

Informatica

CdL in Matematica

Parte 2

Roberto Zunino

Logica di base: connettivi e dimostrazioni

Connettivi Logici: and,or,implica

\wedge	“e” / “and”
\vee	“o” / “or”
\rightarrow / \implies	“implica”

Significato intuitivo:

$p \wedge q$ indica che vale sia p che q .

$p \vee q$ indica che vale p oppure q (possibilmente entrambe).

$p \implies q$ indica che se vale p allora vale anche q .

Esempio 1

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

Informalmente, esprime il seguente fatto: supponendo che valga p o che valgano entrambe p e q , si può concludere che vale p .

L'intuizione ci dice che la formula di sopra vale sempre, qualunque siano p e q .

Esempio 2

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

Informalmente, esprime il seguente fatto: supponendo che valga almeno una tra p o q , e anche che, se p vale, allora vale anche q , si può concludere che vale q .

L'intuizione ci dice che la formula di sopra vale sempre.

Dimostrazioni

Vediamo ora qualche regola per dimostrare una formula.

Una formula dimostrabile viene chiamata **teorema**.

Nota. All'esame **non** vi verrà richiesto di usare queste regole formali per le vostre dimostrazioni, ma dovete **comunque** sapere produrre dimostrazioni corrette, così come per gli altri corsi.

In Informatica capita spesso che ci siano “tante” formule in gioco (per es., tante ipotesi), quindi è fondamentale abituarsi a maneggiarle con disciplina.

Mentre si scrive una dimostrazione, ad ogni singolo punto intermedio, bisogna tenere traccia di:

- un insieme Γ (“gamma”) di formule dette *ipotesi*, che rappresentano le proprietà che sappiamo valere
- una singola formula t detta *tesi*, che rappresenta la proprietà che rimane ancora da dimostrare

$$\text{ipotesi } \Gamma \left\{ \begin{array}{l} IP1 : p_1 \\ \dots \\ IPn : p_n \\ \hline \hline \text{tesi} : t \end{array} \right.$$

Regola base

FUORI
ESAME

Una regola banale di base:


Base Se la tesi t è presente nelle ipotesi, possiamo chiudere la dimostrazione qui.

Nell'uso comune:

... Resta quindi da dimostrare p , che vale per ipotesi. C.V.D.

altre ipotesi (non usate) $\longrightarrow \Gamma$

$$\frac{IP1 : t}{\text{tesi} : t}$$

 Fine della dimostrazione

Ogni connettivo \wedge, \vee, \implies ha associata una regola di introduzione e una di eliminazione.

Introduzione Si “affronta” direttamente la tesi, osservando da quale connettivo logico è formata, e chiedendosi che cosa bisogna fare per dimostrare quel connettivo.

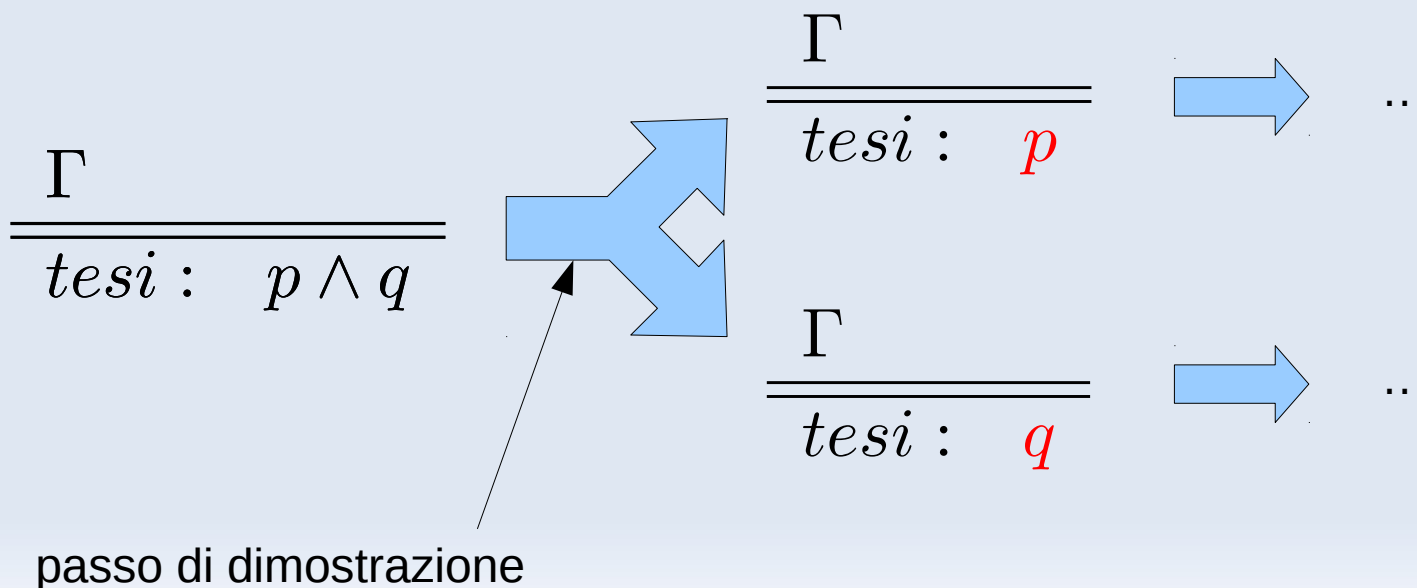
Eliminazione Si “sfrutta” una delle ipotesi, osservando da quale connettivo logico è formata, e ricavandone informazioni.

