Calcolo dei predicati

Alessandro Berarducci

20 Nov. 2017

Indice

1 Logica proposizionale

1.1 Connettivi e tavole di verità

Una **proposizione** è ciò che viene espresso da un enunciato del quale abbia senso chiedersi (o ipotizzare), nel dato contesto o nelle date circostanze, se esso sia vero o falso. Assumeremo che una proposizione non può essere sia vera che falsa, ed è o vera o falsa.

Definizione 1.1. 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 $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$. La loro traduzione approssimativa in italiano è la seguente:

"$\neg A$" significa "non A" (negazione),
"$A \wedge B$" significa "A e B" (congiunzione),
"$A \vee B$" significa "A o B" (disgiunzione),
"$A \rightarrow B$" significa "se A, allora B" (implicazione),
"$A \leftrightarrow B$" significa "A se e solo se B" (doppia implicazione).

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 1.2. Ad una proposizione A 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. 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 una delle proposizioni A e B è vera, senza escludere la possibilità che entrambe siano vere. 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:

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

Veniamo all'implicazione. 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 1.3. L'implicazione "x è dispari $\to x^2$ è dispari " è vera per ogni valore di x. Ad esempio se $x = 3$ essa è vera in quanto sia la premessa (3 è dispari) sia la conclusione (9 è dispari) sono vere, mentre se $x = 2$ è ugualmente vera, perché la premessa 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 fosse invece falsa, l'implicazione sarebbe comunque 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 nella logica classica 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 $\neg A \vee B$.

Nota 1.4. (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 1.5. 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 1.6. 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 un'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 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 1.7. 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).

Nota 1.8. 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 vi 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. 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 1.9. 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 1.10. 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 $(\alpha_1 \wedge \dots \wedge \alpha_n) \to \beta$ è una tautologia, ovvero se in tutti i casi in cui tutte le α_i sono vere, anche β è vera. Scriviamo

$$\alpha_1, \dots, \alpha_n \models \beta$$

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 1.11. $A \wedge (B \vee C)$ 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 $\neg A \wedge \neg B$.

Nota 1.12. Si noti la differenza tra implicazione materiale ($\to$) e conseguenza logica ($\models$). Secondo la tavola di verità dell'implicazione, date due *proposizioni* A e B vale sempre una delle due implicazioni $A \to B$ oppure $B \to A$ (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 $\to$ 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 Forme normali disgiuntive e congiuntive

Esempio 1.13. Sia $F = \{A, B, C\}$ un insieme di formule. Sono equivalenti:

1. $(A \to B) \wedge (\neg A \to C)$ (Se A, allora B, altrimenti C);
2. $(\neg A \vee B) \wedge (A \vee C)$ (Forma normale congiuntiva);
3. $(A \wedge B) \vee (\neg A \wedge C)$ (Forma normale disgiuntiva).

Lemma 1.14 (Forma normale disgiuntiva)**.** *Sia $F = \{\phi_1, \ldots, \phi_n\}$ un insieme di formule e sia ψ una loro combinazione booleana. Allora ψ può essere messa in* ***forma normale disgiuntiva****, ovvero equivale ad una disgiunzione di congiunzioni di formule in F o negazioni di formule in F.*

Dimostrazione. Chiamiamo "implicante primo" una formula della forma $\pm\phi_1 \wedge \ldots \wedge \pm\phi_n$ dove $\pm\phi_i$ è ϕ_i oppure $\neg\phi_i$. Ci sono in tutto 2^n implicanti primi. Ciascuno di loro implica ψ oppure implica $\neg\psi$ (in quanto il valore di verità di un implicante primo determina il valore delle combinazioni booleane delle ϕ_i). La ψ equivale alla disgiunzione degli implicanti primi che la implicano. $\square$

Lemma 1.15 (Forma normale congiuntiva)**.** *Sia $F = \{\phi_1, \ldots, \phi_n\}$ un insieme di formule e sia ψ una loro combinazione booleana. Allora ψ può essere messa in* ***forma normale congiuntiva****, ovvero equivale ad una congiunzione di disgiunzioni di formule in F o negazioni di formule in F.*

Dimostrazione. Chiamiamo "clausola" una formula della forma $\pm\phi_1 \vee \ldots \vee \pm\phi_n$ dove $\pm\phi_i$ è ϕ_i oppure $\neg\phi_i$. La negazione di una clausola equivale ad un implicante primo e viceversa. Metto $\neg\psi$ in forma normale disgiuntiva, poi prendo la negazione e usando le leggi di De Morgan $\neg(A \wedge B) \equiv \neg A \vee \neg B$ ottengo la forma normale congiuntiva di ϕ. $\square$

1.5 Teorie proposizionali

Risulta conveniente 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 Logica del primo ordine

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).

Dare le regole che governano i quantificatori non è così semplice come dare le tavole di verità. Esse verranno date nella sezione sulle regole di inferenza. Per il momento presupponiamo una conoscenza intuitiva dei quantificatori e del loro uso.

2.2 Linguaggi e strutture

L'anello $\mathbb{R}$ dei numeri reali è un esempio di "struttura". L'anello $M_{2,2}(\mathbb{R})$ delle matrici 2×2 a coefficienti reali è un altro esempio di struttura. Entrambe le strutture posseggono una operazione denotata con il simbolo "$+$" (addizione) e una operazione denotata dal simbolo "$\cdot$" (moltiplicazione), che nel caso dei numeri reali denota la moltiplicazione tra numeri reali, e nel caso delle matrici denota la moltiplicazione righe per colonne di matrici. Si tratta di operazioni con proprietà diverse (ad esempio la moltiplicazione tra matrici non è commutativa), che tuttavia vengono denotate con lo stesso simbolo. Diremo che $\mathbb{R}$ e $M_{2,2}(\mathbb{R})$ sono due strutture nel linguaggio $L = \{+, \cdot\}$. Diamo ora le definioni precise.

Definizione 2.1. Un **linguaggio**, o segnatura, per la logica 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. Una corrispondenza[1] $c \mapsto c_M$ 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 anello ordinato $M = (\mathrm{dom}(M); 0_M, 1_M, +_M, \cdot_M, <_M)$ 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 indicheremo talvolta con M sia la struttura stessa che il suo dominio $\mathrm{dom}(M)$ e scriveremo c, f, R invece di c_M, f_M, R_M quando si chiaro dal contesto se ci riferiamo al simbolo o alla sua intepretazione. Ad esempio l'anello dei numeri reali può essere indicato con $(\mathbb{R}; +, \cdot, 0, 1)$ e quello delle matrici con $(M_{2,2}(\mathbb{R}); +, \cdot, 0, 1)$, sebbene i simboli $+, \cdot, 0, 1$ abbiano nei due casi significati diversi e in taluni casi possa essere più opportuno usare dei sottoindici per distinguere.

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

2.3 Morfismi

Le L-strutture formano una "categoria", ovvero è possibile definire il concetto di "morfismo" tra due L-strutture.

Definizione 2.4. Un *morfismo* (o *omomorfismo*) $\phi\colon A \to B$ tra due L-strutture A e B è dato da una funzione $\phi\colon dom(A) \to dom(B)$ tale che:

1. se c è un simbolo di costante, allora $\phi(c_A) = c_B$;
2. se f è un simbolo di funzione di arietà n e $a_1, \ldots, a_n \in dom(A)$, allora $\phi(f_A(a_1, \ldots, a_n)) = f_B(\phi(a_1), \ldots, \phi(a_n))$;
3. se R è un simbolo di relazione di arietà n e $(a_1, \ldots, a_n) \in R_A$, allora $(\phi(a_1), \ldots, \phi(a_n)) \in R_B$.

Definizione 2.5. Un *isomorfismo* $\phi\colon A \to B$ tè un morfismo biunivoco la cui funzione inversa è essa stessa un morfismo. Più esplicitamente un isomorfismo è una bigezione $\phi\colon dom(A) \to dom(B)$ tale che:

1. se c è un simbolo di costante, allora $\phi(c_A) = c_B$;
2. se f è un simbolo di funzione di arietà n e $a_1, \ldots, a_n, a \in dom(A)$, allora $f_A(a_1, \ldots, a_n) = a$ se e solo se $f_B(\phi(a_1), \ldots, \phi(a_n)) = \phi(a)$. Equivalentemente: $\phi(f_A(a_1, \ldots, a_n)) = f_B(\phi(a_1), \ldots, \phi(a_n))$.
3. se R è un simbolo di relazione di arietà n e $a_1, \ldots, a_n \in dom(A)$, allora $(a_1, \ldots, a_n) \in R_A$ se e solo se $(\phi(a_1), \ldots, \phi(a_n)) \in R_B$.

Esempio 2.6. Sia $\mathbb{Z}$ l'anello degli interi e sia $\mathbb{Z}/(n)$ l'anello degli interi modulo n (entrambi considerati come strutture nella segnatura $L = \{0, 1, +, -, \cdot\}$). La funzione che manda un intero x nella sua classe resto modulo n costituisce un omomorfismo da $\mathbb{Z}$ a $\mathbb{Z}/(n)$.

