# Logica Matematica
# 6.3 – Conseguenza Logica, Validità e Soddisfacibilità


Docenti: Alessandro Andretta e Luca Motto Ros

Dipartimento di Matematica
Università di Torino

# Alcune nozioni logiche

Sia $\varphi$ un $L$-enunciato.

- Se $\mathcal{A}$ è una $L$-struttura tale che $\mathcal{A} \models \varphi$ diciamo che $\varphi$ è **vero** nella struttura $\mathcal{A}$, o che $\mathcal{A}$ è un **modello** di $\varphi$, o che $\mathcal{A}$ **soddisfa** $\varphi$.
- Se esiste almeno una $L$-struttura $\mathcal{A}$ tale che $\mathcal{A} \models \varphi$, allora si dice che $\varphi$ è **soddisfacibile** o **coerente**.
- Se non esiste alcun modello di $\varphi$, si dice che $\varphi$ è **insoddisfacibile**, o **incoerente**, o **contradditorio**, o una **contraddizione**.
- Se per ogni $L$-struttura $\mathcal{A}$ si ha che $\mathcal{A} \models \varphi$, si dice che $\varphi$ è (**logicamente**) **valido**, o **logicamente vero**, o una **tautologia**, e si scrive
$$\models \varphi.$$

Queste nozioni si possono estendere anche ad insiemi di $L$-enunciati.

Sia $\Gamma$ un insieme (finito o infinito) di $L$-enunciati.

- Una $L$-struttura $\mathcal{A}$ è un **modello** di $\Gamma$, in simboli

$$\mathcal{A} \models \Gamma,$$

  se $\mathcal{A} \models \varphi$ per ogni $\varphi \in \Gamma$. In questo caso diciamo che $\Gamma$ è **soddisfatto** da $\mathcal{A}$, o che $\mathcal{A}$ **soddisfa** $\Gamma$.
- $\Gamma$ si dice **soddisfacibile** (o **coerente**) se $\mathcal{A} \models \Gamma$ *per qualche* $L$-struttura $\mathcal{A}$; in caso contrario, ovvero se $\mathcal{A} \not\models \Gamma$ per ogni $L$-struttura $\mathcal{A}$, si dice che $\Gamma$ è **insoddisfacibile** (o **incoerente**).
- $\Gamma$ si dice **valido** se $\mathcal{A} \models \Gamma$ *per ogni* $L$-struttura $\mathcal{A}$. In questo caso scriviamo $\models \Gamma$.

Si verifica facilmente che se $\Gamma = \{\varphi_1, \ldots, \varphi_n\}$ è un insieme finito di $L$-enunciati, allora $\Gamma$ è soddisfacibile/insoddisfacibile/valido se e solo l'enunciato $\varphi_1 \wedge \ldots \wedge \varphi_n$ è soddisfacibile/insoddisfacibile/valido.

**Osservazione.** Il numero di interpretazioni di una formula proposizionale è finito (ci sono $2^n$ possibili interpretazioni se la proposizione contiene $n$ lettere proposizionali): dunque si può controllare se essa è una tautologia, o se è insoddisfacibile considerando esplicitamente tutte le possibilità.

Di contro, non c'è limite al numero di $L$-strutture che possono soddisfare o meno un dato $L$-enunciato $\varphi$: dunque sarà in generale più facile dimostrare che $\varphi$ è soddisfacibile (basta trovare una struttura $\mathcal{A}$ tale che $\mathcal{A} \models \varphi$) piuttosto che dimostrare la sua validità o insoddisfacibilità (bisognerebbe controllare se *tutte* le $L$-strutture soddisfano o meno $\varphi$).

# Conseguenza logica

Sia $L$ un linguaggio, sia $\Gamma$ un insieme di $L$-enunciati e sia $\varphi$ un $L$-enunciato. Diremo che $\varphi$ è **conseguenza logica** di $\Gamma$, in simboli

$$\Gamma \models \varphi$$

se: per ogni $L$-struttura $\mathcal{A}$, se $\mathcal{A} \models \Gamma$ allora $\mathcal{A} \models \varphi$.

