Istituzioni di Logica. I parte: Calcolo dei predicati

Alessandro Berarducci

versione 31 Ott. 2006, ancora in corso d'opera e soggetta a revisioni

Indice

1 Logica proposizionale

1.1 Proposizioni e connettivi

Spesso in matematica, per dimostrare una certa tesi B, si usa il seguente metodo, chiamato ragionamento per casi: se riusciamo a dedurre B sia a partire dall'ipotesi che un certo enunciato A sia vero, sia a partire dall'ipotesi che A sia falso, allora B deve necessariamente essere vera (a prescindere dal fatto che si sia riusciti a determinare se A sia vero o falso). Un noto esempio è il seguente.

Esempio 1.1. Supponiamo di voler dimostrare che esistono due numeri irrazionali a, b tali che a^b è razionale. Consideriamo a tal fine il numero $c = \sqrt{2}^{\sqrt{2}}$. Se esso è razionale (ipotesi A) abbiamo finito perché possiamo prendere $a = b = \sqrt{2}$. Altrimenti esso non è razionale (cioè l'ipotesi A è falsa). Ma $c^{\sqrt{2}} = 2$, quindi anche in questo caso abbiamo mostrato che esistono due numeri irrazionali (c e $\sqrt{2}$) che elevati a potenza forniscono un risultato razionale.

La discussione precedente motiva la seguente definizione.

Definizione 1.2. Una **proposizione** è un enunciato di cui ha senso dire (o ipotizzare), nel dato contesto o nelle date circostanze, che esso sia vero, o falso.

Alla base del metodo del ragionamento per casi è vi è la **concezione classica** della verità, secondo la quale (una volta fissato il contesto o le circostanze) una proposizione è o vera o falsa (**principio del terzo escluso**), ma non può essere sia vera che falsa (**principio di non contraddizione**). In queste note ci atterremo alla concezione classica.

Osservazione 1.3. Nell'ambito della filosofia della matematica, il principio del terzo escluso (e quindi il metodo del ragionamento per casi) è stato criticato dalla **scuola intuizionista** di Brouwer (1881-1966). Gli intuizionisti sostengono che la verità matematica può essere intesa solamente nel senso della conoscibilità (o dimostrabilità). Pertanto secondo questa scuola di pensiero si può affermare che un enunciato A è vero o falso solamente se si sa se sia vero o falso, o perlomeno se si conosce un metodo per poter arrivare, almeno in linea di principio, a determinare se A sia vero o se sia falso. (Ad esempio si conosce un tale metodo per determinare se un numero è primo. Quindi un intuizionista, pur non ritenendo accettabile il principio del terzo escluso in generale, lo riterrebbe accettabile se applicato alla proposizione "$2^{230402457} - 1$ è un numero primo".)

Illustriamo il significato dei connettivi secondo la logica classica.

Definizione 1.4. I **connettivi proposizionali** sono usati per costruire proposizioni complesse a partire da proposizioni semplici. Nella formalizzazione del linguaggio matematico i connettivi di cui faremo maggiore uso sono indicati con i simboli $\neg, \wedge, \vee, \to, \leftrightarrow$. La loro traduzione approssimativa in italiano è la seguente:

$$\begin{gathered}
\text{“}\neg A\text{” significa “non } A\text{” (negazione),}\\
\text{“}A \wedge B\text{” significa “}A \text{ e } B\text{” (congiunzione),}\\
\text{“}A \vee B\text{” significa “}A \text{ o } B\text{” (disgiunzione),}\\
\text{“}A \to B\text{” significa “se } A\text{, allora } B\text{” (implicazione),}\\
\text{“}A \leftrightarrow B\text{” significa “}A \text{ se e solo se } B\text{” (doppia implicazione).}
\end{gathered}$$

Le lettere A, B sopra usate indicano generiche proposizioni. La traduzione che abbiamo dato è solo approssimativa: non c'è una perfetta corrispondenza tra l'uso dei connettivi in una lingua naturale come l'italiano e il loro uso nel linguaggio matematico.

Definizione 1.5. Ad una proposizione ϕ associamo il **valore di verità 1** se essa è vera, e il **valore di verità 0** se essa è falsa. I connettivi proposizionali sono *vero-funzionali* nel senso che il valore di verità di una proposizione composta tramite i connettivi dipende solo dal valore di verità delle proposizioni semplici che la costituiscono. Questo avviene secondo le seguenti **tavole di verità** che precisano il significato dei connettivi secondo la logica classica.

A	$\neg A$
0	**1**
1	**0**

La tavola dice che la proposizione $\neg A$ è vera se A è falsa, ed è invece falsa se A è vera. La negazione inverte il valore di verità. Diamo ora le tavole degli altri connettivi.

A	B	$A \wedge B$	$A \vee B$	$A \to B$	$A \leftrightarrow B$
0	**0**	**0**	**0**	**1**	**1**
0	**1**	**0**	**1**	**1**	**0**
1	**0**	**0**	**1**	**0**	**0**
1	**1**	**1**	**1**	**1**	**1**

Le prime due colonne indicano i quattro possibili valori di verità di A e B. Le altre colonne indicano i corrispondenti valori degli enunciati composti $A \wedge B$, $A \vee B$, $A \to B$, $A \leftrightarrow B$.

La tavola della congiunzione ($\wedge$) dice che $A \wedge B$ è vera se e solo se sia A che B sono vere[1].

Discutiamo ora in dettaglio le tavole del $\vee$ e $\to$. La tavola di verità del connettivo $\vee$ dice che $A \vee B$ è vera se almeno uno di A e B è vero, senza escludere la possibilità che entrambi siano veri. Questa modalità di disgiunzione corrisponde al "vel" della lingua latina e viene chiamata *disgiunzione inclusiva*. Esiste anche una *disgiunzione escusiva*, corrispondente all' "aut" latino, che indichiamo con il simbolo $\oplus$ ed è definita dalla seguente tavola di verità:

[1] Confrontiamo tuttavia l'enunciato: "mi sono sentito male e ho preso la medicina" con "ho preso la medicina e mi sono sentito male". Nel linguaggio comune il primo significa ho preso la medicina perché stavo male, il secondo che è stata la medicina a farmi sentire male. Ci sono circostanze in cui è vero il primo enunciato, e altre circostanze in cui è vero il secondo. Tuttavia secondo la tavola di verità $A \wedge B$ equivale a $B \wedge A$, nel senso che risulta vero negli stessi casi. Questo mostra che il connettivo "e" del linguaggio comune non corrisponde perfettamente a "$\wedge$". Mentre $\wedge$ è vero-funzionale (nel senso che può essere spiegato con la tavola di verità), "e" non lo è.

A	B	$A \oplus B$
0	**0**	**0**
0	**1**	**1**
1	**0**	**1**
1	**1**	**0**

Dalle tavole di verità risulta che l'implicazione $A \to B$ è falsa solo nel caso in cui la premessa A è vera e il conseguente B è falso. In particolare se la premessa A è falsa, l'implicazione $A \to B$ è sempre vera: da una premessa falsa segue ogni proposizione. L'implicazione così definita viene detta **implicazione materiale**.

Esempio 1.6. L'implicazione $x > 5 \to x > 2$ è vera per ogni valore di x. Ad esempio se $x = 6$ essa è vera in quanto sia la premessa $(6 > 5)$ che la conclusione $(6 > 2)$ sono vere, mentre se $x = 1$ è ugualmente vera, perché la premessa $(1 > 5)$ è falsa.

Per dimostrare che vale una implicazione $A \to B$ basta dimostrare che B è vera a partire dall'ipotesi che A sia vera. Questo procedimento è giustificato dal fatto che nel caso A sia invece falsa, l'implicazione è sempre vera in base alla tavola di verità.

Volendo si può fare a meno dell'implicazione e definirla in termini di negazione e disgiunzione. Un enunciato della forma $A \to B$ equivale infatti a $\neg A \vee B$, nel senso che ha lo stesso valore di verità comunque si scelgano le proposizioni A, B. Ciò si può verificare utilizzando le tavole di verità (si assegnino nei quattro modi possibili i valori $\mathbf{0}, \mathbf{1}$ ad A, B e si verifichi che $A \to B$ risulta avere sempre lo stesso valore di $\neg A \vee B$).

Osservazione 1.7. (Convenzioni sull'uso delle parentesi) Utilizzando i connettivi e le parentesi si possono costruire proposizioni sempre più complesse a partire da proposizioni date. Le parentesi hanno lo scopo di indicare l'ordine in cui si effettuano le operazioni. Non potremmo scrivere $A \wedge B \vee C$ in quanto non si capirebbe se intendiamo $(A \wedge B) \vee C$ (prendere prima la congiunzione di A e B e poi fare la disgiunzione con C) o se invece intendiamo $A \wedge (B \vee C)$. Possiamo però scrivere senza ambiguità $A \wedge B \wedge C$ in quanto il connettivo $\wedge$ è associativo, ovvero $(A \wedge B) \wedge C$ equivale a $A \wedge (B \wedge C)$ (nel senso che le due formule risultano vere o false negli stessi casi). Analogamente si può verificare che $(A \vee B) \vee C$ equivale a $A \vee (B \vee C)$ (associatività di $\vee$) e quindi possiamo scrivere senza ambiguità $A \vee B \vee C$. Osserviamo che $A \vee B \vee C$ è vero se almeno uno degli enunciati A, B, C è vero mentre $A \wedge B \wedge C$ è vero se tutti e tre gli enunciati A, B, C sono veri. Per un ulteriore risparmio di parentesi stabiliamo la convenzione che in assenza di parentesi $\wedge$ e $\vee$ legano maggiormente di $\to$ e $\neg$ lega maggiormente di $\wedge$ e $\vee$, quindi ad esempio $\neg A \wedge B \to C$ significa $((\neg A) \wedge B) \to C$.

1.2 Formule proposizionali e tautologie

Se pensiamo alle lettere A, B, C come a nomi di proposizioni fissate (ad esempio A sta per "oggi piove", B sta per "oggi nevica", C sta per "oggi vado al cinema"), una espressione come "$(A \wedge B) \vee C$"denota una proposizioni (ed è quindi vera o falsa). Se invece pensiamo alle lettere A, B, C semplicemente come a variabili, ovvero simboli senza significato, allora la medesima espressione non è una proposizione (non ha senso chiedersi se sia vera o falsa) ma è un esempio di "formula proposizionale". Una formula proposizionale è, parlando informalmente, uno schema astratto da cui si possono ottenere infinite proposizioni andando a sostituire al posto delle variabili delle proposizioni. Ad esempio dalla formula $A \to B$ possiamo ottenere la proposizione vera "Nevica $\to$ fa freddo" sostituendo la variabile A con la proposizione "Nevica" e la variabile B con la proposizione "fa freddo". Dalla stessa formula possiamo anche ottenere la proposizione falsa "$3 = 3 \to 1 > 4$" sostituendo "A" con "$3 = 3$" e "B" con "$1 > 4$". Diamo ora la definizione precisa di formula proposizionale.

Definizione 1.8. Un **linguaggio** proposizionale è un insieme L di simboli, chiamati **variabili proposizionali**. L'insieme delle **formule proposizionali** nel linguaggio L è un insieme di espressioni definito induttivamente come segue. Ogni variabile proposizionale in L è una formula proposizionale. Se ϕ e ψ sono formule proposizionali, lo sono anche $(\neg\phi)$, $(\phi \wedge \psi)$, $(\phi \vee \psi)$, $(\phi \to \psi)$. Talvolta conviene introdurre tra le formule proposizionali il simbolo $\perp$, che sta intuitivamente a rappresentare una formula sempre falsa. (Facciamo a meno di $\phi \leftrightarrow \psi$ considerandola come abbreviazione di $(\phi \to \psi) \wedge (\psi \to \phi)$.)