Esempio 2.7. Sia L una segnatura con un simbolo di relazione binario f. Sia $(\mathbb{R}; +)$ la L-struttura avente come dominio i numeri reali e in cui f è interpretato come la funzione somma, e sia $(\mathbb{R}^{>0}, \cdot)$ la L-struttura avente come dominio i numeri reali positivi e in cui f è interpretato come la funzione prodotto. Allora la funzione esponenziale $x \mapsto e^x$ è un isomorfismo da $(\mathbb{R}, +)$ a $(\mathbb{R}^{>0}, \cdot)$.

Esercizio 2.8. Trovare un isomorfismo tra il gruppo additivo $(\mathbb{Z}/6\,\mathbb{Z}, +, 0)$ degli interi modulo 6 e il gruppo moltiplicativo $((\mathbb{Z}/7\,\mathbb{Z})^*, \cdot, 1)$ degli interi diversi da zero modulo 7 (entrambi considerati come strutture in una segnatura con un simbolo di operazione binaria per l'operazione gruppale e un simbolo di costante per l'elemento neutro).

Esempio 2.9. Un morfismo tra due ordini totali $(A, <_A)$ e $(B, <_B)$ è una funzione crescente: $a_1 < a_2$ implica $f(a_1) < f(a_2)$.

Definizione 2.10. Il concetto di *immersione* si ottiene da quello di isomorfismo rinunciando alla richiesta che ϕ sia suriettiva. Una immersione è dunque un isomorfismo verso la sua immagine.

2.4 Sottostrutture

Definizione 2.11. Date due L-strutture A e B diciamo che A è una *sottostruttura* di B se $dom(A) \subseteq dom(B)$ e la funzione di inclusione $i \colon dom(A) \to dom(B)$ è una immersione. Ciò significa che i simboli di costante sono intepretati nello stesso modo in A e in B, e i simboli di funzione e relazione sono interpretati in A come la restrizione agli elementi di A delle funzioni e relazioni che intepretano gli stessi simboli in B. Ad esempio l'anello degli interi $\mathbb{Z} = (\mathbb{Z}, 0, 1, +, -, \cdot)$ è una sottostruttura dell'anello dei reali $(\mathbb{R}, 0, 1, +, -, \cdot)$. Per indicare che A è una sottostruttura di B scriviamo $A \subseteq B$.

Nota 2.12. Osserviamo che in strutture relazionali (ovvero in una segnatura senza senza simboli di funzione e costante) ogni sottoinsieme non vuoto determina una sottostruttura (ad esempio un sottoinsieme di un ordine lineare è un ordine lineare con l'ordine indotto), mentre per strutture con funzioni o costanti questo in genere non accade.

Affinché un sottoinsieme non vuoto $X \subset dom(B)$ del dominio di una struttura B determini una sottostruttura di B occorre (e basta) che X contenga l'interpretazione dei simboli di costante della segnatura (se ve ne sono) e che sia chiuso rispetto alla interpretazione dei simboli di funzione. Se questa condizione è verificata c'è un unica sottostruttura di B avente X come dominio, e possiamo quindi per abuso di linguaggio identificare il sottoinsieme con la sottostruttura.

Nota 2.13. Il concetto di sottostruttura, così come quello di morfismo, dipende in modo essenziale dalla scelta della segnatura. Ad esempio $(\mathbb{N}, +, 0)$ è una sottostruttura di $(\mathbb{Z}, +, 0)$ ma non è un sottogruppo nel senso usuale dell'algebra (non è chiuso rispetto alla funzione sottrazione). Per fare in modo che le sottostrutture dei gruppi siano gruppi, dobbiamo mettere nella segnatura anche un simbolo per l'inversa della operazione gruppale.

Consideriamo ora la segnatura $L = \{+, -, \cdot, 0, 1\}$ degli anelli. Ogni sottostruttura A di un anello B è essa stessa un anello. Tuttavia se A è un campo, non è detto che B sia un campo. Per esserlo deve essere chiuso per la funzione $1/x$. Si noti che non possiamo mettere nella segnatura un simbolo per la funzione $1/x$ perché tale funzione è indefinita per $x = 0$ e nella segnatura ammettiamo solamente simboli per funzioni definite sull'intero dominio della struttura (ovviamente si potrebbe convenire che $1/0 = 0$, ma ciò sarebbe in contrasto con l'uso comune).

2.5 Termini e Formule

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

Definizione 2.14. 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;

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 2.15. 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 2.16. 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 2.17. 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.

Nota 2.18. 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 risparmi di parentesi seguiamo le convenzioni già data per la logica proposizionale (Remark 1.4). 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 2.19. 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 la formula stessa $(\alpha \rightarrow \beta)$ e tutte le sottoformule di α e di β (incluse α e β stesse).

Definizione 2.20. 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. Se le variabili libere di φ sono incluse in $\{x_1, \ldots, x_n\}$ scriveremo anche $\varphi(x_1, \ldots, x_n)$ invece di φ. Una formula senza variabili libere viene detta **formula chiusa** o **enunciato**.

Esempio 2.21. 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).

2.6 Semantica di Tarski

Data una L-struttura M vogliamo definire cosa cosa significhi che una L-formula φ è vera in M. L'idea è semplicemente quella di dire che la formula risulta vera se si interpretano i simboli di L come prescrive la L-struttura M, e si interpretano i quantificatori $\forall x$ e $\exists x$ con $\forall x \in M$ ed $\exists x \in M$ rispettivamente, ovvero si suppone che le variabili varino su elementi di M (o meglio di $\mathrm{dom}(M)$). I connettivi booleani sono intepretati come al solito tramite le tavole di verità, e il simbolo $=$ viene interpretato come la relazione di uguaglianza.

Esempio 2.22. Sia $L = \{0, 1, +, \cdot\}$. La formula $\forall x \exists y (x \cdot y = 1)$ è vera nella L-struttura $\mathbb{R}$ (l'anello dei reali) e falsa in $\mathbb{Z}$ (l'anello degli interi), in quanto nei reali ogni elemento ha un inverso moltiplicativo mentre in $\mathbb{Z}$ ciò non è vero.

Esempio 2.23. Sia $L = \{P, Q, +\}$ dove P, Q sono simboli di predicato unario e $+$ è un simbolo di funzione binaria. Sia M la L-struttura con dominio $\mathbb{N}$ (l'insieme dei numeri naturali) e in cui $+_M : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ è l'addizione, $P_M \subseteq \mathrm{dom}(M)$ è l'insieme dei numeri pari maggiori di quattro e $Q_M \subseteq \mathrm{dom}(M)$ è l'insieme dei numeri primi. Consideriamo la formula $\forall x (P(x) \to \exists y \exists z (Q(y) \wedge Q(z) \wedge x = y + z))$. Essa è vera in M se e solo se, per definizione, per ogni x pari maggiore di quattro esistono y, z primi tali che $x = y + z$, ovvero ogni numero pari maggiore di quattro è la somma di due numeri primi. Si tratta della cosidetta congettura di Goldbach, che non si sa se è vera o falsa, ma che tuttavia, in base alle leggi della logica classica, è vera o falsa.

Passiamo ora alle definizioni formali. La definizione che daremo di "φ è vera in M" sarà per induzione sulla complessità di φ. L'induzione è necessaria solo se si vuole dare la definizione per una formula φ generica, altrimenti se si ha una formula specifica si può semplicemente procedere come negli esempi sopra dati. Siccome le formule possono contenere al loro interno dei termini, dovremo prima dare la semantica dei termini.

Definizione 2.24. Sia $\{x_1, \ldots, x_n\}$ un insieme di variabili e sia M una L-struttura. Una *valutazione* in M delle variabili $x_1, \ldots, x_n$ è una funzione $v : \{x_1, \ldots, x_n\} \to \mathrm{dom}(M)$ che assegna a ciascuna delle variabili x_i un valore $a_i = v(a_i)$ nel dominio della L-struttura M. Scriveremo anche $v = (a_1/x_1, \ldots, a_n/x_n)$ per indicare tale valutazione.

Definizione 2.25. Dato un L-termine t le cui variabili sono incluse nel dominio della valutazione v definiamo induttivamente $M(t(v)) \in dom(M)$ nel modo seguente:

1. Se x è una variabile e v è una valutazione che associa a x il valore $a \in M$, allora $M(x(v)) = a$;

2. Se c è un simbolo di costante di L, allora $M(c(v)) = c_M$;

3. Se t è della forma $f(t_1, \dots, t_n)$, allora $M(t(v)) = f_M(M(t_1(v)), \dots, M(t_n(v)))$.

Ad esempio nella struttura $(\mathbb{R}; +, \cdot, 0, 1)$ il valore del termine $x + 1$ nella valutazione $(3/x)$ è 4. Si noti che in base alle definizioni avremmo dovuto scrivere $+(x, 1)$ anziché $x+1$, ma per le funzioni binarie è prassi usare la notazione infissa anziché prefissa.

Definizione 2.26. Sia M una L-struttura, sia ϕ una L-formula le cui variabili libere siano incluse in $\{x_1, \dots, x_n\}$ e sia $v = (a_1/x_1, \dots, a_n/x_n)$ una valutazione delle variabili con $v(x_i) = a_i \in M$. Diciamo che $\phi(v)$ è vera in M, e scriviamo $M \models \phi(v)$, se ciò segue dalle seguenti clausole induttive. L'induzione viene fatta sul numero dei connettivi della formula.

