \gamma \in \Gamma^*$. Ora vogliamo far vedere che $\beta \in \Gamma^* \wedge \gamma \in \Gamma^* \iff \beta \wedge \gamma \in \Gamma^*$. Se $\beta, \gamma \in \Gamma^*$, allora, per introduzione della congiunzione, $\Gamma^* \vdash \beta \wedge \gamma$ e per la proprietà precedente, $\beta \wedge \gamma \in \Gamma^*$, viceversa se $\beta \wedge \gamma \in \Gamma^*$ allora, per eliminazione della congiunzione, $\Gamma^* \vdash \beta, \gamma$ e per la proprietà precedente, $\beta, \gamma \in \Gamma^*$. Quindi abbiamo dimostrato che v ha la proprietà richiesta. Ovviamene si ha $v \models \Gamma^*$, allora $v \models \Gamma$ perché $\Gamma \subseteq \Gamma^*$, per cui Γ è soddisfacibile. □

Osservazione 3.4. Nota che anche questo teorema, come per (Teorema 3.2), si dimostra col lemma di Zorn.

Teorema 3.6 (Teorema di completezza (calcolo proposizionale))**.** *Sia Σ un insieme di formule e sia α una formula, se $\Sigma \models \alpha$ allora $\Sigma \vdash \alpha$.*

Dimostrazione. Sia per assurdo $\Sigma \nvdash \alpha$, allora per (Lemma 3.4) e (Teorema 3.5) e (Teorema 2.8), si ha $\Sigma \cup \{\neg\alpha\}$ consistente $\iff \Sigma \cup \{\neg\alpha\}$ soddisfacibile $\iff \Sigma \not\models \alpha$ e questo è assurdo. □

Teorema 3.7 (Teorema di validità e completezza (calcolo proposizionale))**.** *Sia Σ un insieme di formule e sia α una formula, allora*

$$\Sigma \vdash \alpha \iff \Sigma \models \alpha$$

Osservazione 3.5. Questo teorema lega i concetti di dimostrabilità e di soddisfacibilità di una formula.

Definizione 3.8 (Insieme di formule completo)**.** Sia Σ un insieme di formule tale che per ogni formula α si ha $\Sigma \vdash \alpha$ o $\Sigma \vdash \neg\alpha$, allora Σ si dice *completo*.

Questa parte viene trattata anche in [Dal08, p.60] (parla dei linguaggi ma non so se è il linguaggio del calcolo dei predicati, anche se credo di sì, o dei "linguaggi delle materie di studio") e in [Dal08, p.68] (qui ci stanno proprio simboli di predicati, ecc)

Capitolo 4

Linguaggi del prim'ordine

Al fine di "descrivere tutta la matematica", abbiamo bisogno di due cose: del calcolo dei predicati (e dei suoi "simboli aggiuntivi") e di un linguaggio adatto a parlare di una certa materia di studio, questo linguaggi vengono detti *linguaggi del prim'ordine* (mi ricordo così ma vedi Wikipedia, ho messo dei link)

Definizione 4.1 (Linguaggio)**.** Sia $\mathcal{L}$ un insieme di simboli, allora $\mathcal{L}$ si dice *linguaggio*.

Definizione 4.2 ($\mathcal{L}$-struttura)**.** VEDI PAG 57 VAN DALEN, MA SOPRATTUTTO [Dal08, p.70] (no comunque non sono la stessa cosa, l'insieme dei termini appare dopo... Quindi credo che sia una definizione diversa, perché lì non si parla di relazioni o predicati, però comunque il dominio di I non mi è chiaro)

Siano $\mathcal{L}$ un linguaggio, si dice $\mathcal{L}$*-struttura* una coppia del tipo $(\mathcal{M}, I)$, con $\mathcal{M}$ insieme non vuoto e I funzione detta *interpretazione* tale che

- Ad un simbolo di costante "c" associa il corrispondente elemento $c^{\mathcal{M}}$ in $\mathcal{M}$
- Ad un simbolo di funzione "f_k^n" associa la funzione $f_k^n : \mathcal{M}^n \to \mathcal{M}$
- Ad un simbolo di relazione (predicato) "P_k^n" associa l'insieme $P_k^n \subseteq \mathcal{M}^n$

Quindi io credo che in certo senso I vada "dall'insieme dei simboli del linguaggio" (credo che sia $\mathcal{L}$) a $\mathcal{M}$. Dopo si parla dell'insieme dei termini $\mathcal{T}$ ma credo che rientri in una definizione diversa.

Osservazione 4.1. Dato un linguaggio $\mathcal{L}$, posso ottenere diverse $\mathcal{L}$-strutture del tipo $(\mathcal{M}, I)$, a seconda di I, cioè a seconda di come interpreto i simboli del linguaggio ottengo "un insieme delle interpretazioni $\mathcal{M}$".

Esempio 4.1. Sia $\mathcal{L}$ un linguaggio atto a descrivere i gruppi, cioè contenente un simbolo di costante ed uno di funzione $\{f, c\} \subseteq \mathcal{L}$, e consideriamo due $\mathcal{L}$-strutture $(\mathbb{Z}, I_1)$ e $(\mathbb{R}, I_2)$, tali che

$$I_1(c) = 0, \quad I_1(f) = +$$

$$I_2(c) = 1, \quad I_2(f) = \cdot$$

Più brevemente, senza citare le interpretazioni I_1, I_2, si dice che $(\mathbb{Z}, +, 0)$ e $(\mathbb{R}, \cdot, 1)$ sono $\mathcal{L}$-strutture (implicitamente abbiamo già interpretato i simboli di costante e funzione).

Definizione 4.3. "Prendo un insieme di termini, lo chiudo per relazione, questa è una formula atomica. Ad esempio $x + y = 0$".

Definizione 4.4 (Formula chiusa)**.** Una formula si dice *chiusa* se tutte le variabili sono sotto l'azione di un quantificatore.

Definizione 4.5 (Variabile libera)**.** Una variabile in un formula si dice *libera* se non è sotto l'azione di nessun quantificatore, altrimenti si dice *vincolata*.

Osservazione 4.2. Nota che tute le formule viste in calcolo proposizionale possono essere viste come formule chiuse, in quanto non esistono variabili libere (pensa ad esempio ad una formula φ, che variabili libere ha? Nessuna).

Se ho una formula chiusa posso sempre dire se la formula è "vera", mentre se ho una formula con variabili libere, "dipende dal valore della variabili libera", questa osservazione è alla base dell'idea di soddisfacibilità alla Tarski.

Definizione 4.6 (Insieme dei termini)**.** Sia $\mathcal{L}$ un linguaggio, il più piccolo insieme $\mathcal{T}$ tale che

1. Contiene i simboli di costante e di variabile

$$c_i, x_i \in \mathcal{T}$$

2. Contiene le immagini di termini

$$t_1, \dots, t_{a_i} \in \mathcal{T} \implies f_i(t_1, \dots, t_{a_i}) \in \mathcal{T} \quad \forall\, 1 \leqslant i \leqslant m$$

Chi è a_i???

si dice *insieme dei termini* e si denota $\mathcal{T}$.

I termini sono variabili, costanti o funzioni applicate a termini.

Definizione 4.7 (Interpretazione insieme dei termini)**.** Sia $\mathcal{M}$ una $\mathcal{L}$-struttura (una $\mathcal{L}$-struttura sarebbe una coppia, qui stiamo sottointendendo la funzione di interpretazione I) e sia s una successione di $\mathcal{M}$, posso definire la funzione

$$s^* : \mathcal{T} \to \mathcal{M}$$

Sia $t \in \mathcal{T}$ un termine, allora se

1. t è una variabile, allora poiché l'insieme delle variabili è numerabile si ha $t = x_i$, con x_i variabile e i naturale e a t associo l'elemento s_i della successione s, cioè $s^*(t) = s^*(x_i) = s_i$

2. t è una costante, cioè $t = c$ con c costante, allora $s^*(t) = s^*(c) = c^{\mathcal{M}}$ elemento di $\mathcal{M}$ dato dall'interpretazione fissata dal $\mathcal{L}$-linguaggio (io credo che fissata l'interpretazione I, sia $s^*(c) = I(c) = c^{\mathcal{M}}$)

3. t è la valutazione di una funzione, cioè $t = f_k^n(t_1, \dots, t_n)$ dove f_k^n è una funzione e $t_1, \dots, t_n$ sono termini, allora $s^*(t) = s^*(f_k^n(t_1, \dots, t_n)) = (f_k^n)^{\mathcal{M}}(s^*(t_1), \dots, s^*(t_n))$ (ricorda che $(f_k^n)^{\mathcal{M}} : \mathcal{M}^n \to \mathcal{M}$ e che coincide con $I(f_k^n)$) che è la valutazione della funzione con quelle date variabili (tutto interpretato in $\mathcal{M}$).

Nota che la funzione s^* è definita in modo ricorsivo nel caso (3).

Osservazione 4.3. Credo che si possa vedere s^* come "complementare" alla funzione di interpretazione I (nel senso che è "può fare delle cose che I non può fare e viceversa", ricorda però che I è fissata una volta fissata la $\mathcal{L}$-struttura, mentre s^* dipende dalla successione s), perché I interpreta le costanti e s^* lo fa uguale, ma interpreta anche le funzioni mentre s^* interpreta solo le valutazioni di funzioni; infine s^* interpreta le variabili, fissata una successione (cioè in realtà quello che fa è che alle variabili scritte in simboli sostituisce un valore "vero e proprio" che sta nella successione di elementi di $\mathcal{M}$, come quando valuti $f(3,5)$) a partire da una funzione $f(x,y) = x^2 + y$, devi "sostituire" ai simboli "x" e "y" rispettivamente i valori 3 e 5 e devi anche interpretare il simbolo di somma, che è una funzione).

In sostanze I interpreta le costanti, i predicati (rappresentano proprietà/relazioni fra termini) e le funzioni, quindi interpreta "tutte le costanti di $\mathcal{M}$" (in certo senso anche le funzioni e le relazioni sono costanti, perché non cambiano sono tutti insiemi, potresti anche dire il contrario, che anche funzioni che costanti sono delle delle relazioni, ma il senso resta questo), mentre s^*, fissata la successione s, "mette i valori alle variabili", quindi per esprimere un qualcosa con variabili libere, hai bisogno di entrambe. Nota che normalmente nessuno fa il ragionamento, ad esempio data la formula $x_1 + x_2 = 0$, "ora prendo la successione (1, -1) la sostituisco alle variabili proposizionali x_1 e x_2 e vedo che la formula è soddisfatta" (senza considerare il fatto che $+$ sarebbe un simbolo di funzione, $=$ esprime una proprietà e 0 è un simbolo di costante, nessuno considera tutte queste cose!), si dice direttamente "1 - 1 = 0", quindi nel linguaggio "colloquiale" tutti questi formalismi sono sottintesi.

Lemma 4.1. *Sia t un termine $t = t(x_1, \dots x_k)$ che dipende dalle k variabili $x_1, \dots x_k$ e siano s, $\bar{s}$ successioni di elementi di $\mathcal{M}$ tali che $s_i = \bar{s}_i$ per ogni $i \in \{1, \dots, k\}$, allora $s^*(t) = \bar{s}^*(t)$.*

Dimostrazione. Non dimostrato □

Definizione 4.8 (Soddisfacibilità alla Tarski, formula soddisfacibile in una $\mathcal{L}$-struttura)**.** Sia $\mathcal{M}$ una $\mathcal{L}$-struttura e siano $\alpha = \alpha(x_1, \dots, x_k)$ una formula dipendente da k variabili (quindi libere, l formule chiuse non dipendono da variabili), e s una successione di elementi di $\mathcal{M}$ tali che

1. Se α è una formula atomica, cioè $\alpha(x_1, \dots, x_k) = P(t_1(x_1, \dots, x_k), \dots, t_n(x_1, \dots, x_k))$, allora $(s^*(t_1), \dots, s^*(t_n)) \in P^{\mathcal{M}}$

2. Se $\alpha(x_1, \dots, x_k) = \neg\beta(x_1, \dots, x_k)$ allora s non soddisfa β

3. Se $\alpha(x_1,\dots,x_k) = \beta_1(x_1,\dots,x_k) \wedge \beta_2(x_1,\dots,x_k)$, allora s soddisfa β_1 e s soddisfa β_2
4. Se $\alpha(x_1,\dots,x_k) = \beta_1(x_1,\dots,x_k) \vee \beta_2(x_1,\dots,x_k)$, allora s soddisfa β_1 o s soddisfa β_2
5. Se $\alpha(x_1,\dots,x_k) = \beta_1(x_1,\dots,x_k) \to \beta_2(x_1,\dots,x_k)$, allora s non soddisfa β_1 o s soddisfa β_2
6. Se $\alpha(x_1,\dots,x_k) = \beta_1(x_1,\dots,x_k) \leftrightarrow \beta_2(x_1,\dots,x_k)$, allora s soddisfa sia β_1 che β_2 o s non soddisfa né β_1 né β_2
7. Se $\alpha(x_1,\dots,x_k) = \forall x_j \beta(x_1,\dots,x_k,x_j)$, allora per ogni successione s' che differisce da s in al più da j s' soddisfa $\beta(x_1,\dots,x_j,\dots,x_k)$
8. Se $\alpha(x_1,\dots,x_k) = \exists x_j \beta(x_1,\dots,x_k,x_j)$, allora esiste una successione s' che differisce da s in al più da j tale che s' soddisfa $\beta(x_1,\dots,x_j,\dots,x_k)$

allora si dice che *s soddisfa la formula α in $\mathcal{M}$*.