Scriveremo $\Gamma \not\models \varphi$ per dire che $\varphi$ NON è conseguenza logica di $\Gamma$.

Quando $\Gamma = \{\psi_1, \dots, \psi_n\}$ è un insieme finito scriveremo

$$\psi_1, \dots, \psi_n \models \varphi$$

invece di $\{\psi_1, \dots, \psi_n\} \models \varphi$, e se $\Gamma = \{\psi\}$ scriveremo semplicemente

$$\psi \models \varphi.$$

Inoltre si verifica facilmente che

$$\psi_1, \dots, \psi_n \models \varphi \qquad \text{se e solo se} \qquad \models (\psi_1 \wedge \dots \wedge \psi_n) \to \varphi.$$

## Attenzione!

Il simbolo $\models$ ha tre significati distinti:

- $\mathcal{A} \models \varphi$ (o $\mathcal{A} \models \varphi[\alpha]$), significa che $\mathcal{A}$ soddisfa $\varphi$ (mediante l'assegnazione $\alpha$); quindi $\models$ denota una relazione tra *strutture* e enunciati/formule (**relazione di soddisfazione**).
- $\models \varphi$ significa che $\varphi$ è un **enunciato valido**, ovvero una **tautologia**; quindi in questo caso $\models$ denota una *proprietà* che gli enunciati possono o non possono avere (quella di essere validi).
- $\Gamma \models \varphi$ significa che l'enunciato $\varphi$ è vero in ogni struttura in cui tutti gli enunciati in $\Gamma$ sono veri; quindi in questo caso $\models$ denota una relazione tra *insiemi di enunciati* e singoli enunciati (**relazione di conseguenza logica**).

Ragionando esattamente come nel caso della logica proposizionale, si dimostra il teorema seguente.

## Teorema

1. $\varphi$ è *valido se e solo se* $\neg\varphi$ è *insoddisfacibile.*
2. $\varphi$ è *soddisfacibile se e solo se* $\neg\varphi$ *non è valido,*
3. $\Gamma \models \varphi$ *se e solo se* $\Gamma \cup \{\neg\varphi\}$ è *insoddisfacibile.*

## Dimostrazione.

1 e 2 sono ovvie.

Dimostriamo che vale anche 3. Se $\Gamma \models \varphi$ e per assurdo $\mathcal{A} \models \Gamma \cup \{\neg\varphi\}$ per qualche $\mathcal{A}$, allora si avrebbe che, in particolare, $\mathcal{A} \models \neg\varphi$ e $\mathcal{A} \models \varphi$ (poiché $\mathcal{A} \models \Gamma$ e $\Gamma \models \varphi$), contraddizione.

Viceversa, supponiamo $\mathcal{A} \models \Gamma$. Se $\Gamma \cup \{\neg\varphi\}$ è insoddisfacibile, allora $\mathcal{A} \not\models \neg\varphi$, cioè $\mathcal{A} \models \varphi$. Poiché $\mathcal{A}$ è arbitrario, segue che $\Gamma \models \varphi$. $\square$

# Equivalenza logica

Sia $L$ un linguaggio. Due $L$-enunciati $\varphi$ e $\psi$ sono **logicamente equivalenti**, in simboli $\varphi \equiv \psi$, se

$$\mathcal{A} \models \varphi \qquad \text{se e solo se} \qquad \mathcal{A} \models \psi$$

per ogni struttura $\mathcal{A}$.

Scriveremo $\varphi \not\equiv \psi$ per dire che $\varphi$ e $\psi$ NON sono logicamente equivalenti.