1. $M \models \neg\phi(v)$ se e solo se $M \not\models \phi(v)$ (cioè non vale $M \models \phi(v)$);

2. $M \models (\phi \wedge \psi)(v)$ se e solo se $M \models \phi(v)$ e $M \models \psi(v)$;

3. $M \models (\phi \vee \psi)(v)$ se e solo se $M \models \phi(v)$ o $M \models \psi(v)$;

4. $M \models (\phi \to \psi)(v)$ se e solo se $M \not\models \phi(v)$ o $M \models \psi(v)$.

In altre parole il valore di verità in M di una formula ottenuta tramite $\neg, \wedge, \vee, \to$ da altre formule si ottiene applicando le tavole di verità ai valori delle sue sottoformule. Veniamo ora ai quantificatori:

5. $M \models (\forall x\phi)(v)$ se e solo se per ogni $a \in dom(M)$, $M \models \phi(a/x, v)$;
   dove indichiamo con $(a/x, v)$ la valutazione che coincide con v sulle variabili diverse da x ed assegna ad x il valore a.

6. $M \models (\exists x\phi)(v)$ se esiste $a \in dom(M)$ tale che $M \models \phi(a/x, v)$.

Restano da trattare le formule atomiche, che costituiscono la base dell'induzione:

7. $M \models R(t_1, \dots, t_n)(v)$ se e solo se $(M(t_1(v)), \dots, M(t_n(v))) \in R_M$;

8. $M \models t_1 = t_2$ se e solo se $M(t_1(v))$ e $M(t_2(v))$ sono lo stesso elemento.

Notazioni: Una formula φ con variabili libere incluse in $\{x_1, \dots, x_n\}$ verrà talvolta indicata con la notazione $\varphi(x_1, \dots, x_n)$. In questo caso, data una valutazione $v = (a_1/x_1, \dots, a_n/x_n)$ con $a_i = v(x_i) \in \mathrm{dom}(M)$, scriveremo $M \models \varphi(a_1, \dots, a_n)$ anzichè $M \models \varphi(v)$. Consideriamo ora una formula che inizia con un quantificatore, come ad esempio $\forall x\varphi$. Se le variabili libere di φ sono incluse in $\{x, x_1, \ldots, x_n\}$ e $v = (a_1/x_1, \ldots, a_n/x_n)$, invece di $M \models (\forall x\phi)(v)$ scriveremo anche $M \models \forall x\varphi(x, a_1, \ldots, a_n)$. In tal modo la clausola del $\forall$ prende la forma seguente: $M \models \forall x\varphi(x, a_1, \ldots, a_n)$ se e solo se, per ogni $a \in M$, $M \models \phi(a, a_1, \ldots, a_n)$. Con analoghe convenzioni abbiamo $M \models \exists x\phi(x, a_1, \ldots, a_n)$ se e solo se esiste $a \in M$ tale che $M \models \phi(a, a_1, \ldots, a_n)$.

Esercizio 2.27. Il valore di verità di $\phi(v)$ in M dipende solo dalla restrizione di v allle variabili libere di ϕ. In altre parole se v e v' coincidono sulle variabili libere di ϕ, allora $M \models \phi(v)$ se e solo se $M \models \phi(v')$.

In particolare se ϕ è un L-enunciato (ovvero una L-formula senza variabili libere) allora il suo valore di verità in M non dipende da v.

Diciamo in tal caso che ϕ è vero in M, e scriviamo $M \models \phi$, se $M \models \phi(v)$ per ogni v (o equivalentemente per qualche v).

Proposizione 2.28. *Data una formula della forma $\varphi(t_1/x_1, \ldots, t_n/x_n)$ (dove ciascun termine t_i è sostituibile al posto di x_i in φ) e una valutazione v delle variabili libere della formula in M, il valore di verità di $\varphi(t_1/x_1, \ldots, t_n/x_n)(v)$ in M dipende solo dai valori $b_i = t_i(v) \in M$ dei termini e non dai termini stessi (cioè se rimpiazziamo i vari t_i con altri termini sostituibili t'_i con la stessa valutazione otteniamo lo stesso valore di verità.)*

Prima di dare la dimostrazione osserviamo che se aggiungessimo alle regole di formazione delle formule costrutti come “Tizio sa che” (oppure “La tale teoria dimostra che”), il teorema non varrebbe. Ad esempio può capitare che Tizio non sappia che 2^{2^5} sia un numero composto, anche se di fatto $2^{2^5} = 641 \cdot 6700417$ e ovviamente Tizio sa che $641 \cdot 6700417$ è composto. Per rendere preciso il discorso dovremmo dare la semantica di “Tizio sa che”, il che coinvolgerebbe la logica modale.

Dimostrazione. La tesi è ovvia nel caso in cui φ sia una formula atomica in quanto in tal caso il valore di verità è stato definito facendo esclusivo riferimento ai valori dei termini e non ai termini stessi. Induttivamente la tesi segue per le altre formule. L'unico caso delicato da considerare è quello in cui φ sia della forma $\forall x\phi$. Supponiamo che $M \models (\forall x\phi)(t_1/x_1, \ldots, t_n/x_n)(v)$ e cerchiamo di dimostrare $M \models (\forall x\phi)(t'_1/x_1, \ldots, t'_n/x_n)(v)$. Per la semantica di Tarski per ogni $a \in M$ abbiamo $M \models \phi(t_1/x_1, \ldots, t_n/x_n)(a/x, v)$. Si noti che la x non compare nei termini t_i altrimenti non sarebbero sostituibili e analogo discorso vale per i termini t'_i. Dall'ipotesi $t_i(v) = t'_i(v)$ segue allora $t_i(a/x, v) = t'_i(a/x, v)$. Per ipotesi induttiva $M \models \phi(t'_1/x_1, \ldots, t'_n/x_n)(a/x, v)$, e siccome ciò vale per ogni $a \in M$ otteniamo $M \models (\forall x\phi)(t'_1/x_1, \ldots, t'_n/x_n)(v)$. $\square$

2.7 Sostituzioni e cattura delle variabil

Definizione 2.29. (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).

Nota 2.30. Non bisogna confondere le sostituzioni di termini con le valutazioni delle variabili. Nelle valutazioni si assegnano ad alcune variabili dei valori nel dominio della struttura ma non viene effettuata alcuna sostituzione, come in $\mathbb{R} \models (x > 1)(\pi/x)$ (pi-greco è maggiore di 1). Nelle sostituzioni di termini invece si rimpiazzano alcune variabili con dei termini del linguaggio, ottenendo una nuova formula, come in $(x > 1)(xy + 1/x) := (xy + 1 > 1$. Nonostante la notazione simile non ci si può sbagliare: le valutazioni coinvolgono elementi nel dominio di una struttura, le sostituzioni coinvolgono termini di un linguaggio.

Nota 2.31. Se φ è una formula possiamo dare una definizione induttiva di $\varphi(t/x)$ nel modo seguente.

1. La sostituzione (t/x) distribuisce sui connettivi booleani. Ad esempio $(\alpha \wedge \beta)(t/x) = \alpha(t/x) \wedge \beta(t/x)$.

2. Se φ inizia con un $\forall x$ o un $\exists x$, la sostituzione (t/x) non viene effettuata. Ad esempio $(\forall x \psi)(t/x) = \forall x \psi$.

3. Se φ inizia con una quantificatore su una variabile y diversa da x, allora $\varphi(t/x)$ si ottiene levando il quantificatore iniziale, effettuando la sostituzione nella formula così ottenuta, e rimettendo il quantificatore. Ad esempio $(\forall y \alpha)(t/x) = \forall y(\alpha(t/x))$.

Rimane il caso in cui φ è una formula atomica, ovvero una formula della forma $R(t_1, \ldots, t_n)$, con R simbolo di predicato, oppure della forma $t_1 = t_2$. In questo caso dobbiamo prima definire $t_i(t/x)$ dove t_i e t sono termini. Ciò viene fatto per induzione sulla complessità di t_i. Se $t_i = f(r_1, \ldots, r_k)$ con f simbolo di funzione e gli r_i sottotermini, $t_i(t/x)$ è il termine $f(r_1(t/x), \ldots, r_k(t/x))$. Se t_i è una costante o una variabile diversa da x, $t_i(t/x)$ coincide con t_i. Se t_i è la variabile x, $t_i(t/x)$ è t. Avendo definito la sostituzione tra termini possiamo definire la sostituzione di un termine in una formula atomica come segue:

4. $R(t_1, \ldots, t_n)(t/x)$ è la formula $R(t_1(t/x), \ldots, t_n(t/x))$.

5. $(t_1 = t_2)(t/x)$ è la formula $t_1(t/x) = t_2(t/x)$.

Esercizio 2.32. 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.

Nota 2.33. 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". Il problema è che la y presente in t è stata "catturata" dal quantificatore $\exists y$.

L'osservazione precedente motiva la seguente definizione.

Definizione 2.34. 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 le variabili di t non diventano legate dopo che si è effettuata la sostituzione $\alpha(t/x)$, ovvero le variabili libere di t rimangono libere in $\alpha(t/x)$.