Definizione 1.9. Una **interpretazione booleana** (o **valutazione booleana**) di un linguaggio proposizionale L è una funzione M che associa ad ogni variabile proposizionale $A \in L$ un valore $M(A) \in \{\mathbf{0}, \mathbf{1}\}$ ($\mathbf{0}$ per falso, $\mathbf{1}$ per vero). Osserviamo che se L contiene n variabili proposizionali, ci sono 2^n possibili interpretazioni. Una volta fissata una interpretazione M tutte le formule del linguaggio ricevono un valore vero o falso in base alle tavole di veritá. Piú precisamente estendiamo M ad una funzione che associa ad ogni formula proposizionale nel linguaggio L un valore di verità procedendo dalle formule più semplici a quelle via via più complesse nel modo seguente: $M(\neg\phi) = \mathbf{1}$ se e solo se $M(\phi) = \mathbf{0}$, $M(\alpha \wedge \beta) = \mathbf{1}$ se e solo se $M(\alpha) = \mathbf{1}$ e $M(\beta) = \mathbf{1}$, $M(\alpha \vee \beta) = \mathbf{1}$ se e solo se almeno uno tra $M(\alpha)$ ed $M(\beta)$ ha il valore $\mathbf{1}$, $M((\alpha \to \beta)) = \mathbf{1}$ in tutti i casi eccetto che nel caso $M(\alpha) = \mathbf{1}$ e $M(\beta) = \mathbf{0}$. Infine stabiliamo che $M(\perp) = \mathbf{0}$, ovvero $\perp$ è una formula falsa in tutte le interpretazioni (non è la sola: anche $A \wedge \neg A$ ha questa proprietà).

Definizione 1.10. Una formula proposizionale ϕ si dice una **tautologia** se è vera per tutte le interpretazioni delle sue variabili.

Ad esempio $A \vee \neg A$ è una tautologia, in quanto risulta vera sia se A è vera, sia se A è falsa. Analogamente $(A \to B) \wedge \neg B \to \neg A$ è una tautologia, in quanto usando le tavole si vede che essa risulta vera nei quattro possibili casi per i valori di A e B (A vera e B vera, A vera e B falsa, A falsa e B vera, A falsa e B falsa).

Osservazione 1.11. Un algoritmo per riconoscere se una formula con n variabili è una tautologia è quello di considerare i 2^n possibili casi per i valori di verità delle sue variabili e verificare usando le tavole che in ognuno dei casi la proposizione composta che ne risulta è vera. Si tratta di una procedura semplice e meccanica ma che nel caso ci siano molte variabili richiede molto tempo, anche da parte di un calcolatore. Il problema di stabilire se esistano metodi che richiedano un tempo polinomiale nel numero delle variabili anziché esponenziale è tuttora irrisolto.

Si noti che secondo la definizione appena data, e nel successivo sviluppo formale della teoria, il concetto di tautologia si applica solo ed esclusivamente alle *formule proposizionali* e non alle proposizioni stesse. Tuttavia, parlando a livello informale, una proposizione ottenuta per sostituzione da una tautologia sarà talvolta chiamata essa stessa tautologia. Ad esempio la proposizione "piove o non piove" sarà informalmente detta una tautologia anche se ciò che realmente si intende è che la formula proposizionale da cui proviene, ovvero la formula $A \vee \neg A$, è una tautologia. Come si vede da questo esempio una tautologia ha contenuto informativo nullo. Affermare "piove o non piove" non ci dà alcuna informazione sul fatto se piova o meno. Proprio perché una tautologia è vera a prescindere dalla verità o falsità degli enunciati elementari che la costituiscono, essa non comunica nulla riguardo alla verità o falsità di questi ultimi. In effetti una tautologia è vera in virtù esclusivamente della sua forma sintattica, e non del suo contenuto.

1.3 Conseguenza (tauto)logica

Abbiamo visto che le tautologie non comunicano informazione. È lecito dunque domandarsi a cosa servano. Una possibile risposta è che esse giocano un ruolo importante nelle dimostrazioni matematiche, e più in generale nelle argomentazioni logiche di qualsiasi tipo. Consideriamo il seguente esempio:

Esempio 1.12. L'assassino è il professore o l'assessore. Ma non è l'assessore. Quindi è il professore.

Per condurre questo ragionamento, cioè per mostrare che la tesi è conseguenza logica delle premesse, abbiamo implicitamente utilizzato la tautologia $((A \vee B) \wedge \neg B) \to A$, applicandola al caso in cui A sta per "l'assassino è il professore", e B sta per "l'assassino è l'assessore".

In generale possiamo dare la seguente definizione di conseguenza logica per la logica proposizionale.

Definizione 1.13. Una formula proposizionale β è **conseguenza logica** (o **conseguenza tautologica**) di una formula proposizionale α, se la formula $\alpha \to \beta$ è un tautologia (cioè β è vera per tutti i valori delle variabili in cui α è vera). Scriviamo

$$\alpha \models \beta$$

per indicare che β è conseguenza logica di α. Più in generale una formula β è conseguenza logica di un insieme di altre formule $\alpha_1, \dots, \alpha_n$, se $(\alpha_1 \wedge \dots \wedge \alpha_n) \to$

β è una tautologia, ovvero se in tutti i casi in cui tutte le α_i sono vere, anche β è vera. Scriviamo

$$\alpha_1, \ldots, \alpha_n \models \beta$$

per indicare questo fatto. Due formule sono **logicamente equivalenti** se ognuna delle due è conseguenza logica dell'altra (ciò equivale a dire che le due formule assumono gli stessi valori di verità per i medesimi valori delle variabili).

Esempio 1.14. $A \wedge (B \vee C)$ è logicamente equivalente a $(A \wedge B) \vee (A \wedge C)$, come si può verificare assegnando ad A, B, C i valori $\mathbf{1}, \mathbf{0}$ negli otto modi possibili e verificando che in ciascun caso il valore di $A \wedge (B \vee C)$ è uguale a quello di $(A \wedge B) \vee (A \wedge C)$. Similmente si verifica che $\neg(A \vee B)$ equivale a $\neg A \wedge \neg B$.

Osservazione 1.15. Si noti la differenza tra implicazione materiale ($\rightarrow$) e conseguenza logica ($\models$). Secondo la tavola di verità dell'implicazione, date due *proposizioni* A e B vale sempre una delle due implicazioni $A \rightarrow B$ oppure $B \rightarrow A$ (infatti se sono entrambe false si implicano a vicenda, mentre se una delle due è vera l'altra certamente la implica). Non è però sempre vero che date due *formule proposizionali* ϕ e ψ una delle due è conseguenza logica dell'altra.

A livello intuitivo possiamo dire che mentre una implicazione materiale può essere vera per motivi contingenti senza che ci sia un reale nesso tra le proposizioni coinvolte (come in " l'acqua bolle a 100 gradi $\rightarrow$ Roma è la capitale d'Italia"), la conseguenza logica esprime invece una implicazione che deve essere necessariamente vera in tutte le possibili circostanze in base al significato stesso dei connettivi.

1.4 Teorie proposizionali

Risulta conveniente, per gli sviluppi successivi della teoria, estendere la definizione di conseguenza logica al caso di un insieme possibilmente infinito Γ di ipotesi. Ciò può essere fatto nel modo seguente.

Definizione 1.16. Fissiamo un linguaggio proposizionale L, cioè un insieme (possibilmente infinito) di variabili proposizionali. Una **L-teoria** proposizionale è un insieme Γ (possibilmente infinito, o anche vuoto) di formule proposizionali nel linguaggio L. Le formule appartenenti a Γ vengono chiamate assiomi della teoria Γ. Un **modello** di una L-teoria Γ è una interpretazione delle variabili di L che rende vere tutte le formule di Γ (ogni singola formula conterrà ovviamente solo un numero finito di variabili). Diciamo che una formula ϕ nel linguaggio L è **conseguenza logica** di Γ, e scriviamo

$$\Gamma \models \phi,$$

se ogni modello di Γ rende vera ϕ. Se Γ è vuoto scriviamo $\models \phi$ per $\Gamma \models \phi$. Osserviamo che se Γ è vuoto tutte le intepretazioni sono modelli di Γ (in quanto, proprio perché vuoto, non può contenere una formula che viene resa falsa). In base alle definizioni $\models \phi$ se e solo se ϕ è una tautologia.

2 Calcolo dei predicati

2.1 Predicati e quantificatori

Un **predicato** o **relazione** è una funzione che associa agli elementi di un dato dominio di oggetti un valore di verità, che può essere vero o falso. Ad esempio il predicato "essere un numero primo", associa **1** (vero) ai numeri primi e **0** ai numeri composti. La relazione $<$ tra numeri reali associa **1** alle coppie di numeri (a, b) che verificano la relazione (ovvero tali che $a < b$) e **0** alle altre. In generale se P è un predicato ad un posto scriviamo $P(x)$ per esprimere il fatto che x verifica il predicato. Similmentre se Q è un predicato a due posti scriviamo $Q(x, y)$ per esprimere il fatto che (x, y) verifica il predicato; se P è un predicato a tre posti scriviamo $P(x, y, z)$ per esprimere il fatto che la terna (x, y, z) lo verifica, e così via.

Assumiamo che il lettore abbia già qualche familiarità a livello intuitivo con i **quantificatori** $\exists$ (esiste) e $\forall$ (per ogni). Ricordiamo che se P è un predicato unario, la proposizione $\exists x P(x)$ esprime il fatto che esiste almeno un oggetto a nel dominio considerato che verifica il predicato, ovvero tale che valga $P(a)$. La proposizione $\forall x P(x)$ dice che per tutti gli oggetto a nel dominio considerato vale $P(a)$. Per predicati binari possiamo avere diverse combinazioni di $\forall$ e $\exists$. $\forall x \exists y P(x, y)$ significa che dato un x posso sempre trovare un y, che in genere dipenderà da x, tale che $P(x, y)$, mentre invece $\exists y \forall x P(x, y)$ significa che è possibile trovare un y che va bene per tutti gli x, ovvero un y tale che per ogni x vale $P(x, y)$. Ad esempio se il dominio delle variabili è un insieme di persone, e $P(x, y)$ è la relazione "y è padre di x", $\forall x \exists y P(x, y)$ dice che ogni persona ha un padre, mentre $\exists y \forall x P(x, y)$ esprime la proposizione falsa che asserisce l'esistenza di una persona y che è padre di tutti (inclusa se stessa).

2.2 Linguaggi del primo ordine

Abbiamo bisogno di un formalismo adatto ad esprimere le leggi logiche valide per i quantificatori.

Definizione 2.1. Un **linguaggio del primo ordine** è un insieme L di simboli (possibilmente anche vuoto) divisi in tre categorie, simboli di costante, simboli di funzione, e simboli di relazione, dove ad ogni simbolo è associato un numero naturale detto "arietà" del simbolo (che servirà ad indicare il numero degli argomenti a cui va applicato il simbolo). L'arietà di ogni simbolo di costante è zero, mentre le arietà dei simboli di funzione e di relazione sono arbitrari interi positivi. Una possibile formalizzazione in termini insiemistici della nozione di simbolo sopra data è la seguente: un simbolo è una terna ordinata (a, i, n) dove a è il nome del simbolo, $i \in \{1, 2, 3\}$ indica il tipo del simbolo, ovvero se si tratti di un simbolo di costante, funzione o relazione, ed n è l'arietà.

Definizione 2.2. Sia L una linguaggio del primo ordine. Una L-*struttura* o (L-**interpretazione**) M consiste di:

1. Un insieme non vuoto $dom(M)$ detto *dominio* (oppure *universo*) della struttura[2].

2. Una corrispondenza[3] $c \mapsto c_M$ che associa ad ogni simbolo di costante c di L un elemento $c_M \in dom(M)$, detto interpretazione del simbolo c in M.

3. Una corrispondenza $f \mapsto f_M$ che associa ad ogni simbolo di funzione f di L di arietà n, una funzione $f_M : dom(M)^n \to dom(M)$, detta interpretazione del simbolo f in M.