Osservazione 4.4. L'espressione "s' che differisce da s in al più da j" significa che $s(i) = s'(i),\ \forall\, i \neq j$; cioè le successioni in generale sono uguali ovunque, tranne in j dove possono coincidere oppure no. Inoltre la scrittura $\beta(x_1,\dots,x_k,x_j)$ significa che $j \in \{1,\dots,k\}$ ma ovviamente $\alpha = \forall x_j \beta(x_1,\dots,x_k,x_j)$ non dipende da x_j (lo stesso se c'è $\exists$), cioè per essere più espliciti si potrebbe scrivere $\alpha = \alpha(x_1,\dots,x_{j-1},x_{j+1},\dots,x_n)$, quindi α non dipende da x_j però in β compare x_j con un quantificatore universale.

Per una definizione di variabile libera in una formula vedi: [Dal08, p.66]

Notazione 4.9 (Successione che soddisfa una formula in una $\mathcal{L}$-struttura)**.** Siano $\mathcal{M}$ una $\mathcal{L}$-struttura e α una formula, se una successione s di elementi di $\mathcal{M}$ soddisfa α in $\mathcal{M}$ si scrive

$$\mathcal{M} \models \alpha[s]$$

Proprietà 4.2. *Siano $\mathcal{M}$ una $\mathcal{L}$-struttura e α una formula, se una successione s di elementi di $\mathcal{M}$ non soddisfa α in $\mathcal{M}$ allora s soddisfa $\neg\alpha$ in $\mathcal{M}$*

Esempio 4.2. Sia $\mathcal{L} \supseteq \{f,c\}$ un linguaggio atto a descrivere i gruppi e consideriamo le due $\mathcal{L}$-strutture $\mathcal{M} = (\mathbb{Z},+,1)$ e $\mathcal{N} = (D_{2n},\cdot,id)$, dove D_{2n} è il gruppo diedrale di ordine $2n$, allora la formula

$$\alpha = \forall y(f(x,y) = f(y,x))$$

ha come variabile libera $x = x_1$ (mentre $y = x_2$), è soddisfatta per ogni successione di elementi di $\mathbb{Z}$ perché la somma $+$ in $\mathbb{Z}$ è commutativa, mentre non lo è il prodotto $\cdot$ in D_{2n}, quindi le successioni di D_{2n} che soddisfano α sono tutte e sole le successioni con s tali che $s_1 \in Z(D_{2n})$.

Altri esempi

Teorema 4.3 (Teorema di coincidenza)**.** *Siano $\mathcal{M}$ una $\mathcal{L}$-struttura e $\alpha(x_0,\dots,x_k)$ formula se $s(i) = \overline{s}(i)$ per ogni $i = 0,\dots,k$, allora*

$$\mathcal{M} \models \alpha[s] \iff \mathcal{M} \models \alpha[\overline{s}]$$

Osservazione 4.5. potrei avere infinite successioni diverse che soddisfano la stessa formula, purché coincidano sugli indici con cui compaiono le variabili libere della formula.

Dimostrazione. Non dimostrata. Però credo che si usi il lemma non dimostrato precedente. □

Notazione 4.10 (Soddisfacibilità di una formula)**.** Siano $s = (s_1,\dots,s_n,\dots)$ una successione e $\alpha(x_1,\dots,x_n)$ formula, se s soddisfa α in $\mathcal{M}$ si scrive

$$\mathcal{M} \models \alpha(x_1 \dots x_n)[s_1 \dots s_n]$$

Osservazione 4.6. Questa notazione è giustificata perché per Teorema 4.3 la soddisfacibilità di una formula $\alpha(x_1,\dots,x_n)$ che dipende n variabili libere dipende solo dai primi n termini della successione (in questo caso $s_1,\dots,s_n$).

Osservazione 4.7 (Significato di soddisfacibilità con "per ogni" e "esiste"). Siano $\alpha(x_0,\dots,x_n) = \forall x_j \beta(x_0,\dots,x_n,x_j)$ e $s = (b_0,\dots,b_n\dots)$ una successione, allora dire che

$$\mathcal{M} \models \alpha(x_0,\dots,x_n)[b_0,\dots,b_n]$$

equivale a dire che per ogni $a \in \mathcal{M}$ si ha

$$\mathcal{M} \models \beta\,(x_0 \dots x_n, x_j)\,[b_0 \dots b_n, a]$$

mentre se $\alpha(x_0,\dots,x_n) = \exists x_j \beta(x_0,\dots,x_n,x_j)$, allora dire che

$$\mathcal{M} \models \alpha(x_0,\dots,x_n)[b_0,\dots,b_n]$$

equivale a dire che esiste $a \in \mathcal{M}$ tale che

$$\mathcal{M} \models \beta\,(x_0 \dots x_n, x_j)\,[b_0 \dots b_n, a]$$

Definizione 4.11 (Formula vera in una $\mathcal{L}$-struttura)**.** Siano $\mathcal{M}$ una $\mathcal{L}$-struttura e α una formula, se ogni successione di elementi di $\mathcal{M}$ soddisfa α allora si dice che α è *una formula vera in* $\mathcal{M}$.

Notazione 4.12 (Formula vera in una $\mathcal{L}$-struttura)**.** Siano $\mathcal{M}$ una $\mathcal{L}$-struttura e α una formula, se α è una formula vera in $\mathcal{M}$, allora si scrive

$$\mathcal{M} \models \alpha$$

Osservazione 4.8. Se α non è vera in $\mathcal{M}$, posso dire che $\neg\alpha$ è vera? Nope. Però puoi dire che α è vera se e solo se $\neg\alpha$ non è soddisfacibile.

Proposizione 4.4. *Siano $\mathcal{M}$ una $\mathcal{L}$-struttura e α una formula, se α è una formula chiusa, allora α oppure $\neg\alpha$ risulta vera in $\mathcal{M}$.*

Definizione 4.13 (Formula soddisfacibile (senza fissare una $\mathcal{L}$-struttura))**.** Sia $\mathcal{L}$ un linguaggio, una formula α è detta soddisfacibile se esiste una $\mathcal{L}$-struttura $\mathcal{M}$ e una successione s che soddisfa α in $\mathcal{M}$.

Osservazione 4.9. Nota che il linguaggio è fissato, mentre la $\mathcal{L}$-struttura no. Ma non possono esistere formule soddisfacibili per qualsiasi linguaggio? Beh sì, pensa al calcolo proposizionale, sono tutte e solo le tautologie, però senza fissare alcun linguaggio (cose del tipo $\varphi \to \varphi$).

Definizione 4.14 (Formula logicamente valida (senza fissare una $\mathcal{L}$-struttura))**.** Siano $\mathcal{L}$ un linguaggio e α una formula, se per ogni $\mathcal{L}$-struttura $\mathcal{M}$ e ogni successione s di elementi di $\mathcal{M}$ s soddisfa α in $\mathcal{M}$, allora α si dice *logicamente valida*. Cioè la formula α è vera in ogni $\mathcal{L}$-struttura.

Notazione 4.15 (Formula logicamente valida)**.** Sia α una formula, se è logicamente valida si denota

$$\models \alpha$$

Teorema 4.5 (Teorema di Church)**.** *Non esiste un algoritmo che permette di stabilire, data una formula α, se essa è una formula logicamente valida.*

Dimostrazione. Non dimostrato □

Definizione 4.16 (Conseguenza logica di una formula)**.** Siano α,β formule, si dice che β è conseguenza logica di α se per ogni $\mathcal{L}$-struttura $\mathcal{M}$ e ogni successione s tale che $\mathcal{M} \models \alpha[s]$ allora $\mathcal{M} \models \beta[s]$.

Osservazione 4.10. Nota la somiglianza (anche formale) con la definizione di conseguenza logica nel calcolo proposizionale, in quel caso avevamo che se $v \models \alpha \implies v \models \beta$.

Osservazione 4.11. Se α e β sono formule chiuse allora β è conseguenza di α se per ogni $\mathcal{L}$-struttura $\mathcal{M}$ si ha

$$\mathcal{M} \models \alpha \implies \mathcal{M} \models \beta$$

Notazione 4.17 (Conseguenza logica di una formula)**.** Siano α,β formule, se β è conseguenza logica di α si scrive

$$\alpha \models \beta$$

Esercizio 4.1. Dimostrare che

$$(\forall x_i\,\alpha \to \beta) \models (\alpha \to \forall x_i \beta)$$

Esercizio 4.2. Esercizio lungo con "$\sigma_1, \sigma_2, \sigma_3$"

Proprietà 4.6 (Caratterizzazione formula vera in una $\mathcal{L}$-struttura)**.** *Sia $\mathcal{L}$ un linguaggio e siano $\mathcal{M}$ una $\mathcal{L}$-struttura e α una formula, allora $\mathcal{M} \models \alpha$ se e solo se $\mathcal{M} \models \forall x_i\,\alpha$*

Dimostrazione. Se non sbaglio è lunghetta, servirà dopo. E' un esercizio □

Esercizio 4.3. Dimostrare che

$$(\forall x_i\,\alpha \to \beta) \to (\alpha \to \forall x_i \beta)$$

dove x_i non compare libera in α, è una formula logicamente valida.

Definizione 4.18 (Formule logicamente equivalenti)**.** Siano α, β formule, si dice che α è logicamente equivalente a β se

$$\alpha \models \beta \wedge \beta \models \alpha$$

Osservazione 4.12. Nota che questa espressione è data come definizione di formule logicamente equivalenti in calcolo dei predicati, mentre in calcolo proposizionale la usiamo come caratterizzazione (Corollario 2.7.1).

Definizione 4.19 (Insieme di formule chiuse soddisfacibili)**.** Siano $\mathcal{L}$ un linguaggio e Σ un insieme di formule chiuse, allora Σ si dice soddisfacibile se esiste una $\mathcal{L}$-struttura $\mathcal{M}$ tale che ogni formula di Σ è vera in $\mathcal{M}$

Osservazione 4.13. OSSERVAZIONE MIA (a tuo rischio e pericolo): Ti potresti chiedere qual è il legame fra la soddisfacibilità del calcolo proposizionale e quella del calcolo dei predicati. Secondo me, come detto altrove, puoi passare dal calcolo dei predicati al calcolo proposizionale semplicemente considerando un linguaggio vuoto (già hai tutti i simboli che ti servono) e di considerare tutte le formula come chiuse, però devi trovare il modo di ottenere una valutazione a partire dal concetto di soddisfacibilità alla Tarski, nota inoltre che l'insieme dei termini in questo caso coincide con l'insieme delle variabili proposizionali. Definirei una valutazione v tale che $v(p) = 1 \iff s^*(p) \in \mathcal{M}$ (ma che succede alla $\mathcal{L}$-struttura se il linguaggio è vuoto? pensaci, magari mi sbaglio), dove $p \in P$ e s è una successione di elementi di $\mathcal{M}$ (perché posso dire che è una qualsiasi successione? Perché la formula è chiusa, quindi o vera in $\mathcal{M}$ o è vera la sua negata, cioè o è soddisfatta da tutte le successioni o da nessuna). Ora dovresti passa dal calcolo proposizionale a quello dei predicati, quindi dovresti costruire una $\mathcal{M}$ struttura in cui la formula è vera (non ci ho ancora pensato).

Definizione 4.20 (Modello)**.** Siano $\mathcal{L}$ un linguaggio e Σ un insieme chiuso di formule, una $\mathcal{L}$-struttura $\mathcal{M}$ è detta modello di Σ, se ogni formula di Σ è vera in $\mathcal{M}$.

Osservazione 4.14. Un insieme di formule è soddisfacibile se e solo se ammette un modello.