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

Vediamo ora come si comportano le sostituzioni dal punto di vista semantico.

Lemma 2.35. *Sia t un L-termine sostituibile al posto di x in nella L-formula φ, M una L-struttura e v una valutazione in M delle variabili libere di $\varphi(t/x)$. Allora*

$$M \models \varphi(t/x)(v) \iff M \models \varphi(b/x, v),$$

dove $b = M(t(v))$ e $(b/x, v)$ è la valutazione che coincide con v sulle variabili diverse da x ed assegna ad x il valore b.

Prima di dare la dimostrazione osserviamo che se aggiungessimo alle regole di formazione delle formule costrutti come "Tizio sa che" (oppure "La tale teoria dimostra che"), il risultato non varrebbe. Ad esempio può capitare che Tizio non sappia che 2^{2^5} sia un numero composto, anche se di fatto $2^{2^5} = 641 \cdot 6700417$ e ovviamente Tizio sa che $641 \cdot 6700417$ è composto. Per rendere preciso il discorso dovremmo dare la semantica di "Tizio sa che", cosa che si può fare attraverso la logica modale.

Dimostrazione. Per induzione sulla complessità della formula φ usando la definizione induttiva di $\varphi(t/x)$. Consideriamo vari casi iniziando con il caso in chi φ è una formula atomica della forma $R(t_1, \ldots, t_n)$.

Per definizione $R(t_1, \ldots, t_n)(t/x)$ è la formula $R(t_1(t/x), \ldots, t_n(t/x))$. Questa formula è vera in (M, v) se la n-upla ordinata dei valori di $t_1(t/x), \ldots, t_n(t/x)$ valutati in (M, v) appartiene a R_M. Ora basta osservare che $M(t_i(t/x)(v)) = M(t_i(b/x, v))$ come si verifica facilmente per induzione sulla complessità di t_i.

Tralasciamo gli altri casi facili e affrontiamo direttamente il caso in cui φ sia della forma $\forall y \alpha$ dove y è una variabile diversa da x. Osserviamo che, essendo sostituibile, il termine t non può contenere la variabile y. Per definizione $(\forall y \alpha)(t/x)$ è la formula $\forall y(\alpha(t/x))$. Per la semantica di Tarski vale $M \models \forall y(\alpha(t/x))(v)$ se e solo se per ogni $m \in M$ vale $M \models \alpha(t/x)(m/y, v)$. Per induzione quest'ultimo giudizio equivale a $M \models \alpha(b'/x, m/y, v)$ dove $b' = M(t(b'/y, v))$. Visto che ciò vale per ogni $m \in M$, ciò equivale a dire che $M \models (\forall y \alpha)(b/x, v)$, concludendo il passaggio induttivo in questo caso. Per finire osserviamo che, essendo sostituibile, t non contiene y, e quindi $b = M(t(v)) = M(t(b/y, v)) = b'$. $\square$

2.8 Insiemi definibili

Definizione 2.36. Sia M una L-struttura. Un sottoinsieme X di M^n è $\emptyset$-*definibile* se esiste una L-formula $\phi(x_1, \dots, x_n)$ tale che X è l'insieme delle n-uple $\vec{a}$ da M tali che $M \models \phi(\vec{a})$. Diciamo che X è *definibile* se esiste una L-formula $\phi(x_1, \dots, x_n, y_1, \dots, y_k)$ e dei parametri $b_1, \dots, b_k \in M$ tale che X è l'insieme delle n-uple $\vec{a}$ da M tali che $M \models \phi(\vec{a}, \vec{b})$. Diremo che X è definibile con parametri da $B \subseteq \mathrm{dom}(M)$ se i b_i possono essere presi in B.

Esercizio 2.37. La circonverenza di raggio r nel piano cartesiano, $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = r^2\}$ è definibile nella struttura $(\mathbb{R}, +, \cdot)$ con parametro $r \in \mathbb{R}$. Si dimostri che se r è razionale (o più in generale reale algebrico), la stessa circonferenza è definibile senza parametri. L'idea è quella di trovare una formula senza parametri $\varphi(z)$ che equivale a $z = r$. Fatto ciò, invece di $x^2 + y^2 = r^2$, possiamo equivalentemente scrivere $\exists z(\varphi(z) \wedge x^2 + y^2 = z^2)$.

Esercizio 2.38. L'insieme dei numeri primi è definibile nella struttura $(\mathbb{N}, +, \cdot)$.

Esempio 2.39. Gödel ha dimostrato che l'insieme delle coppie $(a, b) \in \mathbb{N}^2$ tali che $b = 2^a$ è definibile nella struttura $(\mathbb{N}, +, \cdot)$.

2.9 Teorie e modelli

Definizione 2.40. 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 2.41. 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 2.42. 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**, o **semanticamente coerente**, se ha almeno un modello.

2.10 Conseguenza logica

Definizione 2.43. (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 renda veri tutti gli assiomi di T e non renda 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).

Definizione 2.44. (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 2.45. 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.

2.11 Espansioni e restrizioni del linguaggio

Definizione 2.46. 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 $(\mathbb{R}, +, \cdot, 0, 1)$. Dato un insieme T di L-enunciati e $L' \supseteq L$, possiamo pensare T come ad una L-teoria o ad una L'-teoria. Il prossimo esercizio mostra che ciò non influenza la definizione di $T \models \varphi$.

Esercizio 2.47. 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 $Mod_{L'}(T) \subseteq Mod_{L'}(\phi)$.

Lemma 2.48. *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 $T \cup \{\neg\phi(c)\}$. □

3 Esempi di teorie

3.1 Aritmetica di Robinson

Definizione 3.1. Sia $L = \{0, S, +, \cdot\}$ un linguaggio con un simbolo di costante 0, un simbolo di funzione unaria S, e due simboli di funzione binaria $+, \cdot$. L'aritmetica di Robinson è la L-teoria con i seguenti assiomi, che per brevità enunciamo sottointendendo i quantificatori universali $\forall x, \forall y$ di fronte alle formule:

Q1 $S(x) = S(y) \to x = y$

Q2 $0 \neq S(x)$

Q3 $x \neq 0 \to \exists y(x = S(y))$

Q4 $x + 0 = 0$

Q5 $x + S(y) = S(x + y)$

Q6 $x \cdot 0 = 0$

Q7 $x \cdot S(y) = x \cdot y + x$

Un **modello** dell'aritmetica di Robinson è per definizione un insieme non vuoto dotato di uno zero 0, un successore S, e due operazioni $+, \cdot$ che verificano gli assiomi Q1-Q7.

In numeri naturali sono un modello dell'aritmetica di Robinson. Un altro modello dell'aritmetica di Robinson è il seguente.

Esempio 3.2. Consideriamo l'anello dei polinomi $\mathbb{Z}[t]$ con l'usuale definizione di somma e prodotto tra polinomi. Definiamo 0 come il polinomio costante zero, e definiamo il successore di un polinomio $p(t)$ come il risultato di sommare a $p(t)$ il polinomio costante 1. Questa struttura verifica tutti gli assiomi dell'aritmetica di Robinson tranne l'assioma Q2, ovvero l'assioma che dice che zero non ha un predecessore (in quanto il polinomio costante -1 è il predecessore di 0). Per ottenere un modello dell'aritmetica di Robinson possiamo considerare la sottostruttura

$$\mathbb{Z}[t]^+ \subseteq \mathbb{Z}[t]$$

consistente di tutti i polinomi $a_0 + a_1 t + \ldots + a_n t^n$ con $a_n > 0$ (gli altri coefficienti a_i possono anche essere negativi o zero) e dei polinomi costanti a_0 con $a_0 \geq 0$. Detto in altri termini, un polinomio appartiene a $\mathbb{Z}[t]^+$ se non assume valori negativi per valori di t sufficientemente grandi. Ad esempio $-8 + 4t - 5t^2 + 2t^3$ appartiene a $\mathbb{Z}[t]^+$. Lasciamo al lettore la verifica che $\mathbb{Z}[t]^+$ è un modello dell'Aritmetica di Robinson.

Esempio 3.3. Sia $L = \{0, S, +, \cdot\}$ e consideriamo le L-formula φ data dalla seguente scrittura:

$$\forall x \big(\exists y(y + y = x) \vee \exists y(y + y + S(0) = x)\big).$$

Se come L-struttura prendiamo $\mathbb{N}$, la formula esprime un'affermazione vera, ovvero il fatto che ogni numero naturale è pari o dispari. Se però prendiamo l'anello dei polinomi $\mathbb{Z}[t]$, o la sua sottostruttura $\mathbb{Z}[t]^+$ precedentemente definita, otteniamo un'affermazione falsa, in quanto ad esempio il polinomio $t \in \mathbb{Z}[t]$ non è nè il doppio nè il doppio più uno di un altro polinomio (servirebbe nel primo caso il polinomio $t/2$, che però non è in $\mathbb{Z}[t]$).