And - Introduzione

FUORI
ESAME

Introduzione Per dimostrare una tesi $p \wedge q$, è sufficiente fare due dimostrazioni, una per p e una per q . In entrambe si possono usare le stesse ipotesi.

... Dobbiamo fare vedere che vale $p \wedge q$. Per la parte p si ha che Per la parte q si ha che C.V.D.



And - Eliminazione

FUORI
ESAME

Eliminazione Per usare un'ipotesi $p \wedge q$, basta aggiungere sia p che q all'insieme delle ipotesi.

... Per ipotesi si ha $p \wedge q$. Quindi assumiamo sia p che q . Da questo ...

$$\frac{\Gamma}{\frac{IP1 : p \wedge q}{tesi : t}} \quad \longrightarrow \quad \frac{\Gamma}{\frac{IP1 : p \wedge q}{\frac{IP2 : p}{IP3 : q}}}{tesi : t} \quad \longrightarrow \quad \dots$$

Esercizio Assumendo per ipotesi $p \wedge (q \wedge r)$, dimostrate la tesi $r \wedge p$.

Or - Introduzione

FUORI
ESAME

Introduzione Per dimostrare una tesi $p \vee q$, è sufficiente sceglierne un lato, e dimostrare solo quello.

... Dobbiamo fare vedere che vale $p \vee q$. Basta quindi che valga p . Questo deriva da C.V.D.