Notazione 4.21 (Modello)**.** Siano $\mathcal{L}$ un linguaggio, Σ un insieme chiuso di formule e $\mathcal{M}$ una $\mathcal{L}$-struttura, denotiamo un modello $\mathcal{M}$ di Σ con la scrittura

$$\mathcal{M} \models \Sigma$$

Esempio 4.3. Sia $\mathcal{L} \supseteq \{f, c\}$ un linguaggio atto a descrivere i gruppi e sia $\Sigma_g = \{\forall x \forall y \forall z (f(f(x,y),z) = f(x, f(y,z))), \forall x \exists y (f(x,y) = c), \forall x (f(x,c) = f(c,x) = x)\}$ insieme di formule, allora un gruppo $(G, \cdot, 1)$ è un modello di Σ_g, in quanto le formule di Σ_g possono essere interpretate come: proprietà associatività, esistenza dell'elemento neutro e invertibilità degli elementi, nota che la stabilità non è espressa esplicitamente, però la puoi vedere contenuta nella definizione di $\mathcal{L}$-struttura (pensa ad esempio all'espressione $f(f(x,y),z)$ non avrebbe senso se non fosse $f(x,y) \in G$, però secondo me non è comunque giustificato).

Definizione 4.22 (Conseguenza logica di un insieme di formule)**.** Sia Σ un insieme di formule e sia α una formula. Si dice che α *è conseguenza logica di* Σ, se per ogni $\mathcal{L}$-struttura $\mathcal{M}$ e per ogni successione s che soddisfa ogni formula di Σ in $\mathcal{M}$, s soddisfa anche α in $\mathcal{M}$.

Notazione 4.23 (Conseguenza logica di un insieme di formule)**.** Sia Σ un insieme di formule e sia α una formula. Se α è conseguenza logica di Σ, scriviamo

$$\Sigma \models \alpha$$

Esempio 4.4 (Formula conseguenza logica di un insieme di formule). Siano $\Sigma_g = \{\forall x \forall y \forall z (f(f(x,y),z) = f(x, f(y,z))), \forall x \exists y (f(x,y) = c), \forall x (f(x,c) = f(c,x) = x)\}$ e $\sigma = \forall x \forall y \forall z ((f(x,y) = c \wedge f(x,z) = c) \to y = z)$, allora $\Sigma \models \alpha$.

Definizione 4.24 (Insieme dei modelli di un insieme di formule chiuse)**.** Siano $\mathcal{L}$ un linguaggio e Σ un insieme di formule chiuse, l'insieme

$$\mathrm{Mod}(\Sigma) := \{\mathcal{M}\ \mathcal{L}\text{-struttura} : \mathcal{M} \models \Sigma\}$$

si dice *BOHHHH (Ma ha un nome?)*.

Che ne so che è un insieme? Poi la prof parla di "classe di $\mathcal{L}$-strutture", però credo che si riferisca ad altro, questo dovrebbe essere un insieme per qualche motivo.

Definizione 4.25 (Classe di $\mathcal{L}$-strutture assiomatizzabile)**.** Sia $\mathcal{L}$ un linguaggio, una classe di $\mathcal{L}$-strutture $\mathcal{K}$ si dice *assiomatizzabile* se esiste un insieme di formule chiuse Σ tale che

$$\mathrm{Mod}(\Sigma) = \mathcal{K}$$

se Σ è finito, $\mathcal{K}$ si dice *finitamente assiomatizzabile*.

Osservazione 4.15. Nota che "più grande" è Σ e "più piccolo" è $\mathrm{Mod}(\Sigma)$ e viceversa (perché se ci sono più formule in Σ, allora ci sono meno $\mathcal{L}$-strutture $\mathcal{M}$ che soddisfano Σ, per cui quando devi chiedere delle proprietà in più ad una classe di $\mathcal{L}$-strutture $\mathcal{K}$, devi aspettarti che, se è assiomatizzabbile, ci vorranno "più formule" in Σ, dopo farai l'esempio dell'assiomatizzazione dei gruppi e dei gruppi infiniti e nel secondo caso avrai bisogno di più formule).

Esempio 4.5 (Classe dei gruppi). Sia $\mathcal{L}$ un linguaggio atto a descrivere i gruppi, allora la classe dei gruppi (tutte le $\mathcal{L}$-strutture interpretate come gruppi) è finitamente assiomatizzabile da Σ_g (vedi prima). Inoltre la classe dei gruppi infiniti è assiomatizzabile ma non finitamente Σ_g e le seguenti formule:

$$\exists x_1 \exists x_2 (\neg(x_1 = x_2))$$

$$\exists x_1 \exists x_2 \exists x_3 (\neg(x_1 = x_2) \wedge \neg(x_1 = x_3) \wedge \neg(x_2 = x_3))$$

$$\vdots$$

che sono infinite

Esempio 4.6 (Classe dei campi). La classe dei campi, analogamente a quella dei gruppi, è finitamente assiomatizzabile da Σ_C, mentre la classe dei campi con caratteristica 0 è assiomatizzabile ma non finitamente, perché dobbiamo esprimere la proprietà di essere campo (mediante Σ_C, che è finito) e che la caratteristica del campo non è un numero primo e i numeri primi sono infiniti (quindi avremo infinite formule).

Definizione 4.26 (Termine libero per una variabile in una formula)**.** Siano $\mathcal{L}$ un linguaggio e $\alpha(x)$ una formula con una variabile libera x (ma potrebbe averne anche di più) e sia $t(x_1, \ldots, x_n)$ un termine tale che le variabili presenti in t non sono sotto l'azione di nessun quantificatore presente in α, allora t si dice *termine libero per x in $\alpha(x)$*. Quindi quando sostituisco t ad x in α la variabili in t non devono essere sotto l'azione di nessun quantificatore. DA QUESTA DEFINIZIONE NON EMERGE IL RUOLO DI x, quindi o l'ho scritta male... Boh

Osservazione 4.16. Nota che una variabile libera x in una formula è sempre un termine libero per x in α (questa definizione è una generalizzazione), quindi se pongo $t = x$, allora t è libero per x in $\alpha(x)$, se t è una costante allora t è libero per qualsiasi variabile in α (perché le costanti non possono essere sotto l'azione di quantificiatori per definizione).

Esempio 4.7. Consideriamo un linguaggio $\mathcal{L} \supseteq \{<\}$, allora la formula

$$\alpha(x) = \forall y (x < y \to x = 0)$$

ammette $t_1(x, z) = x + z$ come termine libero per x in α, mentre $t_2(y, z) = y + z$ non lo è perché y compare sotto l'azione del quantificatore $\forall$ in α.

Infatti se sostituisco t_1 a x ottengo

$$\alpha(t_1) = \forall y (x + z < y \to x + z = 0)\,,$$

mentre se sostituisco t_2

$$\alpha(t_2) = \forall y (y + z < y \to x + y = 0)$$

e questo in un certo senso "cambia il senso della formula".

Introduzione ed eliminazione del per ogni

Ripetizione insieme delle dimostrazioni, formule dimostrabili a partire da un insieme di formule, teorema

Teorema 4.7. *Sia Γ un insieme di formule, si ha*

1. *Se x non compare libera in Γ, $\Gamma \vdash \alpha(x)$, allora $\Gamma \vdash \forall x \alpha(x)$.*
2. *Se $\Gamma \vdash \forall x \alpha(x)$, allora $\Gamma \vdash \alpha(t)$, con t termine libero per x in $\alpha(x)$.*

Esercizio 4.4. Dimostrare che:

1. $\forall x \varphi(x) \wedge \forall x \psi(x) \vdash \forall x (\varphi(x) \wedge \psi(x))$
2. $\varphi \to \forall x \psi(x) \vdash \forall x (\varphi \to \psi(x))$
3. $\neg \forall x \alpha(x) \vdash \exists x \neg \alpha(x)$

Teorema 4.8 (Teorema di validità (calcolo dei predicati))**.** *Sia $\mathcal{L}$ un linguaggio, siano Σ un insieme di formule chiuse e α una formula, allora*

$$\Sigma \vdash \alpha \implies \Sigma \models \alpha$$

Dimostrazione. $\implies$) La parte iniziale della dimostrazione è uguale a (Teorema 3.2): si considera una dimostrazione $\alpha_1, \dots, \alpha_n$ di α, si procede per induzione nella seconda forma su n e per $n = 1$ l'assero è ovvio, per $n > 1$ consideriamo l'ultima regola di deduzione applicata per ottenere α. Tutti i casi già visti nella dimostrazione precedente continuano a valere[1], devi considerare i "casi aggiuntivi" del calcolo dei predicati.

Se la regola è l'introduzione del per ogni I$\forall$, allora esiste una formula $\beta(x)$ con una variabile libera x in β che non compare libera nelle derivazioni precedenti e in Σ tale che $\alpha = \forall x \beta(x)$. Allora $\Sigma \vdash \beta(x)$ e la dimostrazione di $\beta(x)$ ha lunghezza $m < n$, quindi per ipotesi induttiva, $\Sigma \models \beta(x)$, cioè per ogni $\mathcal{M}$ modello di Σ (posso direttamente parlare di modello e non di $\mathcal{L}$-struttura e successione, perché so che Σ è un insieme di formule chiuse) si ha $\mathcal{M} \models \beta(x)$. Allora, per (Proprietà 4.6), $\mathcal{M} \models \forall x \beta(x) = \alpha$, quindi $\Sigma \models \alpha$.

Se la regola è l'eliminazione del per ogni E$\forall$, allora esiste una formula $\beta(x)$ con una variabile libera x in β tale che $\alpha = \beta(t)$ con t termine libero per x in $\beta(x)$ e $\Sigma \vdash \forall x \beta(x)$. Allora la lunghezza della dimostrazione di $\forall x \beta(x)$ è di lunghezza inferiore a n e per ipotesi induttiva $\Sigma \models \forall x \beta(x)$, cioè per ogni $\mathcal{M}$ modello di Σ si ha $\mathcal{M} \models \forall x \beta(x) \iff \mathcal{M} \models \beta(x)$, quindi per ogni $a \in \mathcal{M}$ $\mathcal{M} \models \beta(x)[a]$. Noi vogliamo far vedere che $\mathcal{M} \models \beta(t)$, cioè per ogni successione s di $\mathcal{M}$ $\models \beta(t)[s]$, ovvero $\mathcal{M} \models \beta(x)[s^*(t)]$ (perché?) e questo è vero poiché $s^*(t) \in \mathcal{M}$ e per quanto detto prima (ma non è per definizione?), per cui $\Sigma \models \alpha$.

Manca il caso dell'introduzione dell'esistenziale e dell'eliminazione dell'esistenziale (la prof non li dimostra).

In ogni caso si ha l'asserto. □

Teorema 4.9 (Caratterizzazione esistenza di modelli di un insieme di formule chiuse)**.** *Γ insieme di formule chiuse è consistente $\iff$ Γ ha un modello*

Osservazione 4.17. Nota la somiglianza con (Teorema 3.5).

Dimostrazione. Non è dimostrato. □

Lemma 4.10. *Sia Γ insieme di formule chiuse, allora*

$$\Gamma \nvdash \alpha \iff \Gamma \cup \{\neg\alpha\} \text{ è consistente}$$

Dimostrazione. $\implies$) Vero per (Lemma 3.4).

$\impliedby$) Io ragionerei per assurdo e userei l'introduzione della congiunzione, ma la prof fa una dimostrazione più lunga. E usa il teorema precedente. □

Teorema 4.11 (Teorema di completezza (calcolo dei predicati))**.** *Sia $\mathcal{L}$ un linguaggio, siano Σ un insieme di formule chiuse e α una formula, allora*

$$\Sigma \models \alpha \implies \Sigma \vdash \alpha$$

Dimostrazione. Sia per assurdo che $\Sigma \nvdash \alpha$, allora, per il lemma precedente, $\Sigma \cup \{\neg\alpha\}$ è consistente e per il teorema precedente, $\Sigma \cup \{\neg\alpha\}$ ammette un modello $\mathcal{M}$, cioè $\mathcal{M} \models \Sigma \cup \{\neg\alpha\}$. Allora $\mathcal{M} \models \neg\alpha$ e $\mathcal{M} \models \Sigma$, ma poiché $\Sigma \models \alpha$, segue $\mathcal{M} \models \alpha$, ciò è assurdo perché α e $\neg\alpha$ non possono essere entrambe vere. □

Teorema 4.12 (Teorema di validità e completezza (calcolo dei predicati))**.** *Sia $\mathcal{L}$ un linguaggio, siano Σ un insieme di formule chiuse e α una formula, allora*

$$\Sigma \vdash \alpha \iff \Sigma \models \alpha$$

Osservazione 4.18. Nota che la formulazione è quasi identica a quella del calcolo proposizionale, quello che cambia è il significato di $\models$ (anche se si può far vedere la coincidenza in un certo senso). Inoltre nota che non dobbiamo fissare una $\mathbb{L}$-struttura ma solo il linguaggio, per definizione di conseguenza logica 8del calcolo dei predicati).