Il fatto che la formula φ sopra definita non sia vera in tutti i modelli dell'aritmetica di Robinson, (essendo falsa in $\mathbb{Z}[t]^+$) indica che essa non è *conseguenza logica* di tali assiomi. Il fatto che anche la sua negazione $\neg\varphi$ non sia vera in tutti i modelli dell'aritmetica di Robinson (essendo φ vera in $\mathbb{N}$), indica che anche $\neg\varphi$ non è conseguenza logica degli assiomi. In altre parole la formula φ è "indipendente" dagli assiomi di Robinson, i quali pertanto sono "incompleti".

3.2 Aritmetica di Peano

Definizione 3.4. L'aritmetica di Peano del primo ordine, PA, si ottiene aggiungendo a Q infiniti assiomi chiamati assiomi di induzione. Consideriamo una coppia (ϕ, x) dove ϕ è una formula del primo ordine di L, e x è una variabile libera di ϕ (la variabile su cui facciamo l'induzione). Alla coppia (ϕ, x) associamo l'assioma $Ind_{\phi,x}$ definito come $\phi(0) \wedge \forall x(\phi(x) \to \phi(Sx)) \to \forall y \phi(y)$, dove la notazione $\phi(t)$, indica la formula ottenuta sostituendo t al posto delle occorrenze libere di x in ϕ. La formula ϕ potrebbe contenere altre variabili libere oltre alla x, nel qual caso si intende che le rimanenti variabili siano quantificate universalmente nel corrispondente assioma $Ind_{\phi,x}$. Ad esempio se $\phi = \phi(x, z)$ ha come variabili libere x e z, l'assioma $Ind_{\phi,x}$ è $\forall z[\phi(0, z) \wedge \forall x(\phi(x, z) \to \phi(Sx, z)) \to \forall y \phi(y, z)]$, dove l'induzione si fa su x e l'altra variabile libera z si comporta come un parametro.

Esercizio 3.5. Si dimostri in PA che la somma e il prodotto sono commutativi.

4 Deduzione naturale

Tramite opportune regole di inferenza, definiremo una relazione di dimostrabilità formale $\vdash$ che risulterà a posteriori equivalente alla relazione di conseguenza logica $\models$. A sinistra del segno $\vdash$ metteremo un insieme Γ di formule di un fissato linguaggio L, a destra una singola formula ϕ. Se vale la relazione $\Gamma \vdash \phi$ diremo che ϕ è dimostrabile a partire da Γ.

Notatione 4.1. Le virgole a sinistra del segno $\vdash$ indicano un'unione. Ad esempio $\Gamma, \phi \vdash \varphi$ significa $\Gamma \cup \{\phi\} \vdash \varphi$, dove le lettere maiuscole indicano insiemi di formule, le minuscole singole formule.

Tratteremo dapprima il caso proposizionale, poi il caso predicativo.

4.1 Caso proposizionale

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

Definizione 4.2. 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.

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

  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).

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

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

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

  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 (che poi viene scaricata).

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

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

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.

Esempio 4.3. Si ha $A\wedge B\vdash A\vee B$. 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 $(\vdash\perp)$ diventa irrilevante se si assume che $\neg\neg A$ equivalga ad A, ma quest'ultima equivalenza richiede per essere dimostrata proprio la regola RAA (in questo contesto non possiamo usare le tavole di verità).

Esempio 4.4. Mostriamo $\neg\neg A\vdash A$. Per RAA basta far vedere $\neg\neg A,\neg A\vdash\perp$. 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 4.5. Verifichiamo che $\vdash A\vee\neg A$ (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. 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 $\neg(A\vee\neg A)\vdash\neg A$.

4.2 Caso predicativo

Per definire la relazione di dimostrabilità $\vdash$ per la logica del primo ordine dobbiamo aggiungere alle regole proposizionali della Definizione 4.2 delle ulteriori regole per i quantificatori e il simbolo di uguaglianza. A sinistra del segno $\vdash$ metteremo un insieme di formule del primo ordine di un fissato linguaggio L del primo ordine, possibilmente contenenti variabili libere, e a destra una singola formula. Se vale la relazione $\Gamma \vdash \phi$ diremo che ϕ è dimostrabile a partire da Γ.

Definizione 4.6. Diciamo che $\Gamma \vdash \varphi$ se ciò segue dalle seguenti clausole induttive.

- (Regole proposizionali) Tutte le regole della Definizione 4.2, ma applicate a formule della logica del primo ordine anziché a formule proposizionale.

- (Scaricamento ipotesi) Se $\Gamma, \alpha \vdash \beta$, allora $\Gamma \vdash \alpha \to \beta$. Schematicamente:

$$\frac{\Gamma, \alpha \vdash \beta}{\Gamma \vdash \alpha \to \beta}$$

  Se riesco a dimostrare β sotto l'ipotesi aggiuntiva α, allora ho dimostrato $\alpha \to \beta$ senza alcuna ipotesi aggiuntiva.

- (Generalizzazione) Sia y una variabile che non occorre libera nelle formule di $\Gamma \cup \{\varphi\}$. Se $\Gamma \vdash \varphi(y/x)$, allora $\Gamma \vdash \forall x\varphi$. Schematicamente:

$$\frac{\Gamma \vdash \varphi(y/x)}{\Gamma \vdash \forall x\varphi}$$

  L'idea è che per dimostrare $\forall x\varphi(x)$ basta dimostare $\varphi(y)$ per un y "generico", ovvero per un y che non compare nelle ipotesi.

- (Quantificatore esistenziale) $\Gamma \vdash \exists x\varphi$ se e solo se $\Gamma \vdash \neg\forall x\neg\varphi$.

- (Particolarizzazione) Se $\Gamma \vdash \forall x\phi$, allora $\Gamma \vdash \phi(t/x)$, dove t è un qualsiasi termine sostituibile per x in ϕ.

$$\frac{\Gamma \vdash \forall x\phi}{\Gamma \vdash \phi(t/x)}$$

- (Riflessività dell'uguaglianza) Si ha

$$\Gamma \vdash t = t\ ,$$

  dove t è un termine qualsiasi.

- (Sostitutività dell'uguaglianza) Siano t, t' termini sostituibili per x in ϕ. Se $\Gamma \vdash t = t'$ e $\Gamma \vdash \phi(t/x)$, allora $\Gamma \vdash \phi(t'/x)$. Schematicamente:

$$\frac{\Gamma \vdash \phi(t/x) \qquad \Gamma \vdash t = t'}{\Gamma \vdash \phi(t'/x)}.$$

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

Esercizio 4.7. La regola di indebolimento è ridondante in quanto si può dedurre dalle altre. Omettendo la regola di indebolimento si dimostrano le stesse cose.

4.3 Teorema di corretezza

Definizione 4.8. Sia Γ un insieme di L-formule e sia φ una L-formule. Supponiamo che le variabili libere di tutte queste formule siano incluse nell'insieme $\{x_i : i \in I\}$. Possiamo allora considerare queste formule come formule chiuse nel linguaggio $L \cup \{x_i : i \in I\}$ identificando le variabili libere con nuovi simboli di costante. Definiamo $\Gamma \models \varphi$ se i modelli di Γ nel linguaggio $L \cup \{x_i : i \in I\}$ sono inclusi nei modelli di φ nello stesso linguaggio.

Il collegamento tra le regole della deduzione naturale e la relazione di conseguenza logica (sia nel caso proposizionale che predicativo) è il seguente:

Definizione 4.9. 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 4.10. 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.

Nota 4.11. 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 4.8).

Nota 4.12. 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.

Esempio 4.13. La regola di generalizzazione ($\vdash \forall$)

$$\frac{\Gamma \vdash \varphi(y/x)}{\Gamma \vdash \forall x \varphi}$$

è corretta.

Dimostrazione. Supponiamo $\Gamma \models \varphi(y/x)$ nel linguaggio in cui pensiamo le variabili libere come costanti (Definizione 4.8). Per il Lemma 2.48 ne segue che $\Gamma \models \forall x \varphi$. □

Esempio 4.14. La regola di particolarizzazione ($\vdash /e$)

$$\frac{\Gamma \vdash \forall x \varphi}{\Gamma \vdash \varphi(t/x)},$$

con t sostituibile al posto di x in φ, è corretta.