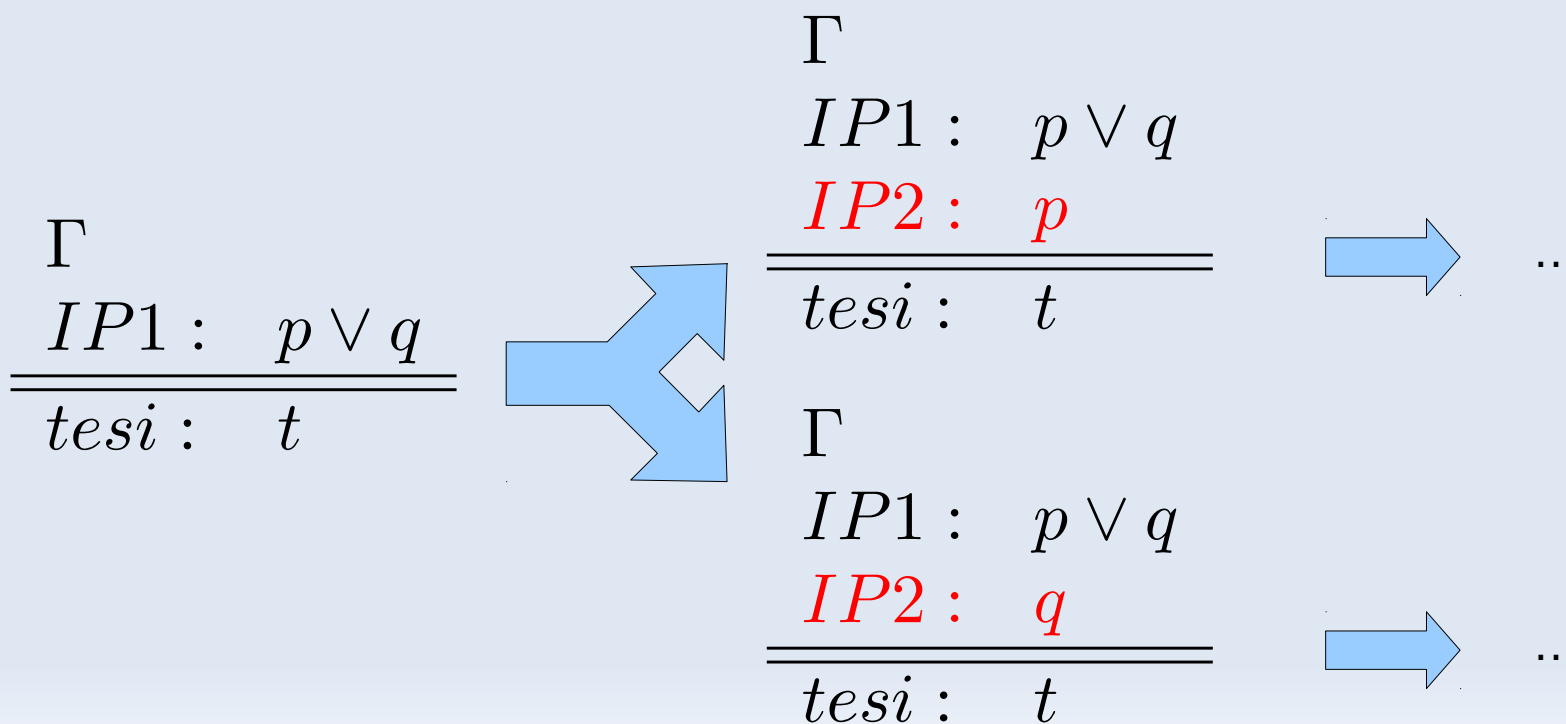
$$\frac{\Gamma}{\text{tesi : } p \vee q} \quad \longrightarrow \quad \frac{\Gamma}{\text{tesi : } p} \quad \longrightarrow \quad \dots$$

(alternativamente, si poteva scegliere q)

Or - Eliminazione

Eliminazione Per usare un'ipotesi $p \vee q$, si procede per casi, facendo due dimostrazioni. Nella prima si considera il caso in cui vale p , aggiungendola come ipotesi. Nella seconda si considera il caso in cui vale q .

... Per ipotesi si ha $p \vee q$. Se vale p , la tesi t deriva da Se vale q la tesi t deriva da



Esercizio Assumendo per ipotesi che valga $p \vee q$ si dimostri $q \vee p$.

Esercizio Assumendo per ipotesi che valga $(p \wedge q) \vee (p \wedge r)$ si dimostri $p \wedge (q \vee r)$.

Implica - Introduzione

FUORI
ESAME

Introduzione Per dimostrare una tesi $p \implies q$, è sufficiente assumere p , aggiungendola alle ipotesi, e dimostrare la nuova tesi q .

...Dobbiamo fare vedere che vale $p \implies q$.
Assumiamo p . La tesi q deriva da C.V.D.