4. Una corrispondenza $R \mapsto R_M$ che associa ad ogni simbolo di relazione R di L di arietà n, una relazione $R_M \subseteq dom(M)^n$, detta interpretazione del simbolo R in M. (Identifichiamo una relazione ad n posti con l'insieme delle n-uple che la verificano.)

Esempio 2.3. Un grafo $G = (V_G, E_G)$ è dato da un insieme non vuoto V_G di *vertici* dotato di una relazione binaria E_G. Esso può essere visto come una L-struttura (con dominio V_G) nel linguaggio $L = \{E\}$, dove E è un simbolo di relazione binaria.

Quando non ci sia rischio di confusione useremo la stessa notazione per indicare sia la struttura che il suo dominio (ad esempio scriveremo $G = (G, E_G)$, dove G indica sia il grafo che l'insieme dei suoi vertici).

Esempio 2.4. Un anello ordinato $M = (M, 0_M, 1_M, +_M, \cdot_M, <_M)$ è un struttura nel linguaggio $L = \{0, 1, +, \cdot, <\}$, dove $0, 1$ sono simboli di costante, $+, \cdot$ sono simboli di funzioni binarie, $<$ è un simbolo di relazione binaria, e i simboli $0, 1, +, \cdot, <$ sono intepretati in modo da soddisfare gli assiomi degli anelli ordinati.

Per semplicità talvolta ometteremo i sottoindici e useremo la stessa notazione per i simboli e la loro interpretazione. Ad esempio l'anello degli interi viene in genere indicato con $(\mathbb{Z}, 0, 1, +, \cdot)$.

2.3 Termini e Formule

Fissiamo un linguaggio L e un insieme infinito V di simboli chiamati **variabili** (o **variabili individuali**).

Definizione 2.5. Definiamo induttivamente l'insieme $Ter_L(V)$ dei **L-termini** (con variabili da V) come il più piccolo insieme di espressioni tale che:

1. Ogni variabile $x \in V$ è un L-termine;

2. ogni simbolo di costante di L è un L-termine;

[2] Sarà il dominio su cui variano le variabili di cui faremo uso. Stiamo quindi facendo l'assunzione che vi sia un unico dominio per tutte le variabili.

[3] Usiamo la parola 'corrispondenza' come sinonimo di 'funzione'.

3. se $t_1, \dots, t_n$ sono L-termini, e f è un simbolo di funzione di arietà n della segnatura L, allora $f(t_1, \dots, t_n)$ è un L-termine.

Un termine in cui non occorrano variabili viene detto **termine chiuso**. Chiaramente i termini chiusi possono esserci solo se il linguaggio contiene almeno un simbolo di costante.

Esempio 2.6. Se L contiene un simbolo di funzione binaria f e un simbolo di costante c, allora l'espressione $f(x, f(c, y))$ (dove x, y sono variabili) è un termine, e l'espressione $f(c, c)$ è un termine chiuso.

Passiamo ora a definire l'insieme delle L-formule.

Definizione 2.7. Una **L-formula atomica** è una espressione della forma $t_1 = t_2$, dove t_1, t_2 sono L-termini, oppure della forma $R(t_1, \dots, t_n)$, dove R è un simbolo di relazione n-aria di L (se ve ne sono) e $t_1, \dots, t_n$ sono L-termini.

Per definire l'insieme delle formule (non atomiche), oltre ai simboli fino ad ora introdotti faremo uso dei simboli $\neg, \wedge, \vee, \rightarrow$ per i connettivi proposizionali, i simboli $\exists$ e $\forall$ per i quantificatori esistenziale e universale, il simbolo $=$ per l'uguaglianza, e le parentesi.

Definizione 2.8. L'insieme delle **L-formule** è definito induttivamente come il più piccolo insieme di espressioni tale che:

1. Ogni L-formula atomica è una L-formula.
2. Se α e β sono L-formule, allora $(\neg\alpha)$, $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$ e $(\alpha \rightarrow \beta)$ sono L-formule.
3. Se α è una L-formula e x è una variabile, allora $(\forall x \alpha)$ e $(\exists x \alpha)$ sono L-formule.

Osservazione 2.9. Nel dare esempi di L-formule ometteremo le parentesi ridondanti quando non sussista ambiguità di lettura, ovvero qualora esista un unico modo di aggiungere le parentesi mancanti in modo da ottenere una L-formula. Ad esempio la formula $(((x = x) \wedge (x = y)) \vee (y = z))$ può essere scritta in forma abbreviata come $(x = x \wedge x = y) \vee y = z$. Per un ulteriore risparmio di parentesi stabiliamo la convenzione che in assenza di parentesi $\wedge$ e $\vee$ legano maggiormente di $\rightarrow$ e $\neg$ lega maggiormente di $\wedge$ e $\vee$, quindi ad esempio $\neg\alpha \wedge \beta \rightarrow \gamma$ significa $(((\neg\alpha) \wedge \beta) \rightarrow \gamma)$. Conveniamo inoltre che un quantificatore seguito da più variabili stia ad indicare la ripetizione del quantificatore su ciascuna variabile. Ad esempio $\forall xy\phi$ sta per $(\forall x(\forall y\phi))$. Resta inteso che queste sono solo abbreviazioni informali e la definizione di L-formula resta quella sopra data.

Definizione 2.10. Le **sottoformule** di una formula ϕ sono per definizione quelle formule che intervengono nella formazione induttiva di ϕ (inclusa la ϕ stessa). Quindi ad esempio le sottoformule di $(\alpha \rightarrow \beta)$ sono $(\alpha \rightarrow \beta)$ e tutte le sottoformule di α e di β (incluse α e β stesse).

Definizione 2.11. Un'occorrenza di una variabile x in una formula α si dice **legata** se occorre in una sottoformula β di α immediatamente preceduta da un quantificatore $\forall x$ o $\exists x$. Un'occorrenza non legata si dice **libera**. Le *variabili libere di una formula* sono le variabili che hanno almeno una occorrenza libera nella formula. Una formula senza variabili libere viene detta **formula chiusa** o **enunciato**.

Esempio 2.12. Ad esempio le variabili libere di $x = y \wedge \forall u \exists x(x = u)$ sono la x e la y (sebbene la x abbia anche una occorrenza legata).

Definizione 2.13. (Sostituzioni) Se α è un termine o una formula, e $t_1, \ldots, t_n$ sono termini, indichiamo con $\alpha(t_1/x_1, \ldots, t_n/x_n)$ il termine o formula risultante da α dalla simultanea sostituzione di ogni occorrenza libera della variabile x_i in α con t_i per $i = 1, \ldots, n$. Se le variabili $x_1, \ldots, x_n$ di cui si sta parlando sono sottointese scriviamo più semplicemente $\alpha(t_1, \ldots, t_n)$ invece di $\alpha(t_1/x_1, \ldots, t_n/x_n)$. Ad esempio $\forall x \alpha(x) \to \alpha(t)$ è la stessa cosa di $\forall x \alpha \to \alpha(t/x)$ (in quanto se sottointendiamo la x, allora $\alpha(t)$ coincide con $\alpha(t/x)$ e $\alpha(x)$ coincide con $\alpha(x/x)$, che è proprio α).

Esercizio 2.14. In generale la formula $\alpha(t_1/x_1, t_2/x_2)$, ottenuta per sostituzione simultanea, non coincide con la formula $\alpha(t_1/x_1)(t_2/x_2)$, in cui la sostituzione (t_2/x_2) viene effettuata *dopo* la sostituzione (t_1/x_1). Nel caso di termini chiusi tutti i modi di effettuare le sostituzioni (simultanee o in sequenza) danno lo stesso risultato.

2.4 Semantica di Tarski

Data una L-formula chiusa ϕ, essa può in generale essere vera in alcune interpretazioni e falsa in altre. Prima di dare le definizioni formali diamo alcuni esempi.

Esempio 2.15. $\forall x \exists y P(x, y)$ è una formula in un linguaggio con un simbolo di predicato binario P. Essa è vera in alcune intepretazioni e falsa in altre. Ad esempio è vera se le variabili x, y variano sui numeri interi e $P(x, y)$ è interpretato come la relazione $x > y$, mentre è falso se le variabili variano sugli interi non negativi e $P(x, y)$ è intepretato di nuovo come $x > y$.

Esempio 2.16. $\forall x(P(x) \to \exists y(f(x, y) = c))$ è una formula in un linguaggio con un simbolo di funzione binaria f, un simbolo di relazione unaria P e un simbolo di costante c. Essa è vera in certe intepretazioni e falsa in altre. Ad esempio supponiamo che le variabili x, y varino sui numeri reali, $P(x)$ è interpretato come "x è diverso da zero", f è interpretata come la moltiplicazione tra due numeri reali e c è interpretata come il numero uno. In questa interpretazione la formula esprime la seguente proposizione: "per ogni numero reale x, se x è diverso da zero, esiste un numero reale y tale che $x \cdot y = 1$". Si tratta di una proposizione vera, che asserisce l'esistenza, nei numeri reali, dell'inverso moltiplicativo di ciascun numero diverso da zero.

Esempio 2.17. $\neg\forall x P(x) \to \exists x \neg P(x)$ è una formula in un linguaggio con un simbolo di predicato unario P. Essa è vera in tutte le intepretazioni (cioè è "logicamente valida").

Passiamo ora alle definizioni formali. Data una L-struttura M, per poter definire cosa significhi che una formula della forma $\forall x\phi$ o $\exists x\phi$ è vera in M, conviene non limitarsi a considerare le L-formule, ma un insieme di formule in un linguaggio più grande in cui abbiamo un simbolo di costante c_a associato ad ogni elemento di M. (Questo permetterà di dare la seguente definizione: $\forall x\phi(x)$ è vera in M se e solo se per ogni $a \in M$ la formula $\phi(c_a)$ è vera in M.)

Definizione 2.18. Data una L-struttura M, sia $L[M]$ il linguaggio ottenuto aggiungendo all'insieme dei simboli di L un nuovo simbolo di costante c_a per ogni elemento a del dominio di M. Sebbene sia importante tener distinto il simbolo c_a dall'elemento a, per non appesantire la notazione spesso scriveremo a invece di c_a. Ad esempio scriveremo $\phi(a/x)$ (o semplicemente $\phi(a)$ se x è sottointesa) per denotare la formula $\phi(c_a/x)$ ottenuta sostituendo le occorrenze libere di x nella formula ϕ con il simbolo c_a. Ribadiamo che si tratta solo di un abuso di notazione e non di una reale identificazione.

Definizione 2.19. Dato un $L[M]$-termine chiuso t, definiamo un elemento $M(t)$ del dominio di M, chiamato l'**interpretazione del termine t in M**, nel modo seguente.

1. Se c_a è la costante associata all'elemento $a \in M$, allora $M(c_a) = a$.
2. Se c è un simbolo di costante di L, poniamo $M(c) = c^M$, dove $c^M \in M$ è l'elemento che la struttura M associa al simbolo di costante c.
3. Sia ora t un termine della forma $f(t_1, \dots, t_n)$, dove f è un simbolo di funzione n-aria di L e i t_i sono $L[M]$-termini chiusi. Induttivamente risultano definiti gli elementi $M(t_i) \in M$ (o più precisamente $M(t_i) \in \mathrm{dom}(M)$). Per definizione di L-struttura risulta data una funzione $f^M \colon M^n \to M$. Possiamo dunque definire $M(f(t_1, \dots, t_n)) = f^M(M(t_1), \dots, M(t_n))$.

Il seguente esempio chiarisce la distinzione tra termini di un linguaggio ed elementi di una struttura.