Dimostrazione. Per il Lemma 2.35. □

Lemma 4.15. *Tutte le regole della deduzione naturale sono corrette.*

Dimostrazione. Ne abbiamo viste alcune, completare come esercizio. □

Theorem 4.16 (Teorema di correttezza)**.** *Se* $\Gamma \vdash \theta$*, allora* $\Gamma \models \theta$*.*

Dimostrazione. Per induzione sulla definizione di $\Gamma \vdash \varphi$. □

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

4.4 Teorema di compattezza: versione sintattica

Theorem 4.17 (Compattezza sintattica)**.** *Se* $\Gamma \vdash \theta$ *allora esiste un sottoinsieme finito* $T \subseteq \Gamma$ *tale che* $T \vdash \theta$*. In particolare, prendendo come* θ *la formula sempre falsa* $\perp$*, si ottiene che una teoria* Γ *è sintatticamente coerente se e solo se ogni sua sottoteoria finita è sintatticamente coerente.*

Dimostrazione. Per induzione sulla definizione di $\Gamma \vdash \theta$. Il caso base si ha quando l'ultima regola adoperata è

$$\frac{\varphi \in \Gamma}{\Gamma \vdash \varphi}$$

In tal caso basta prendere $T = \{\varphi\}$. Un altro caso interessante è quando l'ultima regola adoperata è

$$\frac{\Gamma, \alpha \vdash \beta}{\Gamma \vdash \alpha \to \beta}$$

Per ipotesi induttiva esiste un insieme finito $T \subseteq \Gamma \cup \{\alpha\}$ da cui si può dedurre β. Per indebolimento possiamo supporre che T contenga α e sia quindi della forma $T' \cup \{\alpha\}$ per un certo sottoinsieme finito $T' \subseteq \Gamma$. Abbiamo dunque $T', \alpha \vdash \beta$. Applicando la regola otteniamo $T' \vdash \alpha \to \beta$ e per indebolimento $\Gamma \vdash \alpha \to \beta$, che dimostra la nostra tesi in questo caso. Gli altri casi sono analoghi e più facili. $\square$

Nota 4.18. Alternativamente avremmo potuto cominciare con il definire $T \vdash \varphi$ solo nel caso in cui T è finito, ed estendere poi la definizione al caso generale convenendo che $\Gamma \vdash \varphi$ se esiste $T \subseteq \Gamma$ finito tale che $T \vdash \varphi$.

5 Teorema di completezza

5.1 Lemma di Lindenbaum

Definizione 5.1. Una teoria Γ si dice **incoerente** (o **contradditoria**) se $\Gamma \vdash \perp$. Diciamo che Γ è **coerente** se non è incoerente.

Esercizio 5.2. 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, $\Gamma \vdash \varphi$.

Esercizio 5.3. Se $\Gamma \vdash \varphi$, allora Γ e $\Gamma \cup \{\varphi\}$ hanno gli stessi teoremi.

Lemma 5.4. *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 $\Gamma \vdash \neg\phi$. Essendo ϕ e la sua negazione entrambe dimostrabili da Γ, per la regola delle tautologie otteniamo $\Gamma \vdash \perp$. $\square$

Definizione 5.5. Una L-teoria coerente Γ si dice *completa* se data una L-formula ϕ vale $\Gamma \vdash \phi$ oppure $\Gamma \vdash \neg\phi$.

Definizione 5.6. 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.

Nota 5.7. Supponiamo che Γ sia coerente massimale e $\Gamma \vdash \phi$. Allora $\phi \in \Gamma$.

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

Lemma 5.8. *Sono equivalenti:*

1. *Γ è coerente massimale;*
2. *Γ è coerente e per ogni formula ϕ si ha $\phi \in \Gamma$ 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 5.4 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. □

Lemma 5.9. *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. Per compattezza sintattica esiste un sottoinsieme finito $S \subset \bigcup_i T_i$ tale che $S \vdash \varphi$. Poiché le T_i formano una catena esiste i tale che S è incluso in una delle T_i. Quindi $T_i \vdash \phi$. □

Corollario 5.10. *L'unione di una catena di teorie coerenti è coerente.*

Lemma 5.11. *(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 5.4 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 $\neg\theta$ (in quanto o ϕ_n o la sua negazione appartiene a T_{n+1}). Quindi per il Lemma 5.8 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 5.10. □

5.2 Dimostrazione teorema di completezza: caso proposizionale

Lemma 5.12. *Sia T una L-teoria coerente.*

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 $\psi \in T$).*

Nota 5.13. Se omettiamo le regole sui quantificatori e l'uguaglianza, il sistema di regole di inferenza che abbiamo dato è corretto anche per la logica proposizionale e il Lemma di Lindembaum è valido anche per la logica proposizionale.

Theorem 5.14 (Completezza proposizionale)**.** *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 $T' \supseteq T$. In particolare per ogni variabile proposizionale A di L, $A \in T'$ o $\neg A \in T'$. Sia M la valutazione booleana che assegna $\mathbf{1}$ alle variabili A che appartengono a T' e $\mathbf{0}$ alle variabili la cui negazione appartiene a T'. Per la coerenza di T ogni variabile riceve un solo valore, ovvero M è ben posta. Inoltre, per la massimalità di T, data una qualsiasi variabile proposizionale A del linguaggio, $A \in T$ oppure $\neg A \in T$, e quindi in ogni caso $M(A) \in \{\mathbf{1}, \mathbf{0}\}$ è definito. Usando le tavole di verità ogni formula di L (non solo le variabili proposizionali) riceve da M un valore $\mathbf{1}$ o $\mathbf{0}$. Per induzione sulla complessità delle formule, e usando il Lemma 5.12 per fare i passaggi induttivi, si verifica che ogni formula di T' riceve il valore $\mathbf{1}$ da M. Quindi M è un modello di T', e pertanto anche di T. □

Corollario 5.15. *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 $T \not\models \phi$. □

Si noti che il corollario appena dimostrato sarebbe stato ovvio (in base alle regola di inferenza delle tautologie) se avessimo preso T finito.

Corollario 5.16. *Se $T \models \varphi$, allora esiste un sottoinsieme finito $T' \subseteq T$ tale che $T' \models \varphi$.*

Dimostrazione. Immediato dalla compattezza sintattica e dalla completezza. □

Esercizio 5.17. Una relazione binaria E su un insieme V può essere pensata come un grafo $G = (V, E)$ i cui vertici sono gli elementi di V e i cui lati sono costituiti dalle coppie di vertici in relazione. Un grafo si dice k-colorabile se esiste una funzione $f : V \to k$ dai suoi vertici ad un insieme di k "colori" tale che due vertici collegati da un lato abbiano colori diversi. Si dimostri, usando il teorema di compattezza proposizionale, che un grafo è k-colorabile se e solo se ogni suo sottografo finito lo è.

Dimostrazione. Per ogni coppia di vertici $(i, j) \in V^2$ si introduca una variabile proposizionale $A_{i,j}$ e sia $D(G)$ la teoria che ha come assiomi le formule della forma $A_{i,j}$ per $(i, j) \in E$ e quelle della forma $\neg A_{i,j}$ per $(i, j) \notin E$. Introduciamo ora altre variabili proposizionali $C_{i,c}$ il cui significato intuitivo è che il vertice i ha colore c, con $0 < c < k$. Sia ora T la teoria che ha come assiomi quelli di $D(G)$ e gli assiomi che esprimono il fatto che ogni vertice i ha un colore (ciò può essere espresso dalla formula $C_{i,0} \vee \ldots \vee C_{i,k-1}$) ed uno solo ($C_{i,c} \to \neg C_{i,c'}$) e che vertici adiacenti hanno colori diversi ($A_{i,j} \wedge C_{i,c} \to \neg C_{j,c}$). Si noti che ogni modello M di T induce una colorazione di G (quella in cui $f(i) = c$ se M assegna a $C_{i,c}$ il valore vero), e viceversa. Per compattezza T ha un modello se e solo se ogni suo sottoinsieme finito ha un modello. Ne segue che G è k-colorabile se e solo se ogni sottografo finito è k-colorabile (si usi il fatto che i modelli dei sottoinsiemi finiti di T inducono sottografi finiti k-colorabili di G). □

5.3 Lemma delle costanti

Lemma 5.18 (Lemma delle costanti)**.** *Sia Γ un insieme di L-formule e sia φ una L-formula. Sia c un simbolo di costante non in L. Se $\Gamma \vdash \varphi(c/x)$ nel linguaggio $L \cup \{c\}$, allora esiste una variabile y tale che $\Gamma \vdash \varphi(y/x)$ nel linguaggio L. Inoltre $\Gamma \vdash \forall x \varphi$ nel linguaggio L.*

Dimostrazione. Per compattezza sintattica esiste un sottoinsieme finito $T \subseteq \Gamma$ tale che $T \vdash \varphi(c/x)$. Sia y una variabile che non compare nè in T nè in $\varphi(c/x)$ nè in alcuna delle formule che intervengono nella dimostrazione di $\varphi(c/x)$ da T. Si noti che y esiste in quanto l'insieme di tali formule è finito e abbiamo una quantità infinita (numerabile) di variabili. Sostituendo c con y in tutta la dimostrazione, otteniamo una dimostrazione di $\varphi(y/x)$ da T. Per generalizzazione abbiamo poi $T \vdash \forall x \varphi$, e per indebolimento $\Gamma \vdash \forall x \varphi$. □

Nota 5.19. L'ipotesi che y sia scelta come specificato nella dimostrazione appena data serve ad evitare il seguente problema. Supponiamo che una delle regole usate nella dimostrazione sia

$$\frac{\Sigma(c) \vdash \varphi(y, c)}{\Sigma(c) \vdash \forall y \varphi(y, c)}$$

dove per chiarezza abbiamo evidenziato la possibile presenza di c nelle formule. Se sostituissimo nella dimostrazione c con y otterremmo

$$\frac{\Sigma(y) \vdash \varphi(y,y)}{\Sigma(y) \vdash \forall y \varphi(y,y)}$$

che non è un passaggio lecito in quanto viola la richiesta che il $\forall$ si possa applicare solo a variabili che non compaiono nelle ipotesi (in questo caso $\Sigma(y)$).