[1] A patto che dimostri, e non l'abbiamo fatto, che, nei casi del calcolo proposizionale, l'essere conseguenza logica di un insieme di formule per il calcolo proposizionale e per il calcolo dei predicati sono concetti coincidenti. Cioè $\models$ "ha lo stesso significato" in calcolo proposizionale e in calcolo dei predicati, quando puoi considerare entrambi

Esercizio 4.5. Dimostrare che

$$\vdash \exists\, x\varphi(x) \iff \neg\forall\, x\neg\varphi(x)$$
$$\vdash \nexists\, x\varphi(x) \iff \neg\forall\, x\neg\varphi(x)$$
$$\vdash \neg\forall\, x\varphi(x) \iff \exists\, x\neg\varphi(x)$$
$$\vdash \forall\, x\varphi(x) \iff \neg\exists\, x\neg\varphi(x)$$

Teorema 4.13 (Teorema di compattezza (calcolo dei predicati))**.** *Siano $\mathcal{L}$ un linguaggio e Σ un insieme di formule chiuse, allora Σ ha un modello $\iff$ ogni suo sottoinsieme finito ha un modello.*

Osservazione 4.19. Nota che è una generalizzazione del Teorema di completezza del calcolo proposizionale perché tutte le formule del calcolo proposizionale sono chiuse.

Dimostrazione. $\implies$) Ovvio.

$\impliedby$) Sia per assurdo che Σ non ha modelli, per (Teorema 4.9), allora Σ non è consistente, cioè $\Sigma \vdash \bot$. Allora esiste una dimostrazione di $\bot$ a partire da Σ e quindi un sottoinsieme finito $\Sigma' = \{\alpha_1, \ldots, \alpha_n\} \subseteq \Sigma$ tale che $\Sigma' \vdash \bot$, quindi Σ' è inconsistente. Allora Σ' non ha modelli, ma per ipotesi ogni sottoinsieme finito di Σ, e quindi anche Σ', ha un modello: assurdo. □

Capitolo 5

Numeri naturali

In questa sezione riprendiamo la costruzione "naive" (senza ZF) dei numeri naturali e la ricaviamo dai nostri assiomi, inoltre studiamo una generalizzazione dei naturali: i numeri ordinali, e infine ci concentriamo sui numeri cardinali. Come simbolo per denotare i numeri naturali useremo ω, ovviamente dovremo giustificare l'utilizzo di tale simbolo.

Uno dei modi "classici" per definire l'insieme dei numeri naturali è utilizzando i cosiddetti *assiomi di Peano*, come preannunciato, il nostro scopo è ottenere tali assiomi nella nostra teoria, quindi come conseguenza dei nostri assiomi. Qui vengono introdotti.

Assioma 5.1 (Assiomi di Peano)**.** *I seguenti sono gli assiomi di Peano:*

1. 0 *è un numero naturale*
2. *Se n un numero naturale, anche il suo successore è un numero naturale*
3. *Se due numeri naturali hanno lo stesso successore, allora coincidono*
4. 0 *non è successore di alcun numero naturale*
5. *Assioma d'induzione: Se X è un insieme di numeri naturali* ($X \subseteq \omega$) *tale che contiene lo* 0 ($0 \in X$) *ed è chiuso per successori* ($n \in X \implies n+1 \in X$)*, allora X contiene ogni numero naturale* ($X = \omega$)*.*

Osservazione 5.1. Osserva che l'assioma di induzione è particolarmente utile per dimostrare le proprietà dei numeri naturali, infatti si può seguire il seguente ragionamento:

Sia $P(x)$ una proprietà (abbiamo fissato un linguaggio, ecc) sui numeri naturali, se considero l'Insieme $X = \{x \in \omega : P(x)\}$ (ben definito per l'assioma di separazione e di estensionalità) e dimostro che $0 \in X$ e che è chiuso per successori, allora $X = \omega$, cioè la proprietà P vale per tutti i numeri naturali ($\forall n(n \in \omega \to P(n))$).

Adesso passiamo alla nostra costruzione formale, che è sta fornita da John von Neumann

Definizione 5.1 (Successore di un insieme)**.** Sia n un insieme, si dice *successore di n* l'insieme

$$n^+ := n \cup \{n\}$$

Definizione 5.2 (Definizione numeri naturali come insiemi)**.** Per (Osservazione 1.1) sappiamo che il simbolo $\varnothing$ rappresenta un insieme che esiste ed è unico, quindi, per gli assiomi dell'unione (o della coppia non ordinata) e di estensionalità, poniamo definire i seguenti insiemi

$$0 = \varnothing,\ 1 = 0^+ = \{0\} = \{\varnothing\},\ 2 = 1^+ = \{0,1\} = \{\varnothing, \{\varnothing\}\},\ 3 = 2^+ = \{0,1,2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\},\ \dots$$

Per adesso questi sono solo insiemi, dopo daremo la definizione di numero naturale e dovremo far vedere che i numeri naturali sono tutti e soli questi che ho elencato.

Definizione 5.3 (Insieme induttivo)**.** Sia X un insieme tale che

1. $0 \in X$
2. $x \in X \implies x^+ \in X$

Consiglio. Fai attenzione all'omonimia col concetto di insieme induttivo utilizzato nel Lemma di Zorn.

Assioma 5.2 (Assioma dell'infinito - Prima forma)**.** *Esiste un insieme induttivo.*

Definizione 5.4 (Numero naturale)**.** Un insieme che appartiene ad ogni insieme induttivo si dice *numero naturale*.

Teorema 5.1 (Esistenza dell'insieme dei numeri naturali)**.** *Esiste un insieme i cui elementi sono esattamente i numeri naturali.*

Osservazione 5.2. Per la dimostrazione di questo teorema è necessario l'assioma dell'infinito, è stato dimostrato che è impossibile altrimenti.

Dimostrazione. Per l'assioma dell'infinito, esiste un insieme induttivo X e consideriamo

$$\omega = \{x \in X : x \text{ è un numero naturale}\},$$

per ogni X, questo insieme esiste ed è unico per gli assiomi di separazione ed estensionalità.

Vogliamo dimostrare che n è un numero naturale $\iff n \in \omega$. Sia n numero naturale, allora $n \in X$ perché X è induttivo, quindi $x \in \omega$. Viceversa, sia $n \in \omega$, allora n è naturale. Quindi gli elementi di ω sono tutti e soli i numeri naturali, per l'assioma di estensionalità è unico e non dipende dall'insieme X, allora è lecito usare il simbolo "ω". □

Definizione 5.5 (Insieme dei numeri naturali)**.** Nel teorema precedente, abbiamo dimostrato l'esistenza e l'unicità dell'insieme ω, tale insieme è detto *insieme dei numeri naturali*.

Teorema 5.2 (Minimalità dell'insieme dei numeri naturali)**.** *ω è un insieme induttivo ed è sottoinsieme di ogni insieme induttivo.*

Consiglio. Puoi ricordarlo così: ω è il più piccolo insieme induttivo (rispetto all'inclusione).

Osservazione 5.3. Nota che dimostrare che ω è induttivo equivale a dimostrare che i primi due assiomi di Peano.

Dimostrazione. Vogliamo dimostrare che ω è induttivo, cioè che contiene 0 ed è chiuso per successori. Sia X un insieme induttivo, allora $0 \in X$ e 0 è un numero naturale. Sia n un numero naturale, allora $n \in X$, ma X è chiuso per successori, quindi $n^+ \in X$, cioè $n^+ \in \omega$. Onde ω è induttivo, ora dimostriamo che è il più piccolo insieme induttivo.

Siano X un insieme induttivo e $n \in \omega$, allora $n \in X$, cioè $\omega \subseteq X$. □

Il precedente teorema fornisce un metodo per dimostrare delle proprietà di ω, infatti se abbiamo $X \subseteq \omega$ i cui elementi soddisfano una certa proprietà P (ad esempio usiamo l'assioma di separazione e si ha $X = \{x \in \omega : P(x)\}$), allora $\omega \subseteq X \implies X = \omega$ e anche gli elementi di ω soddisfano la proprietà P (non so se sia proprio questo il principio di induzione, ma credo di sì, VEDI TERNE DI PEANO), in generale puoi utilizzarlo per dimostrare una proprietà di ω che sai essere vera per X.

Teorema 5.3. *Ogni numero naturale diverso da* 0 *è successore di un numero naturale.*

Osservazione 5.4. Nota che questa proprietà non appare fra gli assiomi di Peano, ma penso che si possa dimostrare anche a partire da questi.

Dimostrazione. Si definisce $X = \{n \in \omega : n = 0 \vee n \text{ è successore di un numero naturale}\} \subseteq \omega$ e si fa vedere che X è induttivo. □

Proprietà 5.4. 0 *non è successore di nessun numero naturale.*

Osservazione 5.5. E' il terzo assioma di Peano.

Dimostrazione. Si fa subito per assurdo. □

Nota che fino a questo momento abbiamo utilizzato un linguaggio $\mathcal{L}$ che contiene simboli e notazioni $(0, 1, ^+, \dots)$, quindi consideriamo delle $\mathcal{L}$-strutture (ad esempio (ω, σ), dove intendo la funzione successore), ma non lo diremo esplicitamente.

Ora introduciamo il concetto di Terna di Peano (sono $\mathcal{L}$-strutture), che generalizza delle proprietà possedute dall'insieme dei numeri naturali, quindi accompagnerò alla definizione una "nota intuitiva" per ricordare il legame con i numeri naturali. Successivamente faremo vedere che tutte le terne di Peano sono tra loro "isomorfe" (in un senso che vedremo).

Definizione 5.6 (Terna di Peano)**.** Sia $\langle M, f, e\rangle$ una terna ordinata, con M insieme non vuoto, $f : M \to M$ e $e \in M$ tale che

1. $e \notin \operatorname{ran} f$

   e non è successore di nessun elemento di M

2. f è iniettiva

   Ogni successore è unico

3. $\forall a((a \subseteq M \wedge e \in a \wedge f[a] \subseteq a) \to a = M)$

   Principio di induzione. La parte "$e \in a \wedge f[a] \subseteq a$" è come dire che a è "induttivo"

Definizione 5.7 (Funzione successore dei numeri naturali)**.** La relazione binaria $\sigma = \{\langle n, n^+\rangle : n \in \omega\}$ è una funzione e si dice *funzione successore*.

Proprietà 5.5. *La funzione successore dei naturali è iniettiva.*

Osservazione 5.6. Stiamo provando il terzo assioma di Peano.

Dimostrazione. La dimostrazione non mi sembra banale. □

Definizione 5.8 (Insieme transitivo)**.** Un insieme a si dice *transitivo* se gli elementi degli elementi di a sono elementi di a:

$$x \in y \in a \implies x \in a$$

Proposizione 5.6 (Caratterizzazione insieme transitivo)**.** *Sia a un insieme, allora le seguenti affermazioni sono equivalenti*

1. *a è transitivo*
2. *L'unione di a è contenuta in a*
$$\bigcup a \subseteq a$$
3. *Ogni elemento di a è anche un suo sottoinsieme*
$$\forall x(x \in a \to x \subseteq a)$$

Dimostrazione. Si dimostra direttamente e in modo semplice che $(1) \iff (4)$ (la prof dimostra solo questo). Il resto li hai dimostrati da solo, ma mi scoccio di scriverlo. □

Esempio 5.1 (Esempi di insiemi transitivi). I seguenti sono esempi di insiemi transitivi.

- $\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\ \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$
- $0, 1, 2, 3$
- ...

Proposizione 5.7. *Sia a un insieme, allora a transitivo se e solo se $\bigcup a^+ = a$.*

Teoricamente anche questa è una caratterizzazione, quindi potresti metterla prima, ma la prof differenzia le cose.

Dimostrazione. $\implies$) Si ha in generale $\bigcup a^+ = \bigcup a \cup \bigcup \{a\} = \bigcup a \cup a$. Sia $x \in \bigcup a \iff \exists y \in a : x \in y$, per la transitività di a, si ha $x \in a$, cioè $\bigcup a \subseteq a \implies \bigcup a^+ = a$.