Come nel caso della logica proposizionale, si ha che

$$\varphi \equiv \psi \qquad \text{se e solo se} \qquad \varphi \models \psi \text{ e } \psi \models \varphi$$

$$\varphi \equiv \psi \qquad \text{se e solo se} \qquad \models \varphi \leftrightarrow \psi$$

## Strutture numeriche

Quando venga richiesto di dimostrare che una certa formula $\varphi$ è soddisfacibile, si può tentare di trovare un modello di $\varphi$ che sia una struttura numerica "nota", ovvero una struttura che abbia come universo $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ o $\mathbb{R}$ e tale che i simboli del linguaggio di $\varphi$ vengano interpretati in relazioni e funzioni ben conosciute, come ad esempio i predicati unari "essere pari" o "essere dispari", le relazioni binarie $<$, $\geq$, ..., le funzioni somma, prodotto, elevamento a potenza, esponenziale o altre funzioni "semplici", e così via.

## Esempio

Sia $L = \{f\}$ con $f$ simbolo di funzione unario, e sia $\varphi$ l'enunciato

$$\forall y \exists x (f(x) = y).$$

Per mostrare che $\varphi$ è soddisfacibile, bisogna trovare una $L$-struttura $\mathcal{A}$ tale che $\mathcal{A} \models \varphi$.

Per fare in modo che $\varphi$ sia vero in $\mathcal{A}$, bisogna allora "scegliere" una funzione $f^{\mathcal{A}}$ tale che ogni elemento $y$ del dominio della struttura sia immagine mediante $f^{\mathcal{A}}$ di qualche elemento $x$.

Quindi si può considerare, ad esempio, la struttura $\mathcal{A} = \langle \mathbb{Z}, f^{\mathcal{A}} \rangle$ dove

$$f^{\mathcal{A}} \colon \mathbb{Z} \to \mathbb{Z}, \qquad x \mapsto x + 1.$$

Infatti, in $\mathcal{A}$ è vero che per ogni intero $y$ esiste un intero $x$ tale che $x + 1 = y$: basta prendere $x = y - 1$. Dunque $\mathcal{A} \models \varphi$ e abbiamo mostrato che $\varphi$ è soddisfacibile.

## Esempio (continua)

Se si fosse considerata al posto di $\mathcal{A}$ la struttura $\mathcal{B} = \langle \mathbb{N}, f^{\mathcal{B}} \rangle$, dove $f^{\mathcal{B}} \colon \mathbb{N} \to \mathbb{N}$ è nuovamente definita da $x \mapsto x + 1$, l'enunciato φ

$$\forall y \exists x (f(x) = y)$$

non sarebbe risultato vero in $\mathcal{B}$, poiché se si considera $y = 0$ non esiste nessun numero naturale $x$ tale che $x + 1 = y$. Dunque $\mathcal{B} \not\models \varphi$. Le due strutture $\mathcal{A}$ e $\mathcal{B}$ dimostrano in particolare che φ è soddisfacibile ma non valido.

Più in generale, si può osservare che per ogni $L$-struttura $\mathcal{M}$,

$\mathcal{M} \models \varphi$ se e solo se $f^{\mathcal{M}}$ è una funzione suriettiva.

## Esempio

Consideriamo ora il linguaggio $L = \{R\}$, dove $R$ è un simbolo di relazione binario, e sia $\varphi$ l'enunciato

$$\forall x \forall y (R(x,y) \rightarrow \exists z (\neg(z = x) \wedge \neg(z = y) \wedge (R(x,z) \wedge R(z,y)))).$$

Consideriamo la $L$-struttura $\mathcal{A} = \langle \mathbb{R}, < \rangle$ (ovvero la relazione binaria $R^{\mathcal{A}}$ su $\mathbb{R}$ è $<$). Allora l'"interpretazione" di $\varphi$ in $\mathcal{A}$ è: "per ogni coppia di numeri reali $x$ e $y$ tali che $x < y$ esiste una altro reale $z$ diverso da $x$ e da $y$ tale che $x < z < y$" (ovvero i numeri reali sono *densi* rispetto a $<$). Tale affermazione è vera in $\mathbb{R}$: dati $x$ e $y$ tali che $x < y$, basta prendere ad esempio $z = \frac{x+y}{2}$. Quindi $\mathcal{A} \models \varphi$.