Lemma 5.20. *Sia Γ un insieme di L formule e sia φ una L-formula. Sia C un insieme di simboli di costante non in L. Se $\Gamma \vdash \varphi$ nel linguaggio $L \cup C$, allora $\Gamma \vdash \varphi$ nel linguaggio L.*

Dimostrazione. Usando la compattezza sintattica e la regola di indebolimento possiamo ridurci al caso in cui Γ sia un insieme finito. L'intera dimostrazione coinvolge allora un numero finito di formule, e dunque un numero finito delle costanti C. Rimpiazzando queste costanti con variabili libere che non appaiono nella dimostrazione otteniamo una nuova dimostrazione nel linguaggio L. $\square$

Nota 5.21. Lo stesso risultato vale se C è un insieme di simboli di relazione o funzione anziché di costante, ma non è altrettanto semplice dimostrarlo se non si dimostra prima il teorema di completezza.

5.4 Costanti di Henkin

Lemma 5.22. *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 (in L o equivalentemente in $L \cup \{c\}$ per il Lemma 5.20).*

Dimostrazione. È facile verificare che 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 $\Sigma \cup \{\phi(c)\} \vdash \perp$. Abbiamo allora $\Sigma \vdash \neg\phi(c)$ e poiché c non appare in $\Sigma \cup \phi$ otteniamo $\Sigma \vdash \forall x \neg \phi(x)$. Siccome $\Sigma \vdash \exists x \phi(x) \leftrightarrow \neg \forall x \neg \phi(x)$, ne segue che $\Sigma \cup \{\exists x \phi(x)\} \vdash \perp$. $\square$

Lemma 5.23. *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 per il teorema di completezza proposizionale $\Sigma \vdash \exists x \phi(x)$ e $\Sigma \vdash \neg\phi(c)$. Questo contraddice il Lemma 5.22. $\square$

Definizione 5.24. 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 5.25. 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 5.26. *Sia T una L-teoria coerente. Allora esiste un linguaggio $L' \supseteq L$ e una L'-teoria $T' \supseteq T$ 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 5.23 si dimostra che qualsiasi sottoteoria finita di T^* è coerente, quindi per compattezza sintattica anche T^* è coerente.

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, ciò 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 5.10.

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. $\square$

5.5 Completezza

Lemma 5.27. *Sia Σ un insieme coerente di L-enunciati. Allora esiste un linguaggio $L' \supseteq L$ e un insieme di L'-enunciati $\Sigma' \supseteq \Sigma$ tale che Σ' è coerente massimale e di Henkin.*

Dimostrazione. Prima applichiamo il Lemma 5.26 per trovare una estensione di Henkin $T \supseteq \Sigma$ in un linguaggio esteso $L_T \supseteq L$, poi il Lemma 5.11 per estendere la teoria di Henkin ad una teoria coerente massimale $\Sigma' \supseteq T$ sempre nel linguaggio L_T. Visto che nel secondo passaggio non abbiamo cambiato il linguaggio, Σ' continua ad essere di Henkin. $\square$

Definizione 5.28. (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 5.29. 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 5.30. *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 5.12 $\Sigma' \cup \{\alpha\}$ 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 $\alpha \in \Sigma'$.

Consideriamo ora la clausola del $\exists$. Supponiamo che $\exists x\phi(x) \in T$. Siccome T è di Henkin, $T \vdash \exists x\phi(x) \to \phi(c)$ per qualche costante c. Ne segue che $T \vdash \phi(c)$ e poiché T è coerente massimale $\phi(c) \in T$.

Gli altri casi sono analoghi e lasciati al lettore come esercizio. □

Theorem 5.31. *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. 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.

Per raggiungere l'obiettivo 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 $f^M : dom(M)^n \to dom(M)$ 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 $M \models t = t'$ (dove 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 $\exists x \theta(x)$. □

Nota 5.32. L'insieme delle L-formule ha cardinalità $|L| + \omega$ (che è uguale a $|L|$ se $|L|$ è infinito). L'insieme degli L-termini ha cardinalità $\leq |L| + \aleph_0$.

Theorem 5.33. *Sia T una L-teoria. Se T è coerente allora T ha un modello. Inoltre esiste un modello di cardinalità $\leq |L| + \aleph_0$.*

Dimostrazione. Se T è coerente esiste un insieme di Hintikka $T' \supseteq T$ in un linguaggio $L' \supseteq L$. Per il Teorema 5.31 T' ha un modello M. Quindi anche T ha un modello (la restrizione di M al linguaggio L). □

Theorem 5.34 (Completezza)**.** *Sia T una L-teoria. Se $T \models \phi$, allora $T \vdash \phi$.*

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

6 Teorema di compattezza

Corollario 6.1 (Compattezza)**.** *Se $T \models \phi$, esiste un sottoinsieme finito $T' \subseteq T$ tale che $T' \models \phi$. In particolare, prendendo come ϕ la formula sempre falsa $\bot$,* *una teoria ha un modello se e solo se tutti i suoi sottoinsiemi finiti hanno un modello.*

Esempio 6.2. Sia φ un enunciato nel linguaggio della teoria degli anelli $L = \{0, 1, +, \cdot\}$. Se φ è vero in ogni campo di caratteristica zero, allora φ è vero in ogni campo di caratteristica $p > 0$ sufficientemente grande.

Dimostrazione. Sia T la teoria dei campi. La teoria T_0 dei campi di caratteristica zero si ottiene aggiungendo a T gli infiniti assiomi $0 \neq 1, 0 \neq 1+1, 0 \neq 1+1+1$ etc. Scriviamo per brevità $n \neq 1$ per indicare l'ennesimo di tali assiomi. Se $T \models \varphi$, per compattezza esiste un sottoinsieme finito T' di T tale che $T' \models \varphi$. Se $n \in \mathbb{N}$ è sufficientemente grande, gli unici assiomi di T' che non appartengono a T sono della forma $m \neq 1$ con $m < n$. Ne segue che φ è vero in tutti i campi di caratteristica maggiore di m. $\square$

Esempio 6.3. Sia ZF la teoria degli insiemi di Zermelo-Fraenkel nel linguaggio $L = \{\in\}$. Se ZF è coerente, esiste un modello $(M, \in_M)$ di ZF in cui vi è una catena discendente infinita $a_{n+1} \in_M a_n$ di elementi $a_i \in M$ tali che $M \models a_i \in \omega$.

Dimostrazione. Sia $L' = L \cup C$ dove $C = \{c_n : n \in \mathbb{N}\}$ consiste di infiniti simboli di costante $c_0, c_1, \ldots$. Sia T la teoria che ha come assiomi quelli di ZF e gli infiniti assiomi $c_{n+1} \in c_n$ al variare di n. Ogni sottoteoria finita di T ha un modello che è una espansione di M. Ad esempio se T menziona solo le costanti c_i con $i \leq n$, basta intepretare c_i con il successore $n - i$-esimo dello zero di M. Per compattezza T ha un modello, e la sua restrizione a L verifica le richieste. $\square$

7 Teoremi di Löwenheim-Skolem

7.1 Löwenheim-Skolem verso l'alto: forma debole

Theorem 7.1. *Sia T una L-teoria.*

1. *Supponiamo che per ogni intero positivo n esiste un modello M_n di T di cardinalità maggiore di n. Allora T ha un modello infinito.*

2. *Supponiamo che T abbia un modello infinito. Allora per ogni cardinale infinito $\kappa \geq |L|$, T ha un modello di cardinalità κ.*

Dimostrazione. Assumiamo che per ogni intero positivo n esista un modello M_n di T di cardinalità maggiore di n. (Questa ipotesi è verificata in particolare se T ha un modello infinito.) Sia $\kappa \geq |L|$ un cardinale infinito. Mostriamo che T ha un modello di cardinalità κ (ciò dimostra sia il primo che il secondo punto). Sia L' il linguaggio ottenuto da L con l'aggiunta di un insieme C di cardinalità κ di nuovi simboli di costante. Sia T' la L'-teoria i cui assiomi sono quelli di T più tutti gli assiomi della forma $c \neq c'$, dove c, c' sono costanti distinte di C. Dimostriamo innanzitutto che ogni sottoteoria finita S di T' ha un modello. A tal fine osserviamo che S può menzionare solo un insieme finito - diciamo n -

delle costanti di C. Per ipotesi esiste un modello A di T di cardinalità $\geq n$. Sia A' la L'-struttura che espande A interpretando le n costanti di C menzionate in S con n elementi distinti di A. Tale A' è un modello di S. Per il teorema di compattezza possiamo concludere che T' ha un modello B, che per il teorema 5.33 può essere scelto di cardinalità $\leq \kappa$, ma che d'altra parte deve essere di cardinalità $\geq \kappa$ in quanto dovendo verificare tutti i nuovi assiomi $c \neq c'$ deve interpretare le costanti di C con elementi distinti del dominio. La restrizione di B al linguaggio originale L è un modello di T di cardinalità κ. $\square$

Corollario 7.2. *L'aritmetica di Peano del primo ordine ha un modello non numerabile.*

7.2 Immersioni elementari

Definizione 7.3. Un morfismo $f\colon \mathcal{A} \to \mathcal{B}$ tra due L-strutture si dice una *immersione elementare* se per ogni n e per ogni L-formula $\phi(x_1, \ldots, x_n)$ con variabili libere incluse in $\{x_1, \ldots, x_n\}$ e per ogni $a_1, \ldots, a_n \in A$, si ha:

$$\mathcal{A} \models \phi(a_1, \ldots, a_n), \text{ se e solo se } \mathcal{B} \models \phi(f(a_1), \ldots, f(a_n))$$

Una sottostruttura $\mathcal{B}$ di $\mathcal{A}$ si dice *sottostruttura elementare*, e scriviamo $\mathcal{A} \prec \mathcal{B}$, se e solo se la inclusione di $\mathcal{A}$ in $\mathcal{B}$ è una immersione elementare.