$\impliedby$) Si ha $a \subseteq a^+ \implies \bigcup a \subseteq \bigcup a^+ = a$, cioè a è transitivo (per la caratterizzazione precedente). □

Teorema 5.8 (Transitività dei numeri naturali)**.** *Ogni numero naturale è un insieme transitivo.*

Dimostrazione. Sia $X = \{n \in \omega : n \text{ è transitivo}\}$, allora $0 \in X$. Siano $n \in X$, allora per (Proposizione 5.7), $\bigcup n^+ = n$ e, per (Proposizione 5.6), si ha n^+ transitivo, per cui X è induttivo e $X = \omega$. □

Dimostrazione alternativa. Sia $X = \{n \in \omega : n \text{ è transitivo}\}$, allora $0 \in X$. Siano $n \in X$ e $x \in n^+ = n \cup \{n\}$, allora $x \in n$ o $x = n$, se $x \in n$, per la transitività di n, $x \subseteq n \subseteq n^+$, se $x = n \subseteq n^+$, cioè n^+ è transitivo. Dunque $n^+ \in X$, X è induttivo e $X = \omega$. □

Teorema 5.9. *La terna $\langle \omega, \sigma, 0\rangle$ è una terna di Peano.*

Dimostrazione. Sappiamo che $0 \in \omega$, che 0 non successore di nessun numero naturale (già lo sappiamo), ogni successore è unico (lo dimostriamo) e vale il principio di induzione (già lo sappiamo).

Dimostriamo che σ è iniettiva. Siano $n, m \in \omega$ tali che $n^+ = \sigma(n) = \sigma(m) = m^+$, allora $n = \bigcup n^+ = \bigcup m^+ = m$. □

Teorema 5.10 (Transitività dell'insieme dei numeri naturali)**.** *L'insieme dei numeri naturali è transitivo.*

Osservazione 5.7. Nota che dire che i numeri naturali sono transitivi e che l'insieme dei numeri naturali è transitivo sono due cose bene diverse (infatti abbiamo due teoremi diversi).

Dimostrazione. Dimostra che $X = \{n \in \omega : n \subseteq \omega\}$ è induttivo. □

Definizione 5.9 (Isomorfismo fra terne di Peano)**.** Siano $\langle M_1, f_1, e_1\rangle, \langle M_2, f_2, e_2\rangle$ terne di Peano, sia un'applicazione $\varphi : M_1 \to M_2$ tale che

1. φ è un'applicazione biunivoca
2. $\varphi(f_1(x)) = f_2(\varphi(x))$
3. $\varphi(e_1) = e_2$

allora φ si dice *isomorfismo fra* $\langle M_1, f_1, e_1\rangle$ *e* $\langle M_2, f_2, e_2\rangle$ e le terne di Peano $\langle M_1, f_1, e_1\rangle, \langle M_2, f_2, e_2\rangle$ si dicono *isomorfe*.

Proprietà 5.11. *Se esiste un insieme che coincide col suo singleton è transitivo.*

Osservazione 5.8. Si scrive "se esiste" perché non ci sono esempi di un siffatto insieme (se non sbaglio l'assioma di fondazione asserisce che non esistono e ovviamente ci sono teorie con assiomi che implicano l'opposto: vedi qui).

Definizione 5.10 (Relazione di appartenenza fra elementi di un insieme)**.** Sia a un insieme, definiamo la relazione binaria fra gli elementi di a

$$R_\in(a) \coloneqq \{\langle x, y\rangle \in a \times a : x \in y\}$$

Capitolo 6

Numeri ordinali

In questa sezione, generalizziamo i numeri naturali attraverso la definizione di numeri naturali ed determiniamo un estensione del principio di induzione e del teorema di ricorrenza.

Definizione 6.1 (Numero ordinale)**.** Sia α un insieme, si dice *numero ordinale o ordinale* se α è un insieme transitivo e $R_\in(\alpha)$ è una relazione di buon ordine stretto su α.

Esempio 6.1 (Esempi di numeri ordinali)*.* I seguenti sono numeri ordinali:

- $\varnothing, \{\varnothing\}$

Banalmente dalla definizione si ha che un numero ordinale è sempre un insieme transitivo ma in generale non è vero il viceversa.

Esempio 6.2 (Esempio di insieme transitivo che non è un ordinale)*.* Un esempio di insieme che è transitivo ma non è un numero ordinale è $\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$,perché la relazione di appartenenza non è transitiva.

Proposizione 6.1. *Sia α un ordinale e $\alpha \neq \varnothing$, allora il minimo di $\alpha\backslash\{\varnothing\}$ rispetto alla relazione $R_\in(\alpha)$ è $\varnothing$.*

Osservazione 6.1. Poiché $R_\in(\alpha)$ è una relazione di buon ordine (stretto), l'insieme α ammette minimo rispetto a tale relazione e lo puoi scrivere come l'unico elemento $m \in \alpha$ tale che

$$\forall x(x \in \alpha \implies x = m \vee m \in x)$$

Dimostrazione. Sia m il minimo di α rispetto alla relazione $R_\in(\alpha)$ e supponiamo per assurdo che $m \neq \varnothing$, allora esiste $x \in m \in \alpha$ e poiché α è un ordinale e quindi è un insieme transitivo, $x \in \alpha$ ma ciò è assurdo perché m è il minimo di α. Quindi $m = \varnothing$. □

Proprietà 6.2. *Sia α un ordinale e $\alpha \neq \varnothing$ e $\alpha \neq \{\varnothing\}$, allora il minimo rispetto alla relazione $R_\in(\alpha)$ è $\{\varnothing\}$.*

Osservazione 6.2. Poiché $R_\in(\alpha)$ è una relazione di buon ordine (stretto) su α e $\alpha\backslash\{\varnothing\}$ è un suo sottoinsieme non vuoto (si capisce), ha senso considerarne il minimo.

Dimostrazione. Sia m il minimo di $\alpha\backslash\{\varnothing\} \neq \varnothing$, se fosse $m = \varnothing$ allora $\varnothing \in \alpha\backslash\{\varnothing\}$ e ciò è assurdo, allora $m \neq \varnothing$. Sia $x \in m \in \alpha\backslash\{\varnothing\} \subseteq \alpha$, per la transitività di α, si ha $x \in \alpha$, allora non può succedere che $x \in \alpha\backslash\{\varnothing\}$ perché m è il minimo di $\alpha\backslash\{\varnothing\}$, quindi $x \in \{\varnothing\} \implies x = \varnothing$, cioè $m = \{\varnothing\}$. □

Teorema 6.3 (Segmenti iniziali di un ordinale)**.** *Sia α un numero ordinale, allora i segmenti iniziali di α sono α e i suoi elementi. In particolare $\alpha = S_\alpha$ e la relazione d'appartenenza su α coincide con quella di inclusione su S_α.*

Dimostrazione. α è un ordinale e quindi è un insieme bene ordinato, per la (Teorema 1.17) si ha che i segmenti iniziali di α sono tutti e soli i segmenti iniziali propri determinati dagli elementi di α e α stesso; studiamo i segmenti iniziali propri determinati da elementi di α. Sia $x \in \alpha$, allora, per la transitività di α, $x \subseteq \alpha$ e, ricordando che la relazione d'ordine su α è $\in$, $S_x(\alpha) = \{y \in \alpha : y \in x\} = x \cap \alpha = x$, quindi abbiamo caratterizzato i segmenti iniziali propri di α. Consideriamo $S_\alpha = \{S_x(\alpha) \in \mathcal{P}(\alpha) : x \in \alpha\} = \{x \in \mathcal{P}(\alpha) : x \in \alpha\} = \alpha$. Infine siano $x, y \in \alpha$ tali che $x \in y$, sia $z \in S_x(\alpha) = x \in y = S_y(\alpha)$, cioè $S_x(\alpha) \subseteq S_y(\alpha)$, inoltre $S_x(\alpha) \neq S_y(\alpha)$ perché $x \in S_y(\alpha)$ e $x \notin S_x(\alpha)$, per cui $S_x(\alpha) \subset S_y(\alpha)$. Viceversa se $S_x(\alpha) \subset S_y(\alpha)$ si dimostra (in generale e facilmente per assurdo) che $x \in y$. A questo punto sappiamo che $\langle x, y\rangle \in R_\in(\alpha) \iff \langle S_x(\alpha), S_y(\alpha)\rangle \in R_\subset(S_\alpha)$, ma sappiamo che $S_\alpha = \alpha$ e $\langle x, y\rangle = \langle S_x(\alpha), S_y(\alpha)\rangle$, allora $\langle x, y\rangle \in R_\in(\alpha) \iff \langle x, y\rangle \in R_\subset(\alpha)$, cioè $R_\in(\alpha) = R_\subset(\alpha)$ e $\langle \alpha, \in\rangle = \langle S_\alpha, \subset\rangle$. □

Teorema 6.4 (Condizione sufficiente affinché un insieme ben ordinato sia un ordinale)**.** *Sia $\langle A, <\rangle$ un insieme bene ordinato, se $\langle A, <\rangle = \langle S_A, \subset\rangle$ allora $<$ coincide con $R_\in(A)$ e A è un ordinale.*

Dimostrazione. Dire che $\langle A, <\rangle = \langle S_A, \subset\rangle$ significa che $A = S_A$ e $<=\subset$ ed è una relazione di buon ordine stretto. Si dimostra (la prof non lo fa o forse è un'ipotesi omessa?) che $x = S_x(A)$ per ogni $x \in A$, allora $x \in A \implies x = S_x(A) \subseteq A$ e quindi A è transitivo. Siano $x, y \in A$, allora $x < y \iff x \in S_y(\alpha) = y$, cioè $<= R_\in(\alpha)$, quindi α è un ordinale. □

I due precedenti teoremi possono essere riassunti nel seguente (che la prof non usa ma secondo me è comodo).

Teorema 6.5 (Caratterizzazione numeri ordinali)**.** *Sia $\langle A, <\rangle$ un insieme bene ordinato, allora $<= R_\in(\alpha)$ e A è un ordinale se e solo se $\langle A, <\rangle = \langle S_A, \subset\rangle$.*

Proposizione 6.6 (Gli elementi di ordinali sono ordinali)**.** *Ogni elemento di un ordinale è anch'esso un ordinale.*

Dimostrazione. Siano α un ordinale e $x \in \alpha$ e siano y, z tali che $z \in y \in x$, per la transitività di α e $y \in x \in \alpha$, si ha $y \in \alpha$, quindi $z \in y \in \alpha$ e $z \in \alpha$. Poiché $x, y, z \in \alpha$ e $z \in y \in x$, per la transitività della relazione d'ordine $R_\in(\alpha)$, si ha $z \in x$, quindi x è transitivo.

Poiché $R_\in(\alpha)$ è una relazione di buon ordine stretto, allora vale anche su x, cioè $R_\in(x) = R_\subset(x)$ è di buon ordine stretto, quindi x è un ordinale. □

Dimostrazione alternativa. Siano α un ordinale e $x \in \alpha$ e siano y, z tali che $z \in y \in x$, per la transitività di α e $y \in x \in \alpha$, si ha $y \in \alpha$, quindi $z \in y \in \alpha$ e $z \in \alpha$. Poiché $x, y, z \in \alpha$ e $z \in y \in x$, per (Teorema 6.3), si ha $z \in y \subset x$, quindi x è transitivo.

Poiché $R_\in(\alpha)$ è una relazione di buon ordine stretto, allora vale anche su x, cioè $R_\in(x) = R_\subset(x)$ è di buon ordine stretto, quindi x è un ordinale. □

Dimostrazione alternativa. Siano α un ordinale e $x \in \alpha$, dobbiamo dimostrare che x è un ordinale, quindi consideriamo la relazione $R_\in(x) = R_\in(\alpha)|_x$ (per me è sbagliato, vedi sopra, dovrebbe essere $R_\in(x) = R_\in(\alpha) \cap x \times x$) e vogliamo usare (Teorema 6.4) su $\langle x, \in\rangle$. Poiché α è un ordinale per (Teorema 6.3), si ha $y \in x \iff y \subset x$. Sia $y \in x$, allora

$$S_y(x) = \{z \in x : z \in y\} = x \cap y = y$$

e quindi

$$S_x = \{S_y(x) \in \mathcal{P}(x) : y \in x\} = \{y \in \mathcal{P}(x) : y \in x\} = x\,.$$

Poiché $R_\in(\alpha) = R_\subset(\alpha)$, allora vale anche su x, cioè $R_\in(x) = R_\subset(x)$. Abbiamo dimostrato che $\langle x, \in\rangle = \langle S_x, \subset\rangle$, quindi x è un numero ordinale. □

Proposizione 6.7. *Ogni ordinale non appartiene a sé stesso.*

Dimostrazione. Sia α un ordinale, per ogni $x \in \alpha$ si ha $x \notin x$ poiché $R_\in(\alpha)$ è una relazione di ordine stretto. Sia per assurdo $\alpha \in \alpha$, allora per quanto detto, $\alpha \notin \alpha$ e ciò è assurdo. □

Proprietà 6.8 (Inclusione fra due ordinali)**.** *Siano α, β ordinali, allora*

$$\alpha \in \beta \iff \alpha \subset \beta$$

Dimostrazione. $\implies$) Poiché β è transitivo e $\alpha \in \beta \implies \alpha \subseteq \beta$, ma se fosse $\alpha = \beta$ si avrebbe $\alpha \in \alpha$ ed è assurdo per (Proposizione 6.7).