Invece $\varphi$ è falsa nella $L$-struttura $\mathcal{B} = \langle \mathbb{Z}, < \rangle$, poiché se si considera $y = x + 1$ si ha che $x < y$ ma non esiste nessun intero tra $x$ e $y$ che sia diverso da entrambi. Dunque $\varphi$ è nuovamente soddisfacibile ma non valido.

## Esempio

Sia ora $L = \{+, \cdot, 0, 1\}$ un linguaggio dove $+$ e $\cdot$ sono simboli di funzione binari e $0$ e $1$ sono simboli di costante. Sia $\mathcal{A} = \langle \mathbb{R}, +, \cdot, 0, 1\rangle$ una $L$-struttura (ovvero si interpreti il simbolo $+$ come l'usuale somma tra numeri reali, $\cdot$ come il prodotto, $0$ come il numero reale $0$ e $1$ come il numero reale $1$). Per comodità, utilizzeremo la notazione *infissa*, ovvero scriveremo $x + y$ al posto di $+(x, y)$ e $x \cdot y$ al posto di $\cdot(x, y)$.

Sia φ l'enunciato

$$\forall x \exists y (1 + x \cdot x = y).$$

L'"interpretazione" di φ in $\mathcal{A}$ dice che per ogni reale $x$ deve esistere un reale $y$ tale che $x^2 + 1 = y$: questo è vero in $\mathbb{R}$, dunque $\mathcal{A} \models \varphi$.

Sia ora ψ l'enunciato

$$\forall y \exists x (1 + x \cdot x = y).$$

In questo caso, ψ è falsa in $\mathcal{A}$ poiché se si considera $y = 0$ allora non esiste nessun $x$ tale che $x^2 + 1 = y$. Dunque $\mathcal{A} \not\models \psi$.

## Esempio

Consideriamo il linguaggio $L = \{R\}$ con $R$ simbolo di relazione binario. Consideriamo i seguenti enunciati:

$$\begin{aligned}
\varphi_1 :&\quad \forall x R(x,x)\\
\varphi_2 :&\quad \forall x \forall y (R(x,y) \to R(y,x))\\
\varphi_3 :&\quad \forall x \forall y \forall z (R(x,y) \wedge R(y,z) \to R(x,z).
\end{aligned}$$

Allora per ogni $L$-struttura $\mathcal{A}$ si ha che

$$\begin{aligned}
\mathcal{A} \models \varphi_1 &\quad \text{se e solo se} \quad R^{\mathcal{A}} \text{ è una relazione riflessiva;}\\
\mathcal{A} \models \varphi_2 &\quad \text{se e solo se} \quad R^{\mathcal{A}} \text{ è una relazione simmetrica;}\\
\mathcal{A} \models \varphi_3 &\quad \text{se e solo se} \quad R^{\mathcal{A}} \text{ è una relazione transitiva.}
\end{aligned}$$

Quindi $\mathcal{A} \models \varphi_1 \wedge \varphi_2 \wedge \varphi_3$ se e solo se $R^{\mathcal{A}}$ è una relazione di equivalenza.

...continua

## Esempio (continua)

Siano $L$ e $\varphi_1, \varphi_2, \varphi_3$ come nella slide precedente. Dimostriamo che nessuna delle $\varphi_i$ è conseguenza logica delle rimanenti due, ovvero

$$\{\varphi_2, \varphi_3\} \not\models \varphi_1$$
$$\{\varphi_1, \varphi_3\} \not\models \varphi_2$$
$$\{\varphi_1, \varphi_2\} \not\models \varphi_3$$

Dobbiamo trovare per ogni $1 \leq i \leq 3$ una $L$-struttura $\mathcal{A}_i$ tale che $\mathcal{A}_i \models \varphi_j$ per ogni $j \neq i$ ma $\mathcal{A}_i \not\models \varphi_i$. Allora basta considerare:

- $\mathcal{A}_1 = \langle A, \emptyset \rangle$, ovvero una struttura con dominio un insieme non vuoto e $R^{\mathcal{A}_1}$ la relazione vuota;
- $\mathcal{A}_2 = \langle \mathbb{N}, \leq \rangle$ o più in generale, un qualunque ordine (non banale);
- $\mathcal{A}_3 = \langle \mathbb{Z}, R^{\mathcal{A}_3} \rangle$ dove per ogni $k, l \in \mathbb{Z}$

$$R^{\mathcal{A}_3}(k, l) \quad \text{se e solo se} \quad |k - l| \leq 1.$$

# Ripasso...

- Per dimostrare che un enunciato $\varphi$ è **soddisfacibile** bisogna trovare una struttura $\mathcal{A}$ tale che $\mathcal{A} \models \varphi$.
- Per dimostrare che un enunciato $\varphi$ **NON è valido** bisogna trovare una struttura $\mathcal{A}$ tale che $\mathcal{A} \not\models \varphi$ (equivalentemente, $\mathcal{A} \models \neg\varphi$).
- Per dimostrare che un enunciato $\varphi$ **NON è conseguenza logica** di un insieme di enunciati $\Gamma$bisogna trovare una struttura $\mathcal{A}$ tale che $\mathcal{A} \models \Gamma$ ma $\mathcal{A} \not\models \varphi$. In particolare, per dimostrare che

  $$\psi_1, \ldots, \psi_n \not\models \varphi$$

  bisogna trovare una struttura $\mathcal{A}$ tale che

  $$\mathcal{A} \models \psi_1 \wedge \ldots \wedge \psi_n \wedge \neg\varphi.$$

- Per dimostrare che due enunciati $\varphi$ e $\psi$ **NON sono logicamente equivalenti**, ovvero che $\varphi \not\equiv \psi$, bisogna trovare una struttura $\mathcal{A}$ tale che $\mathcal{A} \models \varphi \wedge \neg\psi$ oppure $\mathcal{A} \models \psi \wedge \neg\varphi$.

### Esercizio

Sia $L = \{f\}$ con $f$ simbolo di funzione binario e $\varphi$ l'enunciato

$$\forall x \exists y \forall z (f(f(x,y),z) = z).$$

Dimostrare che $\varphi$ è soddisfacibile ma non è valido.

Basta osservare che $\langle \mathbb{Z}, + \rangle \models \varphi$ ma $\langle \mathbb{N}, + \rangle \not\models \varphi$.

### Esercizio per casa

È vero che $\langle \mathbb{Q}, \cdot \rangle \models \varphi$?

### Esercizio

Sia $L = \{R\}$ con $R$ simbolo di relazione binario. Dimostrare che

$$\forall x \exists y R(x, y) \not\models \exists y \forall x R(x, y).$$

Bisogna dimostrare che esiste una $L$-struttura $\mathcal{A}$ tale che $\mathcal{A} \models \forall x \exists y R(x, y)$ ma $\mathcal{A} \not\models \exists y \forall x R(x, y)$, ovvero $\mathcal{A} \models \neg \exists y \forall x R(x, y)$.

Basta allora considerare $\mathcal{A} = \langle \mathbb{N}, \leq \rangle$.

## Esercizio

Sia $L = \{P, Q\}$ con $P$ e $Q$ simboli di relazione unari. Dimostrare che

$$\exists x(P(x) \to Q(x)) \not\models \exists x P(x) \to \exists x Q(x).$$

Bisogna trovare una $L$-struttura $\mathcal{A}$ tale che

$$\mathcal{A} \models \exists x(P(x) \to Q(x)) \quad \text{ma} \quad \mathcal{A} \not\models \exists x P(x) \to \exists x Q(x).$$