Scriviamo $\mathcal{A} \precsim \mathcal{B}$ se esiste una immersione elementare da $\mathcal{A}$ a $\mathcal{B}$.

Esempio 7.4. Sia $L = (<)$ e consideriamo la L-struttura costituita dall'insieme ordinato dei numeri interi $\mathbb{Z}$, e la sua sottostruttura $2\,\mathbb{Z}$ costituita dai numeri pari. Allora $2\,\mathbb{Z}$ è elementarmente equivalente a $\mathbb{Z}$ (in quanto è isomorfa), ma non è una sua sottostruttura elementare perchè la formula $\exists x(2 < x \wedge x < 4)$ è vera in $\mathbb{Z}$ ma non in $2\,\mathbb{Z}$.

Definizione 7.5. Sia M una L-struttura e sia A un sottoinsieme del dominio di M. Sia L_A il linguaggio ottenuto da L con l'aggiunta di nuovi simboli di costante c_a corrispondenti agli elementi a di A. Espandiamo M ad una L_A struttura interpretando c_a con a, e denotiamo $(M, a)_{a \in A}$ la struttura espansa. Osserviamo che per ogni L-formula $\phi(x_1, \ldots, x_n)$ e per ogni $a_1, \ldots, a_n \in A$ si ha

$$M \models \phi(a_1, \ldots, a_n) \text{ se e solo se } (M, a)_{a \in A} \models \phi(c_{a_1}, \ldots, c_{a_n}).$$

Indichiamo con $Th((M, a)_{a \in A})$ la teoria completa della struttura $(M, a)_{a \in A}$. In particolare possiamo prendere $A = M$. Il *diagramma elementare* di M è per definizione la L_M-teoria completa

$$ED(M) = Th((M, m)_{m \in M})$$

.

Lemma 7.6. *Siano M, N L-strutture. Allora M può essere immersa elementarmente in N se e solo se N può essere espansa ad un modello di $ED(M)$. In altre parole $M \precsim N_{|L}$ se e solo se $N \models ED(M)$.*

Dimostrazione. Supponiamo che $f\colon M \to N$ sia una immersione elementare. Espandiamo N ad una L_M-struttura $N' = (N, f(m))_{m\in M}$ interpretando c_m con $f(m)$. È immediato verificare che $N' \models ED(M)$.

Viceversa se N ammette una espansione N' modello di $ED(M)$, allora la funzione $f\colon M \to N$ che manda m nell'interpretazione di c_m in N' è una immersione elementare di M in N. $\square$

Corollario 7.7. *Sia M una L-struttura e sia T una L_M-teoria. Una condizione necessaria e sufficiente affinché esista $N \succ M$ tale che $N \models T$ è che $ED(M) \cup T$ sia soddisfacibile.*

7.3 Löweinheim - Skolem verso l'alto: forma forte

Theorem 7.8. *(Löweinheim - Skolem verso l'alto) Sia M una L-struttura infinita. Sia κ un cardinale infinito $\geq |L_M| = |M| + |L| + \omega$. Allora M ha una estensione elementare di cardinalità κ.*

Dimostrazione. Per il Teorema 7.1 $ED(M)$ ha un modello N di cardinalità κ. Per il Lemma 7.6 $M \lesssim N_{|L}$. Rimpiazzando N con una copia isomorfa possiamo assumere $M \prec N_{|L}$. $\square$

7.4 Lowenheim-Skolem verso il basso

Lemma 7.9. *(Criterio di Tarski - Vaught) Consideriamo due L-strutture $\mathcal{A} \subseteq \mathcal{B}$. Supponiamo che per ogni L-formula della forma $\exists y \phi(y, x_1, \dots, x_n)$ e parametri $a_1, \dots, a_n \in A$, si abbia che se $\mathcal{B} \models \exists y \phi(y, a_1, \dots, a_n)$, allora esiste $a \in A$ tale che $\mathcal{B} \models \phi(a, a_1, \dots, a_n)$. Ne segue che $\mathcal{A} \prec \mathcal{B}$.*

Dimostrazione. Per induzione sul numero dei connettivi della formula $\theta(x_1, \dots, x_k)$ mostriamo che per ogni $a_1, \dots, a_k \in A$, $\mathcal{B} \models \theta(a_1, \dots, a_k)$ se e solo se $\mathcal{A} \models \theta(a_1, \dots, a_k)$.

Se θ è atomica, allora l'equivalenza da dimostrare segue dal fatto che $\mathcal{A}$ è una sottostruttura di $\mathcal{B}$.

Se l'equivalenza da dimostrare vale per una classe di formule, essa vale anche per tutte le formule che si ottengono da esse usando i connettivi booleani.

L'unico caso interessante è quello di formule della forma $\exists y \phi(y, x_1, \dots, x_n)$ per le quali ragioniamo come seque. Supponiamo che $\mathcal{B} \models \exists y \phi(y, \vec{a})$. Allora per le ipotesi esiste $c \in A$ tale che $\mathcal{B} \models \phi(c, \vec{a})$. Per ipotesi induttiva $\mathcal{A} \models \phi(c, \vec{a})$. Dunque $\mathcal{A} \models \exists y \phi(y, \vec{a})$. L'implicazione inversa è facile. $\square$

Theorem 7.10. *(Teorema di Lowenheim-Skolem verso il basso) Sia M una L-struttura di cardinalità κ, sia A un sottoinsieme del dominio di M e sia λ un cardinale infinito tale che $|L| + |A| \leq \lambda \leq \kappa$. Allora esiste una sottostruttura elementare $N \prec M$ di cardinalità λ il cui dominio include A.*

Dimostrazione. Sostituendo A con un insieme più grande se necessario possiamo assumere $|A| = \lambda$. La cardinalità dell'insieme delle L_A formule è λ. Per ogni L_A formula $\phi(x)$ tale che $M \models \exists x \phi(x)$ scegliamo un $b_\phi \in M$ tale che $M \models \phi(b_\phi)$ e sia A_1 l'unione di A e dell'insieme dei b_ϕ al variare di $\phi = \phi(x)$ tra la L_A formule nella variabile x. Costruiamo una successione di insiemi $A \subset A_1 \subset A_2 \subset A_3 \subset \dots$ dove ogni A_{i+1} è ottenuto da A_i nello stesso modo in cui A_1 è stato definito a partire da A. Sia $B = \bigcup_{i\in\omega} A_i$ la loro unione. Allora B è un sottoinsieme di M di cardinalità λ e per ogni L_B-formula $\phi(x)$ tale che $M \models \exists x \phi(x)$ esiste $b \in B$ tale che $M \models \phi(b)$ (in quanto i parametri di $\phi(x)$, essendo in numero finito, appartengono a qualche A_i e b può essere scelto in A_{i+1}). È facile vedere che B è il dominio di una sottostruttura di M, e per il Lemma 7.9 B è il dominio di una sottostruttura elementare di M. □

Corollario 7.11. *La teoria degli insiemi di Zermelo Fraenkel, se coerente, ha un modello numerabile.*

7.5 Completezza delle teorie κ-categoriche

Definizione 7.12. Sia κ un numero cardinale. Una L-teoria T è κ-categorica se T ha un modello di cardinalità κ e tutti i modelli di T di cardinalità κ sono isomorfi.

Theorem 7.13. *Sia T una L-teoria senza modelli finiti. Se $\kappa \geq |L|$ è un cardinale infinito e T è κ-categorica allora T è completa.*

Dimostrazione. Siano M, N modelli di T e siano T_1, T_2 le teorie complete di M, N rispettivamente. Tali teorie sono estensioni complete di T. Per il teorema 7.1 (usando il fatto che M, N sono infiniti) T_1 ha un modello M_1 di cardinalità κ e T_2 ha un modello M_2 di cardinalità κ. In particolare M_1, M_2 sono modelli di T di cardinalità κ quindi sono isomorfi per le ipotesi. Ne segue che $T_1 = T_2$ e $M \equiv N$. Quindi T è completa. □

Si può dimostrare che tutti gli ordini densi senza massimo e minimo elemento sono isomorfi a $(\mathbb{Q}, <)$. Ad esempio i razionali diadici sono isomorfi a $\mathbb{Q}$ come ordine (sebbene non sia semplice trovare un isomorfismo). Dal teorema precedente otteniamo:

Corollario 7.14. *La teoria degli ordini densi senza massimo e minimo elemento è completa.*

In modo analogo si dimostra la completezza della teoria dei campi algebricamente chiusi di caratteristica zero. Tale teoria è $\aleph_1$-categorica, e dunque completa.