$\impliedby$) Se dimostriamo che α è un segmento iniziale proprio di β, per (Teorema 6.3) $\alpha \in \beta$. Siano $x \in \alpha$ e $y \in \beta$ tali che $y < x \iff y \in x \in \alpha$, allora $y \in \alpha$ e α è segmento iniziale di β ed è proprio perché $\alpha \subset \beta$. □

Teorema 6.9 (Teorema di tricotomia)**.** *Siano α, β ordinali, allora si verifica una ed una sola delle seguenti*

1. $\alpha = \beta$
2. $\alpha \in \beta$
3. $\beta \in \alpha$

Dimostrazione "parzialmente alternativa". Se $\alpha = \beta$, non può succedere che $\alpha \in \beta = \alpha$ o $\beta \in \alpha = \beta$ per (Proposizione 6.7).

Sia $\alpha \neq \beta$ e sia $\xi = \alpha \cap \beta$, se ξ è un segmento iniziale proprio di α o di β, allora, per (Teorema 6.3), appartiene ad uno dei due ordinali e, per (Proposizione 6.6), è un ordinale. Siano $x \in \xi \subseteq \alpha, \beta$ e $y \in \alpha$ tali che $y < x \iff y \in x \in \beta \implies y \in \beta$, cioè $y \in \alpha \cap \beta = \xi$, quindi ξ è segmento iniziale di α e si ripete lo stesso ragionamento per β. Poiché $\alpha \neq \beta$, non può essere che $\xi = \alpha \wedge \xi = \beta$, quindi ξ dev'essere segmento proprio di α o di β, per quanto detto sopra, ξ è un ordinale.

Supponiamo che ξ è segmento iniziale proprio di α, allora $\xi \subset \alpha$ e, per (Proprietà 6.8), $\xi \in \alpha$, se fosse ξ segmento iniziale proprio anche di β, si avrebbe $\xi \subset \beta \iff \xi \in \beta \implies \xi \in \alpha \cap \beta = \xi$ e questo è assurdo per (Proposizione 6.7). Allora si ha $\beta = \xi \in \alpha$.

Supponiamo che ξ è segmento iniziale proprio di β, allo stesso modo ξ non può essere segmento iniziale proprio di α e quindi $\alpha = \xi \in \beta$. □

Corollario 6.9.1. *Siano α, β ordinali, allora*

$$\alpha \in \beta \iff \alpha \subset \beta$$

Dimostrazione. Avevo già dimostrato questa cosa ma ho scoperto che la prof fa in modo diverso... (non la usa nel teorema precedente e anzi ne è un corollario)

$\implies$) Uguale a sopra.

$\impliedby$) Per (Teorema 6.9), si ha $\alpha = \beta$ o $\alpha \in \beta$ o $\beta \in \alpha$. Poiché $\alpha \subset \beta$ sicuramente non può essere $\alpha = \beta$, se fosse $\beta \in \alpha$, per la transitività di $\alpha, \beta \subseteq \alpha \implies \alpha \subset \beta \subseteq \alpha$ e ciò è assurdo. □

Definizione 6.2 (Formula degli ordinali)**.** La formula che esprime la proprietà di essere ordinale è O_n, cioè questa formula esprime la proprietà di essere un insieme transitivo e che la relazione di appartenenza è di buon ordine stretto. Quindi dato un insieme α esso è un ordinale se e solo se $O_n(\alpha)$.

Notazione 6.3 (Classe degli ordinali)**.** Si usa dire che gli insiemi α tali che $O_n(\alpha)$, cioè che sono oridnali, costituiscano la *classe degli ordinali* O_n, inoltre data una proprietà A, tale che $A(\alpha) \implies O_n(\alpha)$, si dice che *$A$ è sottoclasse di O_n*. Questo modo di esprimersi trova fondamento in altre teorie in cui è presente il concetto di "classe", in ZF non è presente, ma possiamo pensarla come ad una notaazione. Questa notazione si estende ulteriormente, infatti dati α e una sotttoclasse A di O_n tali che $A(\alpha)$, si scrive $\alpha \in A$, si può parle di sottoclassi vuote e non vuote e di sottoclassi proprie, di minimo di una classa, ecc, in generale le notazioni insiemistiche vengono estese alle classi, questo è chiaramente un abuso di notazione, però è "comodo".

Teorema 6.10. *Dati α, β, γ ordinali, valgono*

1. $\alpha \notin \alpha$
2. *Se $\alpha \in \beta$ e $\beta \in \gamma$, allora $\alpha \in \gamma$*
3. *Sia $A(x)$ una formula di ZF, allora*

$$(\forall x(A(x) \to O_n(x)) \wedge \exists x A(x)) \to \exists z(A(z) \wedge \forall y(A(y) \to (y = z \vee z \in y)))$$

"Ogni sottoclasse non vuota di O_n ha minimo (rispetto all'appartenenza), cioè O_n è ben ordinato"

Stiamo dicendo che se abbiamo una formula A, che implica "essere ordinale", ed esiste un elemento che la soddisfa x, allora esiste il "minimo" z.

Dimostrazione. (1) e (2) le abbiamo già dimostrate.

3) Sia A una sottoclasse di O_n non vuota, allora esiste $\delta \in A$. Se δ è il minimo di A, abbiamo concluso, se δ non è il minimo di A, allora esiste $\xi \in \delta$ tale che $A(\xi)$. Denotiamo $A_\delta = \{x \in \delta : A(x)\}$, allora $\xi \in A_\delta$. Poiché δ è un ordinale, A_δ possiede minimo (perché?), che denotiamo con μ. Supponiamo per assurdo che μ non sia il minimo di A, allora esiste $\gamma \in \mu$ e tale che $A(\gamma)$, allora $\gamma \in \mu \in \delta \implies \gamma \in \delta$ e quindi $\gamma \in A_\delta$, ma ciò è assurdo perché μ è il minimo. □

Teorema 6.11. *La classe O_n è ben ordinata rispetto alla relazione di appartenenza. buon ordine stretto*

Dimostrazione. Lo abbiamo dimostrato prima, tale e quale, solo che la prof l'ha scritto separatamente... □

Corollario 6.11.1. *Ogni sottoclasse di O_n è ben ordinata dalla relazione di appartenenza.*

Dimostrazione. Sia T una qualunque sottoclasse di O_n, cioè

$$\forall x(T(x) \to O_n(x))$$

E' sufficiente sostituire $T(x)$ a $O_n(x)$ nella formula precedente (quella lunga e che diceva che O_n è ben ordinato). □

Notazione 6.4 (Relazione d'ordine fra ordinali)**.** Dai risultati precedenti (in particaolare dal teorema di tricotomia, dal f<atto che un ordinale non appartiene a e stesse e che un ordinale appartiene ad un altro se e solo se è incluso) è lecito usare $\alpha < \beta$ per $\alpha \in \beta$ o $\alpha \subset \beta$.

Lemma 6.12. *La classe O_n è transitiva.*
Cioè se $\alpha \in O_n$ allora $\alpha \subseteq O_n$, ovvero ogni elemento di un ordinale è un ordinale.

Osservazione 6.3. Come già detto, i simboli di appartenenza e di inclusione sono impropri, formalmente dovresti dire

$$O_n(\alpha) \to \forall x(x \in \alpha \to O_n(x))$$

Dimostrazione. Lo abbiamo già dimostrato in (Proposizione 6.6). □

Teorema 6.13. *La classe O_n non è un insieme.*

Dimostrazione. Se per assurdo esistesse l'insieme degli ordinali O_n, avendo provato che è transitivo e ben ordinato (rispetto a $R_\in$), avremo che O_n è un ordinale, allora $O_n \in O_n$ e ciò è assurdo (sicuramente per (Proposizione 6.7). □

Proposizione 6.14 (Segmenti iniziali di O_n)**.** *I segmenti iniziali propri di O_n, coincidono con gli elementi di O_n, quindi sono insiemi.*

Osservazione 6.4. Nota che la stessa proprietà vale per gli ordinali, vedi (Teorema 6.3), anche se O_n non è un ordinale.

Dimostrazione. Sia T un segmento iniziale proprio di O_n che formalmente sarebbe

$$\forall x(T(x) \to O_n(x)) \wedge \exists x(O_n(x) \wedge \neg T(x)) \wedge \forall x \forall y((T(x) \wedge O_n(y) \wedge y < x) \to T(y)).$$

Poiché T è una sottoclasse propria, si ha $O_n \backslash T \neq \varnothing$ e poiché O_n è ben ordinato, tale insieme ammette minimo, chiamiamolo μ. Vogliamo far vedere che $\mu = T$. Sia $x \in \mu$, cioè $x < \mu$ e x è un ordinale, poiché μ è il minimo di $O_n \backslash T$, $x \notin O_n \backslash T \implies x \in T$. Sia $T(x) \implies O_n(x)$, quindi x e μ sono entrambi ordinali, per il teorema di tricotomia, si ha $x = \mu$ o $x < \mu$ o $\mu < x$. Sia per assurdo che $\mu \leqslant x \in T$, poiché T è un segmento iniziale di O_n, si ha $\mu \in T$ e cioè assurdo perché $\mu \in O_n \backslash T$. Allora $x < \mu \iff x \in \mu$; abbiamo dimostrato che $\mu = T$ □

Corollario 6.14.1. *Ogni classe transitiva di ordinali o è un numero ordinale oppure coincide con O_n.*

Dimostrazione. Sia T una classe transitiva di ordinali, per la proposizione precedente è sufficiente far vedere che T è un segmento iniziale di O_n. Siano x e y ordinali tali che $T(x)$ e $y < x \iff y \in x \in T \implies y \in T$ per la transitività di T. Allora T è segmento iniziale e quindi $T = O_n$ oppure T è segmento iniziale proprio di O_n e quindi è un ordinale. □

Teorema 6.15. *Per ogni ordinale α, l'insieme $\alpha^+ = \alpha \cup \{\alpha\}$ è un ordinale ed è il più piccolo maggiore di α.*

Dimostrazione. Dimostriamo che α^+ è transitivo. Sia $x \in y \in \alpha^+$, allora $x \in y \in \alpha \implies x \in \alpha \subset \alpha^+$ o $y \in \{\alpha\}$, allora $x \in y = \alpha \subset \alpha^+$ e abbiamo concluso in entrambi i casi.

Si ha che $R_\in(\alpha^+) = R_\in(\alpha) \cup (\alpha \times \{\alpha\})$ (nota che la coppia $\langle \alpha, \alpha \rangle$ non ci sta) e che è una relazione di buon ordine stretto. Quindi α^+ è un ordinale.

Ovviamente $\alpha < \alpha^+$. Sia β un ordinale tale che $\alpha < \beta$, allora $\alpha \in \beta \iff \{\alpha\} \subseteq \beta$ e $\alpha \subset \beta$, quindi $\alpha^+ = \alpha \cup \{\alpha\} \subseteq \beta \iff \alpha^+ \leqslant \beta$, cioè α^+ è il più piccolo ordinale maggiore di α. □

Definizione 6.5 (Ordinale successore)**.** Un ordinale che è successore di un altro ordinale è detto *ordinale successore*.

Abbiamo un esempio banale di ordinale che non è successore di nessun ordinale ed 0, ora vedremo che esistono esempi non banali.

Definizione 6.6 (Ordinale limite)**.** Un ordinale diverso da 0 che non è successore di alcun ordinale è detto *ordinale limite*.

Esempio 6.3. Un ordinale limite è l'insieme dei numeri naturali ω, esso è anche un ordinale infinito ed è anche il più piccolo ordinale limite (sarebbe da dimostrare).

Vogliamo trovare tutte e sole le sottoclassi di O_n che sono insiemi.

Teorema 6.16 (Caratterizzazione sottoclassi di O_n che sono insiemi)**.** *Sia T una sottoclasse di O_n, allora T è limitato superiormente se e solo se T è un insieme e in tal caso $\cup T = \sup T$.*

Dimostrazione. Non dimostrato. □

Osservazione 6.5. Osserva che ω è il più piccolo ordinale limite.