La condizione $\mathcal{A} \models \exists x(P(x) \to Q(x))$ equivale a $\mathcal{A} \models \exists x(\neg P(x) \vee Q(x))$, mentre la condizione $\mathcal{A} \not\models \exists x P(x) \to \exists x Q(x)$ equivale a $\mathcal{A} \models \exists x P(x)$ ma $\mathcal{A} \models \neg \exists x Q(x)$. Per l'ultima condizione, nessun $x$ deve avere la proprietà $Q$. Quindi se si deve avere $\mathcal{A} \models \exists x(\neg P(x) \vee Q(x))$ bisogna che ci sia qualche $x$ per cui non vale $P$. D'altra parte se deve essere vero che $\mathcal{A} \models \exists x P(x)$, vuol dire che ci deve essere qualche $x$ per cui vale $P$. Quindi $\mathcal{A} = \langle A, P^{\mathcal{A}}, Q^{\mathcal{A}} \rangle$ deve essere tale che

$$Q^{\mathcal{A}} = \emptyset \qquad P^{\mathcal{A}} \neq A \qquad P^{\mathcal{A}} \neq \emptyset.$$

Basta allora porre $\mathcal{A} = \langle A, P^{\mathcal{A}}, Q^{\mathcal{A}} \rangle$ con

$$A = \mathbb{N} \qquad P^{\mathcal{A}} = \mathbb{N} \setminus \{0\} \qquad Q^{\mathcal{A}} = \emptyset.$$

## Esercizio

Sia $L = \{f, c\}$ con $f$ simbolo di funzione binario e $c$ simbolo di costante. Trovare un $L$-enunciato φ tale che

$$\langle \mathbb{N}, \cdot, 17 \rangle \models \varphi \quad \text{ma} \quad \langle \mathbb{N}, \cdot, 12 \rangle \not\models \varphi.$$

Osserviamo subito che $17$ è un numero primo mentre $12$ non lo è. Bisogna allora cercare di trovare un $L$-enunciato che dica

$$c \text{ è un numero primo,}$$

ovvero

$$\text{per ogni } x \text{ e } y, \text{ se } x \cdot y = c \text{ allora } x = 1 \text{ oppure } y = 1.$$

L'espressione "$x = 1$" può essere resa, nel linguaggio dato, con

$$\forall z (f(x, z) = z),$$

e similmente per "$y = 1$". Allora φ può essere l'enunciato

$$\forall x \forall y \Big( f(x, y) = c \rightarrow \forall z (f(x, z) = z) \vee \forall z (f(y, z) = z) \Big).$$

## Esercizio

Sia $L = \{R, f, c\}$ con $R$ simbolo di relazione binario, $f$ simbolo di funzione binario e $c$ simbolo di costante. Dimostrare che l'enunciato $\varphi$

$$\forall x R(f(x,x), c)$$

è soddisfacibile ma non valido.

Si ha

$$\langle \mathbb{R}, \geq, \cdot, 0 \rangle \models \varphi$$

ma

$$\langle \mathbb{R}, \leq, \cdot, 0 \rangle \not\models \varphi.$$

**Esercizio**

Sia $L = \{R\}$ con $R$ simbolo di relazione binario. Determinare per quali $1 \leq k \leq 10$ si ha che

$$\langle \mathrm{Div}(k), | \rangle \models \forall x \forall y (R(x,y) \vee R(y,x)).$$

Si ha che $\langle \mathrm{Div}(k), | \rangle \models \forall x \forall y (R(x,y) \vee R(y,x))$ se e solo se $|$ è un ordine lineare su $\mathrm{Div}(k)$. Questo è vero se solo se nella scomposizione in fattori primi di $k$ compare *un solo* numero primo, ovvero se e solo se $k = p^n$ con $p$ primo e $n \in \mathbb{N}$.

Quindi $\langle \mathrm{Div}(k), | \rangle \models \forall x \forall y (R(x,y) \vee R(y,x))$ per $k \in \{1, 2, 3, 4, 5, 7, 8, 9\}$.