Esempio 2.20. Sia L un linguaggio con un simbolo di funzione unaria s, un simbolo di funzione binaria f e un simbolo di costante 0. Sia N la L-struttura il cui dominio è l'insieme dei numeri naturali e in cui s, f e 0 sono interpretati come la funzione successore, la funzione somma, e il numero zero. Ogni elemento di N è allora l'interpretazione di un termine chiuso di L (ad esempio il numero due è l'interpretazione del termine $s(s(0))$). Consideriamo ora la L-struttura R il cui dominio sono i numeri reali, e in cui $s, f, 0$ sono interpretati di nuovo come la funzione successore, la funzione somma e lo zero (dove per definizione il successore di un numero reale x si ottiene sommando uno ad x). In R non è più vero che ogni elemento del dominio è l'interpretazione di un termine chiuso di L (ad esempio $\sqrt{2}$ è un numero reale che non è l'interpretazione di alcun termine di

L). Tuttavia se consideriamo il liguaggio esteso $L[R]$ in cui abbiamo aggiunto una costante c_a per ogni elemento a del dominio di R, allora ogni elemento a del dominio è l'interpretazione di almeno un termine (la costante c_a). In generale può capitare che vi siano termini diversi con la stessa interpretazione (ad esempio 0 e $f(0,0)$, se f è interpretata come la funzione somma e 0 come lo zero). Quindi la corrispondenza tra termini chiusi ed elementi del dominio (ovvero la funzione che manda un termine chiuso t nella sua intepretazione) può non essere iniettiva, e inoltre se ci restringiamo a termini del linguaggio non esteso L può non essere neppure surgettiva.

Una L-struttura M determina una partizione dell'insieme delle $L[M]$-formule atomiche chiuse in due sottoinsiemi: quello delle formule vere e quello delle formule false.

Definizione 2.21. Sia R un simbolo di relazione n-ario di L (se ve ne sono), e siano $t_1, t_2, \ldots, t_n$ dei $L[M]$-termini chiusi.

1. Diciamo che la formula $R(t_1, \ldots, t_n)$ è vera in M se e solo se la n-upla $(M(t_1), \ldots, M(t_n))$ appartiene ad R_M.
2. Diciamo che la formula $t_1 = t_2$ è vera in M se e solo se $M(t_1)$ e $M(t_2)$ sono lo stesso elemento.

Quindi ad esempio la formula $0 = f(0,0)$ è vera nella struttura R dell'esempio 2.20.

Consideriamo ora il caso delle $L[M]$-formule chiuse arbitrarie, ovvero non necessariamente atomiche.

Lemma 2.22. *Data una partizione delle formule atomiche chiuse di $L[M]$ in due sottoinsiemi V ed F (ad esempio la partizione in formule atomiche vere e false) esiste un unico modo di definire una partizione dell'insieme di tutte le $L[M]$-formule chiuse in due sottonsiemi $V' \supset V$ ed $F' \supset F$ in modo che:*

1. *Se ϕ è atomica, $\phi \in V'$ se e solo se $\phi \in V$.*
2. *Se ϕ è una qualsiasi $L[M]$-formula chiusa, ϕ appartiene ad uno e uno solo dei due insiemi V' ed F'.*
3. *$(\forall x \phi) \in V'$ se e solo se per ogni $a \in dom(M)$, $\phi(a/x) \in V'$.*
4. *$(\exists x \phi) \in V'$ se e solo se esiste $a \in dom(M)$ tale che $\phi(a/x) \in V'$.*
5. *$\neg\phi \in V'$ se e solo se $\phi \in F'$.*
6. *$(\phi \wedge \psi) \in V'$ se e solo se $\phi \in V'$ e $\psi \in V'$.*
7. *$(\phi \vee \psi) \in V'$ se e solo se $\phi \in V'$ o $\psi \in V'$.*
8. *$(\phi \to \psi) \in F'$ se e solo se $\phi \in V'$ e $\psi \in F'$.*

Dimostrazione. L'appartenenza di una formula a V' o F' è determinata dall'appartenenza a V' o F' di formule di complessità minore (cioè con meno connettivi o quantificatori). Quindi per induzione V' ed F' esistono e sono unici. $\square$

Definizione 2.23. Una L-struttura M determina, come abbiamo visto, una partizione delle $L[M]$-formule atomiche in due sottoinsiemi V ed F, quello delle formule atomiche vere, e quello delle formule atomiche false. Il lemma precedente ci permette di definire due altri insiemi V', F', che partizionano l'insieme delle $L[M]$-formule chiuse (non solo quelle atomiche). Per definizione diciamo che le formule di V' sono vere in M, e che quelle di F' sono false in M. Scriviamo

$$M \models \phi$$

per indicare il fatto che ϕ è vera in M.

Abbiamo così definito l'insieme delle $L[M]$-formule chiuse vere in M, e quindi in particolare il sottoinsieme delle L-formule chiuse vere in M. Spesso sono queste ultime quelle a cui siamo principalmente interessati, ma per poterle definire siamo dovuti passare attraverso le $L[M]$-formule per poter trattare i quantificatori. La seguente osservazione mette in luce l'aspetto non costruttivo della definizione di verità che abbiamo dato.

Osservazione 2.24. Si noti che V' ed F', sebbene siano stati definiti induttivamente a partire da V, F, non sono stati definiti in modo costruttivo, ovvero non è chiaro dalla definizione se vi sia un algoritmo stabilire se una $L[M]$-formula chiusa sia in V' o in F' (anche supponendo che vi sia un tale algoritmo per il sottoinsieme delle formule atomiche). Per strutture finite la definizione è in effetti costruttiva, ma se la il dominio di M è infinito, per stabilire se $\forall x \phi$ sia in V' dovrei controllare se $\phi(a/x)$ sia in V' per ognuna delle infinite possibili scelte di $a \in M$, cosa evidentemente impossibile da realizzare con un algoritmo. Ciò tuttavia non esclude che, per determinate strutture infinite, vi possa essere un algoritmo in grado di stabilire se una formula chiusa sia vera nella data struttura (magari limitandosi alle formule del linguaggio non esteso L). Un tale algoritmo si potrebbe basare su una caratterizzazione delle formule vere in una data struttura M equivalente, ma più costruttiva, di quella fornita dalla definizione (e che funziona solo per la data M e non per altre strutture). Ad esempio si può dimostrare che per la struttura dei numeri naturali, in un linguaggio L con un simbolo per lo zero, il successore e la somma, esiste un algoritmo per il riconoscimento delle L-formule chiuse vere (Presburger). Tuttavia se mettiamo nel linguaggio anche un simbolo per il prodotto, un tale algoritmo non esiste più (Gödel), e lo stesso avviene per i numeri razionali (J. Robinson), mentre invece per i numeri reali (sempre con somma e prodotto) si conoscono degli algoritmi per riconoscere gli L-enunciati veri (A. Tarski). Molti dei problemi irrisolti della matematica, come ad esempio la congettura di Goldbach (ogni numero pari maggiore di 3 è somma di due numeri primi), equivalgono a chiedersi se una data formula in un linguaggio con somma a prodotto è vera nei numeri naturali; non deve dunque stupire che non esista un algoritmo generale per risolvere tali questioni, anche se naturalmente aver dimostrato che non esiste è un notevole risultato (tutto ciò dipende naturalmente anche dalla definizione di algoritmo).

2.5 Insiemi definibili

Definizione 2.25. Sia M una L-struttura. Un sottoinsieme A di M^n è **0-definibile** se esiste una L-formula $\phi(x_1, \ldots, x_n)$ (con variabili libere incluse tra le $x_1, \ldots, x_n$) tale che A è l'insieme di tutte quelle n-uple $(a_1, \ldots, a_n)$ di elementi di M che verificano la formula, ovvero tali che $M \models \phi(a_1, \ldots, a_n)$. Analogamente diciamo che A è **definibile** se esiste una formula $\phi(x_1, \ldots, x_n)$ del linguaggio ampliato $L[M]$ tale che A è l'insieme delle n-uple $(a_1, \ldots, a_n)$ tali che $M \models \phi(a_1, \ldots, a_n)$.

Esercizio 2.26. Il cerchio unitario $\{(x, y) \in \mathbb{R}^2 \mid x^2+y^2 = 1\}$ è 0-definibile nella struttura $(\mathbb{R}, +, \cdot)$, mentre il cerchio di raggio π (pur non essendo 0-definibile) è definibile. In generale si può dimostrare che il cerchio di raggio r è 0-definibile se e solo se r è un numero reale algebrico.

Esercizio 2.27. L'insieme dei numeri primi è definibile nella struttura $(\mathbb{N}, +, \cdot)$.

Esempio 2.28. Gödel ha dimostrato che l'insieme delle coppie $(a, b) \in \mathbb{N}^2$ tali che $b = 2^a$ è definibile nella struttura $(\mathbb{N}, +, \cdot)$.

2.6 Conseguenza logica

Definizione 2.29. Una **teoria** T è una coppia consistente di una segnatura L e di un insieme di L-enunciati chiamati *assiomi di* T. Quando L sia sottointeso identifichiamo T con l'insieme dei suoi assiomi, e penseremo quindi a T come ad un insieme di L-enunciati.

Definizione 2.30. La teoria dei gruppi ha come assiomi le formule

$$\begin{aligned}
&x \cdot (y \cdot z) = (x \cdot y) \cdot z,\\
&x \cdot 1 = x,\\
&1 \cdot x = 1,\\
&x \cdot x^{-1} = 1,\\
&x^{-1} \cdot x = 1,
\end{aligned}$$

implicitamente precedute da $\forall xyz$, e formulate in una segnatura con un simbolo di costante 1 per l'elemento neutro, un simbolo di funzione binaria $\cdot$ per l'operazione di gruppo, e un simbolo di funzione unaria per l'inverso moltiplicativo x^{-1}.

Definizione 2.31. Un **modello** di una L-teoria T è una L-struttura in cui risultano veri tutti gli assiomi di T. (Ad esempio un gruppo è, per definizione, un modello della teoria dei gruppi.) Se M è un modello di T scriviamo $M \models T$. Quindi $M \models T$ se per ogni assioma ϕ di T, si ha $M \models \phi$. Indichiamo con $Mod_L(T)$ la classe di tutti i modelli di T. Una L-teoria T si dice **soddisfacibile**, se ha almeno un modello.

Definizione 2.32. (Conseguenza logica) Sia ϕ una L-formula chiusa e T una L-teoria. Diciamo che ϕ **segue logicamente** da T, e scriviamo $T \models \phi$, se ϕ è vera in tutti i modelli di T, ovvero non esiste alcuna L-struttura che rende veri tutti gli assiomi di T e non rende vera ϕ. In altre parole:

$$T \models \phi \text{ se e solo se } Mod_L(T) \subseteq Mod_L(\phi).$$

In particolare se T è **insoddisfacibile**, cioè se $Mod_L(T) = \emptyset$, allora vale sempre $T \models \phi$ (in quanto l'insieme vuoto è contenuto in ogni altro insieme).

Esercizio 2.33. Sia T un insieme di L-enunciati, sia ϕ un L-enunciato, e sia $L' \supset L$. Allora $Mod_L(T) \subseteq Mod_L(\phi)$ se e solo se $Mod_{L'}(T) \subseteq Mod_{L'}(\phi)$.

L'esercizio giustifica la scelta di non aver reso esplicito il linguaggio L nella notazione $T \models \phi$. Il linguaggio è irrilevante, a condizione naturalmente che esso contenga tutti i simboli presenti in ϕ e nelle formule di T (anche se potrebbe contenerne anche altri).

Definizione 2.34. (Formule logicamente valide) Sia L una data segnatura e sia ϕ una L-formula chiusa. Diciamo che ϕ è logicamente valida, e scriviamo $\models \phi$, se ϕ è vera in ogni L-struttura. Osserviamo che se T è la L-teoria con un insieme vuoto di assiomi, allora ogni L-struttura è modello di T, e pertanto si ha $\models \phi$ se e solo se $T \models \phi$.