Assioma 6.1 (Assioma dell'infinito - forme equivalenti)**.** 1. *Esiste un insieme induttivo*

2. *Esiste un ordinale limite*
3. *Esiste un ordinale non finito (cioè infinito?? Sì)*
4. *Gli ordinali finiti sono in insieme*
5. *Gli ordinali finiti sono superiormente limitati*

Dovresti dimostrare che le forme sono equivalenti (la prof non lo fa).
Nota che $\{\omega, \omega^+\}, \{\omega, \omega^+, \omega^{+^+}\}, \dots$ sono insiemi, ma dobbiamo chiederci

$$\{\omega, \omega^+, \omega^{+^+}, \dots\}$$

è un insieme?? (O una classe?)

Definizione 6.7 (Ordinale finito)**.** Un ordinale α è detto *finito* se α risulta essere uguale a 0 o risulta essere un successore di un ordinale e tutti i suoi elementi sono uguali a 0 o sono successori di un ordinale.

Teorema 6.17. *Siano α e β ordinali, se esiste una similitudine tra α e β, essa è l'identità.*

Dimostrazione. Sia $\varphi : \alpha \to \beta$ una similitudine, e consideriamo $\gamma = \{x \in \alpha : x \neq \varphi(x)\} \subseteq \alpha$. Sia per assurdo $\gamma \neq \varnothing$, allora, essendo α bene ordinato, γ possiede minimo, chiamiamolo μ. Poiché $\mu \in \gamma$, $\mu \neq \varphi(\mu)$, ma $\mu \in \alpha$ e $\varphi(\mu) \in \beta$, quindi sono ordinali e vale il teorema di tricotomia, allora $\mu < \varphi(\mu)$ o $\varphi(\mu) < \mu$. Sia $\varphi(\mu) < \mu$, allora $\varphi(\mu) \in \mu \in \alpha \implies \varphi(\mu) \in \alpha$ e poiché μ è il minimo di γ, $\varphi(\mu) \notin \gamma \implies \varphi(\mu) = \varphi(\varphi(\mu))$, ma φ è iniettiva, quindi $\mu = \varphi(\mu)$ e ciò è assurdo. Supponiamo $\mu < \varphi(\mu)$, allora $\mu \in \varphi(\mu) \in \beta \implies \mu \in \beta$. per la suriettività di φ, esiste $\nu \in \alpha$ tale che $\mu = \varphi(\nu)$ e dev'essere $\nu \neq \mu$. Per il teorema di tricotomia, si ha $\mu < \nu$ o $\nu < \mu$, se $\mu < \nu$ allora, poiché φ è una similitudine, $\varphi(\mu) < \varphi(\nu) = \mu$ e ciò è assurdo perché $\mu < \varphi(\mu)$. Se $\nu < \mu$, $\varphi(\nu) = \mu \neq \nu \implies \gamma$, allora ν è un elemento di γ minore di μ e ciò è assurdo perché μ è il minimo di γ. In ogni caso abbiamo trovato un assurdo, quindi $\gamma = \varnothing$ e φ coincide con l'identità. □

Assioma 6.2 (Schema di assiomi di rimpiazzamento (o assioma di rimpiazzamento))**.** *Sia F una relazione su un insieme a, allora*

$$\forall x \forall y \forall y' (xFy \wedge xFy' \to y = y') \to \forall x \exists y (\forall z (z \in y \longleftrightarrow \exists t (t \in x \wedge tFz)))$$

Si dice schema di assiomi in quanto vale per infinite relazioni F. Lo schema di assiomi dice "Per ogni applicazione su un insieme, l'immagine è un insieme" (mi verrebbe da dire, ma noi non lo sappiamo già? Non basta considerare ran F*?). Inoltre si dimostra che dall'assioma di rimpiazzamento si possono ottenere gli assiomi di separazione e della coppia non ordinata.*

Osservazione 6.6. Sia $F(x, y)$ è una qualunque formula di ZF, con due variabili libere, allora

1. E' uno schema di assiomi (ma in che senso?)
2. Non solo è un insieme b la collezione delle immagini degli elementi di a tramite F ma è anche un insieme quello formato dalle coppie ordinate $\langle x, y \rangle$ con $x \in a$ e $y \in b$.

Esempio 6.4. Sia a un insieme su cui è definita l'applicazione F e sia b la sua immagine mediante F.

1. Sia $F(x, y) = (x \neq x \wedge y \neq y)$
   Qualunque sia a otteniamo $b = \varnothing$

2. Sia $F(x,y) = (y = x \wedge P(x))$ con $P(x)$ qualunque formula con una variabile libera. La formula $F(x,y)$ soddisfa l'antecedente (credo sia l'ipotesi) di ** (CREDO che sia l'assioma di rimpiazzamento). Dall'assioma di rimpiazzamento è un insieme b costituito da tutti gli y uguali a un $x \in a$ e che soddisfa la proprietà P, esiste il sottoinsieme a.

   Dunque ho ottenuto l'assioma di separazione da quello di rimpiazzamento.

3. Vediamo che a partire da x, y esiste $\{x,y\}$

   A partire dal $\varnothing$ dall'assioma dell'insieme delle parti $\mathcal{P}(\varnothing) = \{\varnothing\}, \mathcal{P}(\mathcal{P}(\varnothing)) = \{\varnothing, \{\varnothing\}\}$

   Dati a e b formule di due variabili libere, prendo come funzione biunivoca tra

   $\mathcal{P}(\mathcal{P}(\varnothing))$ e $\{a,b\}$

$$F(x,y) \quad (x = \varnothing \wedge y = a) \vee (x = \{\varnothing\} \wedge y = a) \vee (x = \{\varnothing\} \wedge y = b)$$

Teorema 6.18. *Sia A un insieme ben ordinato, allora esiste uno ed uno solo ordinale α simile ad A e la similitudine è unica.*

Teorema 6.19 (Teorema di ricorrenza - Prima forma)**.** *Sia A un insieme e sia $a \in A$, sia $G : A \to A$. Allora esiste ed è unica una funzione $f : \omega \to A$ tale che $f(0) = a$ e per ogni $n \in \omega$, $f(n^+) = G(f(n))$*

Osservazione 6.7. Pratiamente noi abbiamo un insieme A, fissiamo $a \in A$, "elememto di partenza della successione", quindi possiamo definire un'unica successione per ricorrenza f, mediante G. Infatti ho $f(0) = a, f(1) = G(a), f(2) = G(f(1)), \ldots, f(n^+) = G(f(n))$.

Notazione 6.8. ${}^nA \coloneqq \{f : n \to A\}$

Teorema 6.20 (Teorema di ricorrenza - Seconda forma)**.** *Dati un insieme A e $G : A^* \to A$, dove $A^* = \bigcup_{n\in\omega} {}^nA$ esiste ed è unica la funzione $f : \omega \to A$ tale che*

$$f(n^+) = G(f|_n), \quad \forall n \in \omega$$

dove

$${}^nA = \{f | f : \omega \to A\}$$

Osservazione 6.8. Ricordiamo che $n = \{0, 1, \ldots, n-1\}$, quindi $f|_n$ rappresenta i valori di f ristretti ai naturali strettamente minori di n.

Teorema 6.21 (Tutte le terne di Peano sono isomorfe)**.** *Date due qualsiasi terne di Peano, esse sono isomorfe.*

Teorema 6.22 (Principio generale di induzione)**.** *Sia P una proprietà (cioè una formula), per ogni ordinale α, se la proprietà vale per ogni ordinale più piccolo di α allora P vale per α. Quindi vale per ogni ordinale α.*

$$\{\forall\alpha(\forall\beta(\beta < \alpha \to P(\beta)) \to P(\alpha))\} \to \forall\alpha P(\alpha)$$

Dimostrazione. Supponiamo per assurdo chew la collezione degli ordinali per cui la proprità non vale è non vuota, allora tale collezione ammette minimo perché O_n è ben ordinato, sia μ. Ma vale l'antecente (perché?), allora vale $P(\mu)$, ma per μ questa proprietà non dovrebbe vale perché è il minimo senza questa prprietà. □

Teorema 6.23 (Principio di induzione per α)**.** *Siano α un ordinale e P una proprietà, supponiamo che per ogni ordinale $\beta < \alpha$ vale che se P vale per tutti gli ordinali più piccoli di β vale anche per β, allora P vale per ogni ordianle più piccolo di α.*

$$\forall\beta(\beta < \alpha \to (\forall\gamma(\gamma < \beta \to P(\gamma)) \to P(\beta))) \to \forall\beta(\beta < \alpha \to P(\beta))$$

Notazione 6.9 (Insieme delle applicazioni da un ordinale ad un insieme)**.** Sia β un ordinale e sia A un insieme, l'insieme delle applicazioni da β in A (La prof giustifica perché è un insieme) si denota col simbolo ${}^\beta A$

Notazione 6.10. Viene utilizzata la notazione Siano α un ordinale e A un insieme, si denota

$$A^{(\alpha)} \coloneqq \bigcup \{{}^\beta A : \beta \in \alpha\}$$

Teorema 6.24 (Teorema di ricorrenza per α)**.** *Siano α un ordinale e A un insieme, sia $G : A^{(\alpha)} \to A$ allora esiste ed è unica $f : \alpha \to A$ tale che*

$$\forall \beta(\beta < \alpha \to f(\beta) = G(f|_\beta))$$

Definizione 6.11 (Somma di ordinali)**.** Siano α e β ordinali, si definisce $\alpha+\beta$ *somma di α e β* per ricorrenza.

1. Se $\beta = 0$, allora $\alpha + 0 = \alpha$
2. Se $\alpha + \beta$ è già definito, allora $\alpha + \beta^+ = (\alpha + \beta)^+$
3. Se β è un ordinale limite, allora $\alpha + \beta = \sup\{\alpha + \gamma : \gamma < \beta\}$

Osservazione 6.9. Nota che è importante distinguere i tre casi perché i primi due servono per definire la somma fra ordinali che sono 0 o successori di un altro ordinale, il caso rimanente corrisponde agli ordinali limite.

Proprietà 6.25 (La somma di ordinali non è commutativa)**.** *La somma di ordinali non è commutativa, infatti si ha*

$$\omega + 1 = \omega^+ \neq \omega = 1 + \omega$$

Definizione 6.12 (Prodotto di ordinali)**.** Siano α e β ordinali, si definisce $\alpha \cdot \beta$ *prodotto di α e β* per ricorrenza.

1. Se $\beta = 0$, allora $\alpha \cdot 0 = 0$
2. Se $\alpha \cdot \beta$ è già definito, allora $\alpha \cdot \beta^+ = \alpha \cdot \beta + \alpha$
3. Se β è un ordinale limite, allora $\alpha \cdot \beta = \sup\{\alpha \cdot \gamma : \gamma < \beta\}$

Osservazione 6.10. Nota che è importante distinguere i tre casi perché i primi due servono per definire il prodotto fra ordinali che sono 0 o successori di un altro ordinale, il caso rimanente corrisponde agli ordinali limite.

Definizione 6.13 (Potenza di ordinali)**.** Siano α e β ordinali, si definisce α^β *potenza di α alla β* per ricorrenza.

1. Se $\beta = 0$, allora $\alpha^0 = 1$
2. Se α^β è già definito, allora $\alpha^{\beta^+} = \alpha^\beta \cdot \alpha$
3. Se β è un ordinale limite, allora $\alpha^\beta = \sup\{\alpha^\gamma : \gamma < \beta\}$

Osservazione 6.11. Nota che è importante distinguere i tre casi perché i primi due servono per definire il prodotto fra ordinali che sono 0 o successori di un altro ordinale, il caso rimanente corrisponde agli ordinali limite.

Definizione 6.14 (Insiemi equipotenti)**.** Siano a e b insiemi, allora si dicono *equipotenti* se esiste una ocrrispondenza biunivoca fra a e b.

Notazione 6.15 (Insiemi equipotenti)**.** Due insiemi a e b che sono equipotenti si denotano $a \cong b$.

Proprietà 6.26. *La relazione di equipotenza $\cong$ è una relazione di equivalenza.*

Esempio 6.5 (Esempi notevoli di insiemi equipotenti). $\omega \cong \mathbb{Z}\ \omega \cong \mathbb{Q}\ \omega \ncong \mathbb{R}\ \mathbb{R} \cong (0,1)$

Teorema 6.27 (Teorema di Cantor)**.** *ω no è equipotente a $(0,1)$.*

Teorema 6.28. *Per ogni insieme A si ha $A \ncong \mathcal{P}(A)$*

Teorema 6.29. *Per ogni insieme A si ha $\mathcal{P}(A) \cong {}^A2$.*

Cantor, dopo aver dimostrato che ω e $\mathbb{R}$ non sono equipotenti, tentò ripetutamente di dimostrare che i sottoinsiemi infiniti di R sono equipotenti a ω oppure a $\mathbb{R}$ (che poi è equipotente a $\mathcal{P}(\omega)$, ma perché? Non mi ricordo), ma fall; tale idea è detta *ipotesi del continuo* e si espreime anche nel mdoo seguente.