Esercizio 2.35. Sia L la segnatura con un simbolo di funzione binario f. La L-formula

$$\forall xyz(f(f(x,y),z) = y) \to \forall xy(x = y)$$

è logicamente valida.

2.7 Termini sostituibili

Osservazione 2.36. L'implicazione espressa dalla formula $\forall x\alpha(x) \to \alpha(t)$ non è sempre logicamente valida. Sia $\phi(x)$ la formula $\exists y(x = y)$ e sia t il termine $y + 1$. Allora $\forall x\phi(x)$ è l'enunciato $\forall x\exists y(x = y)$, che è sempre vero, mentre $\phi(t)$ è l'enunciato $\exists y(y + 1 = y)$ che non è vero se interpretiamo i simboli $+, 1$ come la addizione tra numeri naturali e come il numero naturale "uno".

L'osservazione precedente motiva la seguente definizione.

Definizione 2.37. Un termine t è **sostituibile al posto della variabile** x **nella formula** α se per ogni variabile y in t, nessuna occorrenza libera di x in α appare all'interno di una sottoformula della forma $\exists y\beta$ o $\forall y\beta$. In altre parole questo significa che le variabili di t non diventano legate dopo che si è effettuata la sostituzione $\alpha(t/x)$.

Si noti che un termine chiuso è sempre sostituibile al posto di qualsiasi variabile in qualsiasi formula.

Lemma 2.38. *Sia t un termine sostituibile al posto di x nella formula α e supponiamo che le variabili libere di $\forall x\alpha(x) \to \alpha(t)$ siano incluse in $\{y_1, \dots, y_n\}$. Allora $\forall y_1, \dots, y_n(\forall x\alpha(x) \to \alpha(t))$ è logicamente valida.*

Dimostrazione. Dobbiamo mostrare che per ogni L-struttura M, abbiamo

$$M \models \forall y_1, \dots, y_n(\forall x\alpha(x) \to \alpha(t)) \tag{1}$$

Siano $a_1, \dots, a_n \in dom(M)$ sia s la sostituzione $(a_1/y_1, \dots, a_n/y_n)$. Dobbiamo dunque mostrare che:

$$M \models ((\forall x\alpha(x))^s \to \alpha(t)^s) \qquad (2).$$

Ora poichè t è sostituibile, $\alpha(t)^s = \alpha^s(t^s)$ e t^s è un termine senza variabili (verificare!). Esiste quindi $b \in dom(M)$ con $b = M(t^s)$. Ne segue che $M \models \alpha^s(t^s) \leftrightarrow \alpha^s(b)$, e quindi (2) equivale a:

$$M \models (\forall x\alpha^s(x) \to \alpha^s(b)) \tag{4}$$

La verità di questa ultima asserzione segue dalla semantica di Tarski del $\forall$ applicata alla formula con parametri $\alpha^s(x)$. □

2.8 Espansioni del linguaggio

Definizione 2.39. Dati due linguaggi L ed $L' \supset L$, diciamo che la L'-struttura A è una *espansione* della L-struttura B (o che B è una *restrizione* di A), se A e B hanno lo stesso dominio e interpretano nello stesso modo i simboli di L.

Ad esempio il gruppo $(\mathbb{R}, +, 0)$ è una restrizione del campo $(\mathbb{R}, +, \cdot, 0, 1)$.

Lemma 2.40. *Sia T un insieme di L-enunciati, sia $\phi(x)$ una L-formula e sia c un simbolo di costante non in L. Sono equivalenti:*

1. *$T \models \phi(c)$ (nel linguaggio $L \cup \{c\}$).*
2. *$T \models \forall x\phi(x)$ (nel linguaggio L).*

Dimostrazione. Se $T \not\models \forall x\phi(x)$, allora esiste un modello A di T ed un elemento $a \in A$ con $A \models \neg\phi(a)$. La struttura (A, a) che espande A interpretando c con a è allora un modello di $T \cup \{\neg\phi(c)\}$. □

2.9 Conseguenza logica con variabili libere

Definizione 2.41. Vogliamo estendere la definizione di conseguenza logica $T \models \phi$ al caso in cui le formule di T o di ϕ possano contenere delle variabili libere, che possiamo supporre siano prese da un certo insieme che chiamiamo C. Anziché considerare le formule in questione come formule aperte nel linguaggio L, possiamo considerarle come formule chiuse in un linguaggio espanso $L \cup C$ dove questa volta le C sono pensate come simboli di costante anziché di variabile (supponendo di aver ridenominato se necessario le variabili quantificate in modo da non usare per queste ultime i simboli di C). Definiamo: $T \models \phi$ se ϕ è vera in ogni modello di T, dove per modello di T intendiamo una $L \cup C$-struttura M che rende vere tutte le formule di T.

Esempio 2.42. Sia L un linguaggio con un simbolo di predicato unario P e siano x, y due variabili distinte. Secondo le nostre definizioni si ha

$$P(x) \not\models P(y),$$

ovvero il giudizio $P(x) \models P(y)$ non è valido (cioè esiste una $L \cup \{x, y\}$-struttura in cui $P(x)$ è vera e $P(y)$ è falsa). Altri autori adottano una convenzione diversa secondo la quale il giudizio $P(x) \models P(y)$ ha lo stesso significato di $\forall x P(x) \models \forall y P(y)$, ed è quindi da ritenersi valido. Mentre la nostra convenzione è in accordo con il sistema dimostrativo della deduzione naturale, l'altra è in accordo con il sistema dimostrativo di Hilbert-Frege.

Lemma 2.43. *Se $\Gamma \models \phi$ e t è un termine sostituibile per x in ϕ, allora $\Gamma \models \phi(t/x)$. (Ammettiamo la presenza di variabili libere, anche diverse da x, sia nelle formule di Γ che in ϕ.)*

Dimostrazione. Segue dal Lemma 2.38. □

3 Deduzione naturale

Nella logica proposizionale per verificare che una certa tesi ϕ è conseguenza logica di certe ipotesi Γ (ovvero $\Gamma \models \phi$) possiamo utilizzare le tavole di verità. Nel calcolo dei predicati la relazione di conseguenza logica $\Gamma \models \phi$ è stata invece definita in modo altamente non costruttivo facendo riferimento a tutte le possibile L-strutture. In questa sezione definiremo una relazione $\vdash$ (o più precisamente $\vdash_{DN}$) che risulterà a posteriori equivalente a $\models$ ma che è definita in modo più costruttivo. Il metodo si applica sia alla logica proposizionale che a quella dei predicati. Per semplicità iniziamo con il calcolo proposizionale.

3.1 Caso proposizionale

Nella seguente definizione usiamo il termine "formula" per indicare una formula del calcolo proposizionale in un certo fissato linguaggio.

Definizione 3.1. Le lettere greche minuscole α, β, ϕ denotano delle formule. La lettera greca maiuscola Γ denota un insieme finito di formule. Scriviamo Γ, ϕ per l'insieme $\Gamma \cup \{\phi\}$, cioè l'insieme contenente ϕ e tutte le formule di Γ. A livello intuitivo $\Gamma \vdash \phi$ va letto come "ϕ è dimostrabile a partire da Γ". La barra orizzontale va letta come una implicazione. Le seguenti regole vanno intese come una definizione induttiva di $\vdash$.

- (Ax)$\phi \vdash \phi$

  Dall'ipotesi ϕ posso dedurre ϕ.

- (Wk)$\dfrac{\Gamma \vdash \phi}{\Gamma, \alpha \vdash \phi}$

  Se posso dedurre ϕ da un dato insieme Γ di ipotesi, allora posso dedurlo anche se aggiungo una ulteriore ipotesi[4].

- $(\vdash \wedge)\dfrac{\Gamma \vdash \alpha \qquad \Gamma \vdash \beta}{\Gamma \vdash \alpha \wedge \beta}$

  Se da un dato insieme di ipotesi posso dedurre sia α che β allora posso dedurre $\alpha \wedge \beta$.

- $(\wedge \vdash)\dfrac{\Gamma, \alpha \vdash \gamma}{\Gamma, \alpha \wedge \beta \vdash \gamma} \qquad (\wedge \vdash)\dfrac{\Gamma, \beta \vdash \gamma}{\Gamma, \alpha \wedge \beta \vdash \gamma}$

  Se rimpiazzo una ipotesi (α) con una ipotesi più forte ($\alpha \wedge \beta$) posso continuare a dedurre ciò che deducevo prima (γ).

- $(\vee \vdash)\dfrac{\Gamma \vdash \alpha}{\Gamma \vdash \alpha \vee \beta} \qquad (\vee \vdash)\dfrac{\Gamma \vdash \beta}{\Gamma \vdash \alpha \vee \beta}$

  Se posso dedurre α posso dedurre anche la tesi più debole $\alpha \vee \beta$.

- $(\vdash \vee)\dfrac{\Gamma, \alpha \vdash \gamma \qquad \Gamma, \beta \vdash \gamma}{\Gamma, \alpha \vee \beta \vdash \gamma}$

  Se posso dedurre una certa tesi (γ) sia utilizzando una certa ipotesi (α) che utilizzandone un'altra (β), allora la posso dedurre dalla loro disgiunzione ($\alpha \vee \beta$) (oltre al resto delle ipotesi Γ).

- $(\vdash\rightarrow)\dfrac{\Gamma, \alpha \vdash \beta}{\Gamma \vdash \alpha \rightarrow \beta} \qquad (\rightarrow /e)\dfrac{\Gamma \vdash \alpha \qquad \Gamma \vdash \alpha \rightarrow \beta}{\Gamma \vdash \beta}$

  Per dedurre un'implicazione ($\alpha \rightarrow \beta$) basta riuscire a dedurre β aggiungendo come ulteriore ipotesi α.

  Se posso dedurre sia α che $\alpha \rightarrow \beta$, allora posso dedurre β.

- $(\vdash\perp)\dfrac{\Gamma \vdash \alpha \qquad \Gamma \vdash \neg\alpha}{\Gamma \vdash\perp} \qquad (\perp)\ \dfrac{\Gamma \vdash\perp}{\Gamma \vdash \alpha}$

  Se deduco sia una tesi α che la sua negazione $\neg\alpha$ ho dedotto una contraddizione ($\perp$). Inoltre se deduco una contraddizione, posso dedurre qualsiasi cosa.

- $(\neg \vdash)\dfrac{\Gamma \vdash \alpha}{\Gamma, \neg\alpha \vdash\perp}$

  Se da certe ipotesi posso dedurre α, allora aggiungendo $\neg\alpha$ alle ipotesi ottengo una contraddizione ($\perp$).

$(\vdash \neg)\dfrac{\Gamma, \alpha \vdash\perp}{\Gamma \vdash \neg\alpha}$

Se da certe ipotesi deduco una contraddizione ($\perp$), allora posso dedurre la negazione di una qualsiasi delle ipotesi a partire dalle rimanenti. Alcuni

[4] Qui la logica matematica si discosta dal buon senso comune, dove può capitare che ulteriori informazioni portino a rivedere le conclusioni precedentemente acquisite.

autori definiscono $\neg A$ come $A \to \perp$. Così facendo la regola appena data diventa ridondante in quanto si ottiene da $\vdash \to$ prendendo $\beta = \perp$.

- (RAA) $\dfrac{\Gamma, \neg\alpha \vdash \perp}{\Gamma \vdash \alpha}$

Per dimostrare α da certe ipotesi Γ è sufficiente riuscire a dedurre una contraddizione aggiungendo $\neg\alpha$ alle ipotesi. Questa è la regola delle dimostrazioni per assurdo (RAA = reductio ad absurdum), e come vedremo essa è alla base delle dimostrazioni non costruttive.

Definizione 3.2. Diciamo che il giudizio $\Gamma \vdash \phi$ è derivabile, se è possibile ottenerlo con un numero finito di applicazioni delle regole date a partire da giudizi della forma $\phi \vdash \phi$ (Ax). Detto ancora in altri termini, $\Gamma \vdash \phi$ è derivabile se appartiene alla più piccola classe di giudizi che contiene tutti o in della forma (Ax) e che è chiuso per applicazione delle regole (quest'ultima condizione significa che se i giudizi al di sopra della barra orizzontale di una regola sono derivabili lo è anche, per definizione, quello al di sotto).

Se T è una teoria, possibilmente con un numero infinito di assiomi, e ϕ è un L-enunciato, diremo che ϕ è **dimostrabile** in T (nel sistema della deduzione naturale), se esiste un sottoinsieme finito Γ degli assiomi di T tale che il giudizio $\Gamma \vdash \phi$ è derivabile usando le regole sopra date. Se ϕ è dimostrabile in T diremo che ϕ è un **teorema** di T, e scriveremo $T \vdash \phi$ per esprimere questo fatto.

Esempio 3.3. $A \wedge B \vdash A \vee B$ è derivabile dalle regole della deduzione naturale. Infatti da A deduco $A \vee B$ in base alla regola ($\vdash \vee$). Quindi da $A \wedge B$ deduco $A \vee B$ in base alla regola ($\wedge \vdash$).

La differenza tra le regole (RAA) e ($\vdash\perp$) potrebbe sembrare irrilevante se si da per scontato che $\neg\neg A$ equivale ad A, ma quest'ultima equivalenza richiede per essere dimostrata proprio la regola RAA. Ovviamente l'equivalenza tra $\neg\neg A$ e A segue anche dalle tavole di verità, ma lo scopo del sistema della deduzione naturale è per l'appunto quello di fornire un approccio alternativo rispetto alle tavole di verità, che quindi non possono essere utilizzate in questo contesto.

Esempio 3.4. Mostriamo che $\neg\neg A \vdash A$ è derivabile. Per RAA basta far vedere che $\neg\neg A, \neg A \vdash \perp$ è derivabile. Questo è facile perché da $\neg\neg A, \neg A$ deduco sia $\neg A$ che la sua negazione $\neg\neg A$, e quindi per ($\vdash\perp$) deduco $\perp$.

Un esempio più complicato dove si utilizza RAA è il seguente.

Esempio 3.5. Verifichiamo che $\vdash A \vee \neg A$ è derivabile (dove a sinistra del $\vdash$ abbiamo l'insieme vuoto). La difficoltà sta nel fatto che potremmo non essere in grado di dimostrare nessuno dei due disjunti singolarmente presi (cioè nè $\vdash A$ nè $\vdash \neg A$ sono derivabili). Ragioniamo allora per assurdo, cioè cerchiamo di dimostrare $\neg(A \vee \neg A) \vdash \perp$ (per poi concludere applicando RAA). Per la regola ($\vdash\perp$), basta riuscire a derivare (1) $\neg(A \vee \neg A) \vdash A$ e (2) $\neg(A \vee \neg A) \vdash \neg A$. Sempre ragionando per assurdo (cioè utilizzando la RAA), per derivare (1) basta derivare $\neg(A \vee \neg A), \neg A \vdash \perp$. Questo è facile perché da $\neg A$ deduco $A \vee \neg A$ che insieme all'altra ipotesi $\neg(A \vee \neg A)$ conduce a $\perp$. (Più formalmente: $\neg A \vdash \neg A$ per (Ax), quindi $\neg A \vdash A \vee \neg A$ per ($\perp \vee$), quindi $\neg(A \vee \neg A), \neg A \vdash A \vee \neg A$ per (Wk). Ma siccome ho anche $\neg(A \vee \neg A), \neg A \vdash \neg(A \vee \neg A)$ per (Ax) e (Wk), ne concludo $\neg(A \vee \neg A), \neg A \vdash \perp$.) Per (2) ragioniamo analogamente: dall'ipotesi A deduco $A \vee \neg A$, e aggiungendo $\neg(A \vee \neg A)$ alle ipotesi ottengo $\perp$. Quindi per ($\vdash \perp$) ottengo $\neg(A \vee \neg A) \vdash \neg A$.

3.2 Caso predicativo

Analogamente a quanto fatto nel caso proposizionale definiremo una relazione $\vdash_{DN}$ che, come poi vedremo, risulterà equivalente a $\models$.

Definizione 3.6. Sia L un linguaggio del primo ordine. Considereremo **giudizi** della forma $\Gamma \vdash \phi$ dove Γ è un insieme finito di L-formule e ϕ è una L-formula chiusa. Un giudizio è derivabile se si può ottenere in base alle seguenti regole.

- Tutte le regole già date nel caso proposizionale, applicate però a formule del primo ordine del linguaggio L anziché a formule proposizionali.

- $(\vdash \forall)\dfrac{\Gamma \vdash \phi(y/x)}{\Gamma \vdash \forall x\phi}$ dove y è una variabile che non occorre libera nelle formule di $\Gamma \cup \{\phi\}$.

  L'idea è che per dimostrare $\forall x\phi$ basta dimostrare $\phi(y/x)$ per un elemento generico y, ovvero per una variabile y su cui non sono state fatte ipotesi.

- $(\forall/e)\dfrac{\Gamma \vdash \forall x\phi}{\Gamma \vdash \phi(t/x)}$ dove t è un qualsiasi termine sostituibile per x in ϕ.

  Dal generale al particolare: se dimostro che $\phi(x)$ vale per ogni x, allora vale anche per t.

- $(\vdash \exists)\dfrac{\Gamma \vdash \phi(t/x)}{\Gamma \vdash \exists x\phi}$ dove t è un qualsiasi termine sostituibile per x in ϕ.

  Si tratta del metodo delle dimostrazioni costruttive di esistenza: per dimostrare che esiste un x tale che $\phi(x)$ basta esibire un t per il quale si sa dimostrare $\phi(t)$.

- $(\exists \vdash)\dfrac{\Gamma, \phi(y/x) \vdash \gamma}{\Gamma, \exists x\phi \vdash \gamma}$ dove y è una variabile che non occorre libera in Γ o in γ.

  Questa è la regola più difficile da giustificare a livello intuitivo. L'idea è la seguente. Supponiamo di voler dimostrare γ a partire da $\exists x\phi(x)$. A livello informale un modo comune di procedere è il seguente. Visto che vale $\exists x\phi(x)$ possiamo immaginare di scegliere un elemento y che verifica $\phi(y)$ (nelle dimostrazioni informali questo passsaggio è accompagnato in genere da commenti come "sappiamo che $\exists x\phi(x)$. Sia dunque y un tale x") e proseguire poi la dimostrazione cercando di dedurre γ da $\phi(y)$. Se ci riusciamo possiamo affermare di aver dimostrato γ da $\exists x\phi(x)$. È importante che y sia una variabile non usata in precedenza, perché in genere potremmo non sapere se la x di cui si asserisce l'esistenza coincida con uno degli elementi nominati in precedenza nella dimostrazione.

- $(\vdash=)\Gamma \vdash t = t$, dove t è un termine qualsiasi.

- $(=/e)\dfrac{\Gamma \vdash \phi(t/x) \qquad \Gamma \vdash t = t'}{\Gamma \vdash \phi(t'/x)}$, dove t, t' sono termini sostituibili per x in ϕ.

  La regola dice che se $t = t'$, tutto ciò che posso affermare di t lo posso affermare di t'.

Esempio 3.7. La regola (RAA), in combinazione con le regole per i quantificatori, viene usata in modo essenziale nella dimostrazione che $\neg\forall xP(x) \rightarrow \exists x\neg P(x)$. L'idea della dimostrazione è la seguente (saltando qualche passaggio). Abbiamo $\neg P(a) \vdash \exists x\neg P(x)$. Aggiungendo $\neg\exists x\neg P(x)$ alle ipotesi otteniamo allora facilmente $\neg\exists x\neg P(x), \neg P(a) \vdash\perp$. Quindi per (RAA) $\neg\exists x\neg P(x) \vdash P(a)$. Ora la a non compare più tra le ipotesi e può pertanto essere quantificata universalmente: $\neg\exists x\neg P(x) \vdash \forall xP(x)$. Ma allora se aggiungo $\neg\forall xP(x)$ alle ipotesi ottengo una contraddizione: $\neg\forall xP(x), \neg\exists x\neg P(x) \vdash\perp$. Utilizzando di nuovo (RAA) otteniamo $\neg\forall xP(x) \vdash \exists x\neg P(x)$. Infine scaricando l'ipotesi $\vdash \neg\forall xP(x) \rightarrow \exists x\neg P(x)$.

L'implicazione $\vdash \neg\forall xP(x) \rightarrow \exists x\neg P(x)$ è a sua volta alla base di molte dimostrazioni non costruttive in matematica, come ad esempio quella del teorema che ogni successione infinita di numeri reali nell'intervallo $[0, 1]$ ha un punto di accumulazione.

3.3 Correttezza della deduzione naturale

Il collegamento tra le regole della deduzione naturale e le interpretazioni (sia nel caso proposizionale che predicativo) è il seguente:

Definizione 3.8. Una regola di inferenza è **corretta** se, rimpiazzando nella regola $\models$ al posto di $\vdash$, il giudizio al di sotto della barra verticale è valido ogniqualvolta lo sono quelli al di sopra della barra.

Esempio 3.9. Verifichiamo ad esempio la correttezza della regola

$$(\vdash\rightarrow)\frac{\Gamma, \alpha \vdash \beta}{\Gamma \vdash \alpha \rightarrow \beta}$$

A tal fine dobbiamo mostrare che, comunque si scelgano le formule in questione, si ha:

$$\text{Se } \Gamma, \alpha \models \beta, \text{ allora } \Gamma \models \alpha \rightarrow \beta.$$

Assumiamo dunque che valga $\Gamma, \alpha \models \beta$. Dato un modello M di Γ dobbiamo allora verificare che esso rende vera $\alpha \rightarrow \beta$. Questo è chiaro se α è falsa in M, perché una implicazione con la premessa falsa è vera. Se invece α è vera in M, allora M è un modello di Γ, α, e siccome stiamo supponendo che $\Gamma, \alpha \models \beta$, nel modello M deve essere vera β, e quindi anche $\alpha \rightarrow \beta$ in base alle tavole di verità.

Osservazione 3.10. La dimostrazione appena data funziona è valida sia nel caso proposizionale che predicativo. Nel primo caso le formule sono formule proposizionali e M è una valutazione booleana, nel secondo caso le formule sono formule di un linguaggio del primo ordine L ed M è una $L \cup C$-struttura, dove C è l'insieme delle variabili libere presenti (si veda la definizione 2.41).

Osservazione 3.11. Il lettore avrà forse notato che per dimostrare la correttezza della regola ($\vdash\rightarrow$) abbiamo usato nella "metateoria" lo stesso tipo di ragionamento espresso formalmente dalla regola stessa. Nessun dramma: non stiamo cercando di spiegare quali siano i ragionamenti corretti, ma solo di rappresentarli formalmente, presupponendo naturalmente che tutti si sappia già ragionare a livello informale.

Lemma 3.12. *Le regole* ($\vdash \forall$) *e* ($\vdash /e$) *sono corrette.*

Dimostrazione. La correttezza della prima regola segue immediatamente dal Lemma 2.40. La seconda dal Lemma 2.43. □

Similmente si dimostra:

Lemma 3.13. *Tutte le regole della deduzione naturale sono corrette.*

Dimostrazione. Lasciato al lettore come esercizio. □

Ne segue immediatamente (per induzione sul numero delle regole applicate) che:

Teorema 3.14. *Sia* Γ *un insieme di formule e sia* ϕ *una formula. Se* $\Gamma \vdash_{DN} \phi$, *allora* $\Gamma \models \phi$, *dove* $\Gamma \models \phi$ *significa che* ϕ *è vera in tutti i modelli di* Γ *e* $\Gamma \vdash_{DN} \phi$ *significa che* $\Gamma \vdash \phi$ *è derivabile dalle regole della deduzione naturale.*

Molto più difficile dimostrare che se $\Gamma \models \phi$ allora $\Gamma \vdash_{DN} \phi$. Ciò esprime esprime la completezza delle regole della deduzione naturale, e ne posponiamo la dimostrazione.