Assioma 6.3 (Ipotesi del continuo)**.** *Non esistono infiniti fra ω e $\mathcal{P}(\omega)$.*

L'ipotesi del continuo può essere cosniderato un assioma poiché è indipendenta dalla teoria ZF e dall'assioma della scelta, cioè vuol dire che gli uni non dimostrano l'altro e viceversa, in sostanza deve essere operata la scelta, a seconda della teoria che si vuole costroire, se accettare o no l'ipotesi del continuo.

Definizione 6.16 (insieme finito)**.** Sia A un insieme se esiste un naturale $n \in \omega$ tale che $A \cong n$, allora A si dice un *insieme finito*, altrimenti si dice *insieme infinito*.

Teorema 6.30. *nessuna parte propria di un numero naturale n è equipotente a n stesso. Cioè*

$$\forall n \forall x (n \in \omega \wedge x \subseteq n \wedge x \cong n \rightarrow x = n)$$

Corollario 6.30.1. *Nessun insieme finito è equipotente ad un suo sottoinsieme proprio.*

Corollario 6.30.2. *Ogni insieme equipotente ad una sua parte propria è infinito. In particolare ω è infinito.*

Definizione 6.17 (Insieme che domina un insieme)**.** Siano A e B due insiemi, si dice che *A è dominato da B* e si scrive $A \leqslant B$ se esiste un'applicazione iniettiva da A in B. Scrivere inoltre $A < B$ se $A \leqslant B$ e $A \ncong B$.

Proprietà 6.31 (Proprietà insiemi dominati)**.**

1. $\forall A (A \leqslant A)$
2. $\forall A \forall B \forall C ((A \leqslant B \vee B \leqslant C) \rightarrow A \leqslant C)$
3. $\forall A \forall A' \forall B \forall B' \left((A \leqslant B \wedge A \cong A' \wedge B \cong B') \rightarrow A' \leqslant B'\right)$
4. $\forall A \forall B (A \cong B \rightarrow (A \leqslant B \wedge B \leqslant A))$
5. $\forall A \forall B (A \leqslant B \longleftrightarrow \exists B' : B' \subseteq B \wedge A \cong B')$

Osservazione 6.12. Nota che il teorema di Hartogs e il Teorema di Cantor-Bernstein ci daranno informazioni ulteriori

Teorema 6.32 (Teorema di Cantor-Bernstein)**.** *Siano A e B insiemi, se $A \leqslant B$ e $B \leqslant A$, allora $A \cong B$.*

Dimostrazione. Sappiamo che esistono $f : A \rightarrow B$ e $g : B \rightarrow A$ iniettive e supponiamo per assurdo che le funzioni siano non suriettive. Allora $A_0 = A \backslash g[B] \neq \varnothing$, siano $B_0 = f[A_0]$, $A_1 = g[B_0] = g[f[A_0]]$ e definiamo

$$B_n = f[A_n]$$

$$A_{n+1} = g[B_n] = g[f[A_n]]$$

Nel secondo caso usiamo il teorema di ricorrenza. La successione risultante $\varphi : \omega \rightarrow \mathcal{P}(A)$ è tale che

$$\varphi(0) = A_0$$

$$\varphi(n^+) = A_{n+1}$$

Definiamo $h : A \rightarrow B$ tale che

$$h(x) = \begin{cases} f(x) & \text{se } x \in \bigcup_{n \in \omega} A_n \\ g^{-1}(x) & \text{se } x \notin \bigcup_{n \in \omega} A_n \end{cases}$$

La funzione è ben definita in quanto $x \notin \bigcup_{n \in \omega} A_n \implies x \notin A_0 = A \backslash g[B] \implies x \in g[b]$ e quindi possiamo considerare l'inversa di g.

Dimostriamo che l'applicazione è sia iniettiva che suriettiva. □

Capitolo 7

Numeri cardinali

Definizione 7.1 (Numero cardinale di un insieme)**.** Sia X un insieme se è ben ordinato, si dice *numero cardinale di X* o *cardinalità di X*

1. Il più piccolo ordinale equipotente ad esso (in realtà simile), se X è un insieme bene ordinato
2. l'insieme $\mathcal{B}(A_x)$ dove A_x è la classe di tutti gli insiemi equipotenti a X, se X non è ben ordinato

Osservazione 7.1. La prima parte è garantita dal fatto che dato un insieme ben ordinato esiste un ordinale simile.. Per la seconda parte è necessario l'assioma di fondazione. Nota inoltre che se introducessimo nella teoria l'assioma della scelta allora non avrei bisogno di distinguere i due casi, perché tutti gli insiemi sarebbero bene ordinati (per il teorema di Zermelo).

Notazione 7.2 (Numero cardinale di un insieme)**.** Sia X un insieme, denotiamo il suo numero cardinale con i simboli $\text{card}(X)$ e $|X|$.

Assioma 7.1 (Assioma della scelta)**.** *Data una famiglia infinita di insiemi $(X_i)_{i\in I}$, allora esiste l'insieme i cui elementi sono scelti da ciascun insieme.*

Lemma 7.1 (Lemma di Hartogs)**.** *Dato un qualunque insieme a esiste un ordinale α che non è dominato da a.*

Teorema 7.2 (Teorema di Zermelo)**.** *Dato un insieme A esiste una relazione di buon ordine su A*

Osservazione 7.2. Osserva che è equivalente all'assioma della scelta.

Teorema 7.3 (Teorema di Hartogs)**.** *Siano A e B insiemi, allora $A \leqslant B$ oppure $B \leqslant A$.*

Osservazione 7.3. E' equivalente al Teorema di Zermelo (la prof lo dimsotra).

Lemma 7.4 (Lemma di Zorn)**.** *Sia $(A, \subseteq)$ un insieme parzialmente ordinato e tale che ogni sua catena possiede maggiorante.*

Proprietà 7.5. *I cardinali di insiemi ben ordinati sono gli ordinali che non sono equipotenti a nessun ordinale minore (CREDO nel senso che dato un insieme X esiste sempre un ordinale a cui è equipotente, però gli ordinali sono sempre confrontabili, quindi posso considerare gli "ordinali minori"nel senso della relazione di inclusione/appartenenza definita in (Notazione 6.4) e io sto dicendo che i cardinali non sono equipotenti a nessuno di questi ordinali minori), per cui vengono detti anche* ordinali iniziali.

Osservazione 7.4. Osserva che se assumiamo l'assioma della scelta, tutti i cardinali sono ordinali ma non è vero il viceversa in generale.

Esempio 7.1 (Esempi di ordinali che sono cardinali). Gli ordinali finiti e ω sono cardinali. (Perché non sono equipotenti ad un sottoinsieme proprio, dice la prof).

Notazione 7.3 (Classe dei numeri cardinali)**.** Si denota col simbolo C_n la classe di tutti i numeri cardinali, possiamo osservare che $\omega \subseteq C_n$. Indichiamo inoltre con $C'_n := C_n \backslash \omega$ la classe dei dei cardinali infiniti, con $C_{n_0} := C_n \cap O_n$ la classe dei cardinali che sono ordinali e con $C'_{n_0} := C'_n \cap O_n$ la classe dei cardinali infiniti che sono ordinali.

Definizione 7.4 (Relazione d'ordine fra numeri cardinali)**.** Siano k e λ due numeri cardinali, si dice che $k \leqslant \lambda$ se esistono due insiemi K e L tali che $|K| = k$ e $|L| = \lambda$ e $K \leqslant L$.

Si dimostra facilmente che la relazione $\leqslant$ fra numeri cardinali è una relazione d'ordine.

Osservazione 7.5. Osserviamo che la definizione non dipende dalla scelta di K e L per la (Proprietà 6.31)

Proprietà 7.6. *Siano k e λ due cardinali bene ordinati, allora k e λ sono ordinali e*

$$k \leqslant_O \lambda \iff k \leqslant_C \lambda,$$

dove $\leqslant_O$ denota la relazione d'ordine fra ordinali e $\leqslant_C$ denota la relazione d'ordine fra numeri cardinali.

Osservazione 7.6. Nota che per k cardinale vale k bene ordinato se e solo se k ordinale.

Esempio 7.2 (Ordinali che non sono cardinali). Si ha che ω^+ è un ordinale maggiore di ω (perché ω vi è incluso propriamente) ma sono equipotenti, quindi ω^+ non può essere un cardinale. Anche $\omega + \omega$ è un ordinale che non è un cardinale.

Lemma 7.7. *Valgono le seguenti affermazioni:*

1. *Sia k un numero cardinale, allora esiste un cardinale maggiore di k*
2. *Sia k un numero cardinale bene ordinato, allora esiste un cardinale bene ordinato maggiore di k*

Dimostrazione. Si usa il lemma di Hartogs □

Lemma 7.8. *Sia A un insieme di cardinali bene ordinati. Allora $\bigcup A$ è un cardinale bene ordinato (ed è il sup).*

Teorema 7.9. *Le classi C_n e C_{n_0} non sono insiemi.*

Dimostrazione. Si dimostra solo per C_{n_0} (è una conseguenza che vale per C_n) e si usano i due lemmi precedenti. □

Corollario 7.9.1. *Le classi C'_n e C'_{n_0} non sono insiemi.*

Definizione 7.5 (Aleph)**.** Si ha che C_{n_0} è una classe propria bene ordinata, definiamo l'applicazione

$$\aleph : O_n \to C'_{n_0}$$

per ricorrenza. Poniamo $\aleph(0) = \omega$ e per ogni $\alpha \in O_n$ poniamo $\aleph(\alpha) = \min\{k \in C'_n \cap O_n : k > \aleph_\beta \forall \beta < \alpha\}$

Notazione 7.6 (Aleph)**.** Per aleph si usa anche la notazione $\aleph_\alpha = \aleph(\alpha)$

Proprietà 7.10. *α_0 è il più piccolo cardinale infinito bene ordinato, quindi $\aleph_1 = \omega$. $\aleph_1$ è il più piccolo cardinale infinito strettamente maggiore di ω, quindi è il più piccolo cardinale infinito non numerabile*

Proprietà 7.11. *Valgono le seguenti proprietà:*

1. *Se $\alpha < \beta$ allora $\aleph_\alpha < \aleph_\beta$*
2. $\aleph\alpha^+) = \min\{k \in C'_n \cap O_n : k > \aleph_\alpha\}$
3. *Sia A un isnieme di ordinale e sia $\sigma = \sup A = \bigcup A$, allora $\aleph_\sigma = \sup\{\aleph_\alpha : \alpha \in A\}$*
4. *Se λ è un ordinale limite, allora $\aleph_\lambda = \sup\{\aleph_\alpha : \alpha < \lambda\}$*

Definizione 7.7 (Cardinale successore)**.** Sia α un ordinale, allora $\aleph(\alpha^+)$ è detto cardinale sucessore (di α??).

Definizione 7.8 (Cardinale limite)**.** Sia α un ordinale limite, allora $\aleph(\alpha)$ è detto cardinale limite.

Proposizione 7.12. *Ogni cardinale infinito bene ordinato R è un ordinale limite*

Senza assioma della scelta non posso nemmeno dire che $|\mathcal{P}(\omega)|$ è un aleph. se lo assumo posso dire che invece è un certo aleph, se inoltre assumo l'ipotesi del continuo, posso anche dire che coincide con $\aleph_1$

Assioma 7.2 (Ipotesi del continuo generalizzata)**.** *Sia α un cardinale, allora $|\mathcal{P}(\aleph_\alpha)| = \aleph_{\alpha+1}$*

Definizione 7.9 (Operazioni fra cardinali)**.** Siano k e λ cardinali e siano K e L insiemi tali che $|K| = k$ e $|L| = \lambda$, si definiscono le operazioni:

$$k + \lambda = |K \cup L|$$

$$k \cdot \lambda = |K \times L|$$

Assioma 7.3 (Assioma di fondazione)**.** *In ogni insieme x non vuoto esiste un elemento $y \in x$ tale che $x \cap y = \varnothing$.*

Bibliografia

[End77] Herbert B. Enderton. *Elements of Set Theory*. Academic Press, 1977. ISBN: 9780122384400.

[Dal08] Dirk van Dalen. *Logic and Structure*. Springer, 2008. ISBN: 9783540208792.

[AF14] Vito Michele Abrusci e Lorenzo Tortora Falco. *Logica*. Springer Milano, 2014. ISBN: 9788847055384.