4 Completezza

4.1 Caso proposizionale

Sebbene in questa sezione siamo interessati alla logica proposizionale, osserviamo che i risultati e le definizioni di questa sezione si applicano (con minime modifiche) sia al caso proposizionale che predicativo.

Definizione 4.1. Una teoria Γ si dice **incoerente** (o **contraddittoria**) se $\Gamma \vdash \perp$. Diciamo che Γ è **coerente** se non è incoerente.

Esercizio 4.2. Sono equivalenti:

1. $\Gamma \vdash \perp$;

2. Esiste una formula θ tale che $\Gamma \vdash \theta$ e $\Gamma \vdash \neg\theta$;

3. Per ogni formula φ, $\Gamma \vdash \varphi$.

Lemma 4.3. *Sia Γ una teoria e ϕ una formula. Se Γ è coerente, allora almeno una delle due teorie Γ, ϕ o $\Gamma, \neg\phi$ è coerente.*

Dimostrazione. Supponiamo che le teorie $\Gamma \cup \{\neg\phi\}$ e $\Gamma \cup \{\neg\phi\}$ siano entrambe incoerenti. Poichè $\Gamma \cup \{\neg\phi\}$ è incoerente abbiamo $\Gamma \vdash \phi$. Similmente dall'incoerenza di $\Gamma \cup \{\phi\}$ otteniamo $\Gamma \vdash \neg\phi$. Mettendo insieme le due dimostrazioni otteniamo $\Gamma \vdash \perp$. $\square$

Definizione 4.4. Una L-teoria coerente Γ si dice *completa* se data una L-formula ϕ o $\Gamma \vdash \phi$ o $\Gamma \vdash \neg\phi$.

Definizione 4.5. Fissato un linguaggio (proposizionale o predicativo) L, una L-teoria Γ si dice **coerente massimale** se è coerente e non è propriamente inclusa in alcun'altra L-teoria coerente.

Osservazione 4.6. Supponiamo che Γ sia coerente massimale e $\Gamma \vdash \phi$. Allora $\phi \in \Gamma$.

Dimostrazione. Se $\phi \notin \Gamma$ allora $\Gamma \cup \{\neg\phi\}$ è una estensione propria di Γ ed è pertanto incoerente. Ma siccome $\Gamma \vdash \phi$, Γ e $\Gamma \cup \{\phi\}$ hanno gli stessi teoremi, e pertanto anche Γ sarebbe incoerente. $\square$

Lemma 4.7. *Sono equivalenti:*

1. *Γ è coerente massimale;*

2. *Γ è coerente e per ogni formula ϕ, $\phi \in \Gamma$ oppure $\neg\phi \in \Gamma$.*

Dimostrazione. $1 \to 2$. Supponiamo che $\phi \notin \Gamma$ e $\neg\phi \notin \Gamma$. Allora entrambe le teorie $\Gamma \cup \{\theta\}$ e $\Gamma \cup \{\neg\theta\}$ estendono propriamente Γ. Ma per il Lemma 4.3 una di queste due teorie è coerente, contraddicendo la massimalià di Γ.

$2 \to 1$. Assumendo (2) dobbiamo mostrare che Γ non è estendibile ad una teoria coerente $\Delta \supset \Gamma$. Infatti se $\phi \in \Delta \setminus \Gamma$, per (2) abbiamo $\neg\phi \in \Gamma$. Ma allora Δ conterrebbe sia ϕ che $\neg\phi$ e pertanto non sarebbe coerente. $\square$

Lemma 4.8. *Consideriamo una famiglia $\{T_i \mid i \in I\}$ di L-teorie che formano una catena, cioè per ogni $i, j \in I$ $T_i \subset T_j$ o $T_j \subset T_i$. Sia $\bigcup_{i \in I} T_i$ l'unione della catena. Supponiamo che $\bigcup_{i \in I} T_i \vdash \varphi$. Allora esiste $i \in I$ tale che $T_i \vdash \varphi$.*

Dimostrazione. Gli assiomi effettivamente utilizzati in una dimostrazione formale sono sempre in numero finito. Esiste quindi un sottoinsieme finito $S \subset \bigcup_i T_i$ tale che $S \vdash \varphi$. D'altra parte sicuramente esiste i tale che S è incluso in una delle T_i (qui si usa l'ipotesi che le T_i formino una catena). Quindi $T_i \vdash \phi$. □

Corollario 4.9. *L'unione di una catena di teorie coerenti è coerente.*

Lemma 4.10. *(Lemma di Lindenbaum) Ogni L-teoria coerente Γ è contenuta in una L-teoria coerente massimale.*

Dimostrazione. Per semplicità consideriamo dapprima il caso in cui L sia numerabile. Possiamo allora fissare una enumerazione $\{\phi_n \mid n \in \mathbb{N}\}$ dell'insieme delle L-formule. Sia $T_0 = \Gamma$ e induttivamente definiamo T_{n+1} come $T_n \cup \{\phi_n\}$ se questa teoria è coerente, e come $T_n \cup \{\neg\phi_n\}$ nel caso contrario. Per il lemma 4.3 T_{n+1} è coerente se T_n lo è. Quindi per induzione tutte le T_n sono coerenti e per il corollario precedente lo è la loro unione $T' = \bigcup_{n\in\mathbb{N}} T_n$. Data una qualsiasi formula $\theta \in \{\phi_n \mid n \in \mathbb{N}\}$, T' deve contenere una delle due formule θ o $\neg\theta$ (se $\theta = \phi_n$, o θ o la sua negazione appartiene a T_{n+1}). Quindi per il Lemma 4.7 T' è coerente massimale.

Il caso in cui L non è numerabile si dimostra applicando il lemma di Zorn all'insieme di tutte le L-teorie coerenti contenenti Γ ordinate per inclusione. Le ipotesi del lemma di Zorn sono verificate grazie al Corollario 4.9. □

Lemma 4.11. *Sia T una L-teoria coerente (rispetto alle regole della deduzione naturale).*

1. *se $\neg\neg\phi \in T$, allora T, ϕ è coerente (quindi se T è coerente massimale, $\phi \in T$).*
2. *se $\phi \wedge \psi \in T$, allora T, ϕ, ψ è coerente (quindi se T è coerente massimale, $\phi \in T$ e $\psi \in T$).*
3. *se $\neg(\phi \wedge \psi) \in T$, allora $T, \neg\phi$ è coerente, o $T, \neg\psi$ è coerente (quindi se T è coerente massimale, $\neg\phi \in T$ o $\neg\psi \in T$);*
4. *se $\phi \vee \psi \in T$, allora T, ϕ è coerente, o T, ψ è coerente (quindi se T è coerente massimale, $\phi \in T$ o $\psi \in T$).*
5. *se $\neg(\phi \vee \psi) \in T$, allora $T, \neg\phi, \neg\psi$ è coerente (quindi se T è coerente massimale, $\neg\phi \in T$ e $\neg\psi \in T$).*
6. *se $\phi \to \psi \in T$, allora $T, \neg\phi$ è coerente, o T, ψ è coerente (quindi se T è coerente massimale, $\neg\phi \in T$ o $\psi \in T$).*

Teorema 4.12. *Sia L un linguaggio proposizionale e sia T una teoria proposizionale coerente nel linguaggio L. Allora T ha un modello proposizionale.*

Dimostrazione. Per il lemma di Lindenbaum esiste una L-teoria coerente massimale $T' \supset T$. In particolare per ogni variabile proposizionale A di L, $A \in T'$ o $\neg A \in T'$. Sia M la valutazione booleana che assegna **1** alle variabili A che appartengono a T' e **0** alle variabili la cui negazione appartiene a T'. Per la coerenza di T ogni variabile riceve da M un solo valore, e per la massimalità di T nessuna variabile del linguaggio L rimane esclusa. Usando le tavole di verità ogni formula di L (non solo le variabili proposizionali) riceve da M un valore **1** o **0**. Per induzione sulla complessità delle formule, e usando il Lemma 4.11 per fare i passaggi induttivi, si verifica che ogni formula di T' riceve il valore **1** da M. Quindi M è un modello di T', e pertanto anche di T. $\square$

Teorema 4.13. *Sia T una teoria proposizionale, e sia ϕ una formula proposizionale. Se $T \models \phi$ allora $T \vdash \phi$.*

Dimostrazione. Supponiamo che $T \nvdash \phi$. Allora $T, \neg\phi$ è coerente. Quindi $T, \neg\phi$ ha un modello M. Tale modello testimonia il fatto che $T \not\models \phi$. $\square$

4.2 Caso Predicativo

Esattamente come nel caso proposizionale si dimostra:

Lemma 4.14. *Sia Γ una teoria e ϕ una formula chiusa. Se Γ è coerente, allora almeno una delle due teorie Γ, ϕ o $\Gamma, \neg\phi$ è coerente.*

Corollario 4.15. *L'unione di una catena di teorie coerenti è coerente.*

Lemma 4.16. *(Lemma di Lindenbaum) Ogni L-teoria coerente Γ è contenuta in una L-teoria coerente massimale.*

Lemma 4.17. *Sia Σ un insieme di L-enunciati, sia $\exists x\phi(x)$ un L-enunciato e sia c sia un simbolo di costante non occorrente nè in Σ nè in $\exists x\phi(x)$. Allora $\Sigma \cup \{\phi(c)\}$ è coerente se e solo se $\Sigma \cup \{\exists x\phi(x)\}$ è coerente.*

Dimostrazione. Poiché $\Sigma \vdash \phi(c) \to \exists x\phi(x)$, se $\Sigma \cup \{\phi(c)\}$ è coerente allora $\Sigma \cup \{\exists x\phi(x)\}$ è coerente. Viceversa supponiamo che $\Sigma \cup \{\phi(c)\}$ sia incoerente, ovvero $\Sigma \cup \{\phi(c)\} \vdash \perp$. Rimpiazzando c con una nuova variabile y che non compare nella dimostrazione, $\Sigma \cup \{\phi(y)\} \vdash \perp$ (verificare!). Ma allora per una delle regole della deduzione naturale, $\Sigma \cup \{\exists x\phi(x)\} \vdash \perp$. $\square$

Lemma 4.18. *Sia Σ un insieme coerente di L-enunciati, sia $\exists x\phi(x)$ un L-enunciato e sia c sia un simbolo di costante non occorrente nè in Σ nè in $\exists x\phi(x)$. Allora $\Sigma \cup \{\exists x\phi(x) \to \phi(c)\}$ è coerente.*

Dimostrazione. Supponiamo che $\Sigma \cup \{\exists x\phi(x) \to \phi(c)\} \vdash \perp$. Ma allora è facile vedere che $\Sigma \vdash \{\exists x\phi(x)\}$ e $\Sigma \vdash \neg\phi(c)$. Questo contraddice il Lemma 4.17. $\square$

Definizione 4.19. Sia T una L-teoria. Diciamo che T è una **teoria di Henkin** se per ogni L-enunciato della forma $\exists x\phi(x)$ esiste almeno un simbolo di costante c in L tale che la formula $\exists x\phi(x) \to \phi(c)$ è dimostrabile in T. (Quindi se $\exists x\phi(x)$ è dimostrabile in T anche $\phi(c)$ lo è.)

Esempio 4.20. Sia T la teoria nel linguaggio $L = \{0, 1, +, \cdot\}$ che ha come assiomi tutti gli L-enunciati veri nel campo dei numeri reali $\mathbb{R}$ (interpretando i simboli di L come lo zero, l'uno, la somma e il prodotto). Allora T non è una teoria di Henkin. Infatti T dimostra $\exists x(x^2 = 2)$ (dove x^2 sta per $x \cdot x$ e 2 sta per $1 + 1$) ma non esiste alcuna costante c del linguaggio tale che $T \vdash c^2 = 2$. (La radice quadrata di due esiste nel dominio della struttura $\mathbb{R}$, ma non corrisponde ad alcun simbolo del linguaggio L).

Lemma 4.21. *Sia T una L-teoria coerente. Allora esiste un linguaggio $L' \supset L$ e una L'-teoria $T' \supset T$ tale che T' è coerente e di Henkin.*

Dimostrazione. Definiamo una operazione tra teorie $T \mapsto T^*$ nel modo seguente. Sia L^* il linguaggio che si ottiene da $L = L(T)$ con l'aggiunta, per ogni enunciato di L della forma $\exists x\alpha$, di una corrispondente nuova costante che indicheremo c_α (distinti enunciati corrispondendo a distinte costanti). Sia T^* la teoria nel linguaggio L^* i cui assiomi comprendono quelli di T e tutti gli enunciati della forma $\exists x\alpha(x) \to \alpha(c_\alpha)$ dove $\exists x\alpha(x)$ è un enunciato di L.

Usando ripetutamente il Lemma 4.18 si dimostra che qualsiasi sottoteoria finita di T^* è coerente, quindi anche T^* è coerente (in quanto una eventuale dimostrazione di una contraddizione può coinvolgere solo un numero finito di assiomi).

Si noti che T^* non è necessariamente una teoria di Henkin perchè, pur essendo vero che tutti gli $\exists$-enunciati di $L(T)$ hanno una costante associata, cio' non è necessariamente vero per tutti gli $\exists$-enunciati di $L(T^*)$. Per porre rimedio a ciò dobbiamo iterare il procedimento $T \mapsto T^*$ infinite volte come segue.

Sia $T_0 = T, T_{n+1} = T_n^*$. Sia T_ω l'unione delle teorie T_n per $n \in \omega$. Poichè tutte le T_n sono coerenti lo è anche T_ω per il Lemma 4.15.

Per finire verifichiamo che T_ω è una teoria di Henkin. Sia infatti $\exists x\alpha(x)$ un enunciato di $L(T_\omega)$. Poichè $\exists x\alpha(x)$ puo' contenere solo un numero finito delle nuove costanti, esiste $n \in \omega$ tale che $\exists x\alpha(x)$ è un enunciato di $L(T_n)$. Ma allora $\exists x\alpha(x) \to \alpha(c_\alpha)$ è un assioma di T_{n+1} e quindi di T_ω. □

Lemma 4.22. *Sia Σ un insieme coerente di L-enunciati. Allora esiste un linguaggio $L' \supset L$ e un insieme di L'-enunciati $\Sigma' \supset \Sigma$ tale che Σ' è coerente massimale e di Henkin.*

Dimostrazione. Prima applichiamo il Lemma 4.21 per trovare una estensione di Henkin $T \supset \Sigma$ in un linguaggio esteso $L' \supset L$, poi il Lemma 4.16 per estendere la teoria di Henkin ad una teoria coerente massimale $\Sigma' \supset T$ sempre nel linguaggio L'. Visto che nel secondo passaggio non abbiamo cambiato il linguaggio, Σ' continua ad essere di Henkin. □

Definizione 4.23. (Insiemi di Hintikka) Sia T un insieme di L-formule chiuse. Diciamo che T è un insieme di Hintikka (per L) se per ogni scelta di L-formule chiuse ϕ, ψ si ha:

1. se $\phi \in T$, allora $\neg\phi \notin T$,

2. se $\neg\neg\phi \in T$, allora $\phi \in T$,
3. se $\phi \wedge \psi \in T$, allora $\phi \in T$ e $\psi \in T$,
4. se $\neg(\phi \wedge \psi) \in T$, allora $\neg\phi \in T$ o $\neg\psi \in T$,
5. se $\phi \vee \psi \in T$, allora $\phi \in T$ o $\psi \in T$,
6. se $\neg(\phi \vee \psi) \in T$, allora $\neg\phi \in T$ e $\neg\psi \in T$,
7. se $\phi \to \psi \in T$, allora $\neg\phi \in T$ o $\psi \in T$,
8. se $\neg(\phi \to \psi) \in T$, allora $\phi \in T$ e $\neg\psi \in T$,
9. se $\forall x\phi(x) \in T$, allora per ogni L-termine chiuso t, $\phi(t) \in T$,
10. se $\neg\forall x\phi(x) \in T$, allora esiste un L-termine chiuso t tale che $\neg\phi(t) \in T$,
11. se $\exists x\phi(x) \in T$, allora esiste un L-termine chiuso t, tale che $\phi(t) \in T$,
12. se $\neg\exists x\phi(x) \in T$, allora per ogni L-termine chiuso t, $\neg\phi(t) \in T$.
13. (riflessività) per ogni L-termine chiuso t, $t = t \in T$,
14. (sostituibilità) per ogni L-formula $\phi(x)$ e termini chiusi t e t', se $t = t' \in T$, allora $\phi(t) \in T$ se e solo se $\phi(t') \in T$.

(Nella ultima clausola possiamo anche limitarci a formule atomiche $\phi(x)$.)

Esercizio 4.24. Si consideri un linguaggio senza simbolo di uguaglianza nella segnatura $L = \{R, c\}$, dove R è un simbolo di relazione binario e c è un simbolo di costante. Si trovi un insieme di Hintikka contenente la formula $\forall x\exists y(R(x,y) \vee R(y,x))$.

Lemma 4.25. *Sia T una L-teoria coerente massimale di Henkin. Allora T è di Hintikka.*

Dimostrazione. Verifichiamo ad esempio la clausola del $\vee$ nella definizione di insieme di Hintikka. Supponiamo che $\alpha \vee \beta \in \Sigma'$. Allora per il Lemma 4.11 $\Sigma' \cup \{\alpha\}$ è coerente, o $\Sigma' \cup \{\beta\}$ è coerente. Supponiamo senza perdita di generalità che $\Sigma' \cup \{\alpha\}$ sia coerente. Essendo Σ' coerente massimale, si deve allora avere $\alpha \in \Sigma'$. Gli altri casi sono analoghi e lasciati al lettore come esercizio. $\square$

Teorema 4.26. *Ogni insieme di Hintikka T ha un modello M. Inoltre possiamo prendere M in modo tale che ogni elemento del dominio di M è l'interpretazione di un termine chiuso del linguaggio L di T.*

Dimostrazione. Per semplicità consideriamo prima il caso di linguaggi senza il simbolo di uguaglianza né simboli di funzione. In questo caso gli unici termini chiusi di L sono le costanti. Prendiamo come $dom(M)$ l'insieme delle costanti di L. Dato un simbolo di relazione R di arietà n, definiamo la sua interpretazione $R^M \subseteq dom(M)^n$ come l'insieme di tutte le n-uple $(c_1, \ldots, c_k)$ tali che

$R(c_1, \dots, c_n) \in T$. In questo modo abbiamo definito una L-struttura che rende veri tutti gli enunciati atomici in T, e falsi gli enunciati atomici non in T. Sia ora ϕ un arbitrario L-enunciato. Usando le proprietà di Hintikka segue per induzione sul numero dei connettivi di ϕ che se $\phi \in T$, allora $M \models \phi$ (se T è un insieme di Hintikka completo sarà anche vero che se $\phi \notin T$, allora $M \models \neg\phi$).

Consideriamo ad esempio il caso $\neg\phi \in T$. Dalle proprietà di Hintikka segue che $\phi \notin T$. Se ϕ è atomica, concludiamo che $M \models \neg\phi$ per definizione di M. Se invece ϕ non è atomica, allora deve cominciare con un connettivo. Supponiamo ad esempio che tale connettivo sia $\vee$, cioè $\neg\phi = \neg(\alpha \vee \beta)$. Usando le proprietà di Hintikka abbiamo $\neg\alpha \in T$ e $\neg\beta \in T$. Per induzione possiamo concludere $M \models \neg\alpha$ e $M \models \neg\beta$, da cui poi segue $M \models \neg(\alpha \vee \beta)$.

Lasciamo al lettore la verifica degli altri casi. Questo conclude la dimostrazione nel caso il linguaggio non abbia simboli di funzione e il simbolo di uguaglianza.

Consideriamo ora il caso generale. Ricordiamo che il simbolo di uguaglianza deve essere interpretato come la relazione di uguaglianza, quindi se $t = t' \in T$ dobbiamo fare in modo che t e t' siano interpretati con lo stesso elemento del modello M che vogliamo costruire.

A tal fine prendiamo come $dom(M)$ l'insieme degli L-termini chiusi quozientato rispetto alla relazione di equivalenza $\sim$ definita da $t \sim t'$ sse $t = t' \in T$. Segue dalle proprietà degli insiemi di Hintikka che $\sim$ è in effetti una relazione di equivalenza. Indichiamo con $t/\sim$ la classe di equivalenza di t rispetto a $\sim$.

Dato un simbolo di funzione f di L di arietà n definiamo la sua interpretazione $f^M \colon dom(M)^n \to dom(M)$ ponendo: $f^M(t_1/\sim, \dots, t_n/\sim) = f(t_1, \dots, t_n)/\sim$. Questa definizione è ben posta perchè dalla clausola di sostituibilità nella definizione degli insiemi di Hintikka (applicata ripetute volte) segue che se $t_1 \sim t'_1, \dots, t_n \sim t'_n$ allora $f(t_1, \dots, t_n) \sim f(t'_1, \dots, t'_n)$.

Resta solo da definire l'interpretazione R^M dei simboli di relazione di L (se ve ne sono). Se R ha arietà n e $t_1, \dots, t_n$ sono termini chiusi, poniamo $(t_1/\sim, \dots, t_n/\sim) \in R^M$ sse $R(t_1, \dots, t_n) \in T$. Questo è ben posto per la clausola di sostituibilità. Abbiamo così definito una L-struttura M.

Per induzione sulla lunghezza dei termini chiusi t, segue che $t^M = t/\sim$. Quindi se $t = t' \in T$, allora $t^M = t/\sim = t'/\sim = t'^M$, e quindi $M \models t = t'$ (si noti che per abuso di linguaggio abbiamo usato "=" sia come simbolo che come la vera relazione di uguaglianza). Viceversa se $t = t' \notin T$, allora $t/\sim \neq t'/\sim$ e $M \models t \neq t'$. Quindi M rende veri gli enunciati di T della forma $t = t'$, e falsi gli enunciati della forma $t = t'$ che non sono in T. Similmente si verifica che $R(t_1, \dots, t_n) \in T$ sse $M \models R(t_1, \dots, t_n)$. Quindi tra gli enunciati atomici (senza connettivi) M rende veri tutti e soli quelli che sono in T. Ragionando per induzione sulla complessità della formula, usando le proprietà di Hintitkka per i passi induttivi, vediamo che ogni $\phi \in T$ (non necessariamente atomica) è vera M. Consideriamo nel dettaglio il caso in cui ϕ è della forma $\exists x\theta(x)$. Se $\phi \in T$, allora essendo T di Hintikka deve esistere un termine chiuso t tale che $\theta(t) \in T$. Per induzione $\theta(t)$ è vero nel modello M. Ma allora deve essere vero anche $\exists x\theta(x)$. $\square$

Teorema 4.27. *Sia T una L-teoria. Se T è coerente allora T ha un modello.*

Dimostrazione. Se T è coerente esiste un insieme di Hintikka $T' \supset T$ in un linguaggio $L' \supset L$. Per il Teorema 4.26 T' ha un modello. Quindi anche T ha un modello. $\square$

Teorema 4.28. *Sia T una L-teoria. Se $T \models \phi$, allora $T \vdash \phi$ (nel sistema della deduzione naturale).*

Dimostrazione. Se $T \nvdash \phi$ allora $T, \neg\phi$ è coerente, e quindi ha un modello. Tale modello testimonia che $T \not\models \phi$. $\square$