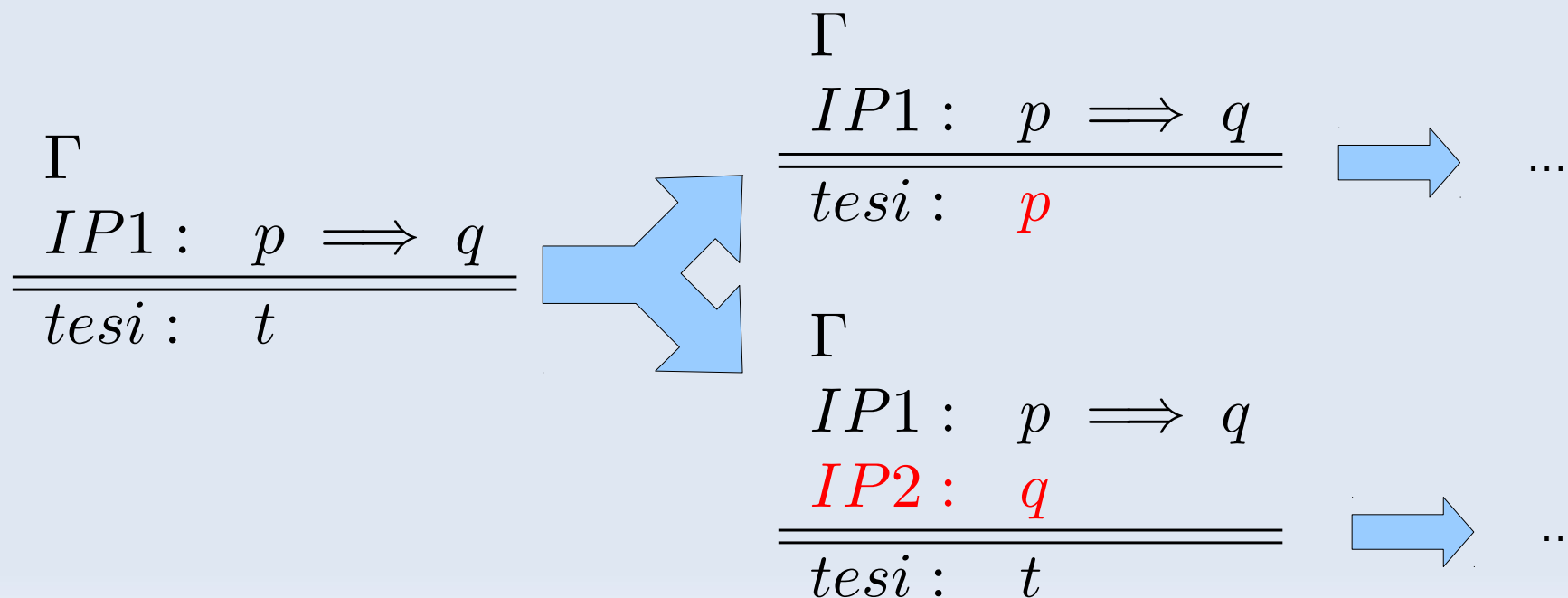
$$\frac{\Gamma}{\text{tesi : } p \implies q} \quad \longrightarrow \quad \frac{\Gamma}{\text{IP1 : } p} \quad \longrightarrow \quad \frac{\Gamma}{\text{tesi : } q} \quad \longrightarrow \quad \dots$$

Implica - Eliminazione

FUORI
ESAME

Eliminazione Per usare un'ipotesi $p \implies q$, bisogna fare due dimostrazioni. Nella prima, bisogna ricavare p come tesi. Nella seconda si aggiunge q alle ipotesi, e si continua (con la tesi originale t).

... Per ipotesi si ha $p \implies q$. Tuttavia, p vale siccome Quindi vale anche q . Quindi



Esercizi

Esercizio. Dimostrare le formule seguenti

$$(p \wedge q) \implies (q \wedge p)$$

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

$$((p \implies q) \wedge (q \implies r)) \implies (p \implies r)$$

$$((p \wedge q) \implies r) \implies (p \implies (q \implies r))$$

$$(p \implies (q \implies r)) \implies ((p \wedge q) \implies r)$$

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

$$(p \implies (q \implies r)) \implies ((p \implies q) \implies (p \implies r))$$

“Se e solo se”

Def. $p \iff q$ (“ p se e solo se q ”, o anche “ p è equivalente a q ”) sta per

$$(p \implies q) \wedge (q \implies p)$$

Esercizio. Dimostrare che

$$(p \implies q) \iff (p \implies (p \wedge q))$$

Esercizio. Dimostrare l'implicazione

$$\begin{aligned} & ((p \implies q) \wedge (q \implies r) \wedge (r \implies p)) \\ & \implies \\ & ((p \iff q) \wedge (q \iff r) \wedge (r \iff p)) \end{aligned}$$

Introduzione Una tesi $t = \text{vero}$ vale sempre.

Eliminazione (Non c'è per vero)

$$\frac{\Gamma}{\text{tesi} : \text{vero}}$$
  Fine della dimostrazione

Esercizio: dimostrare che

$$p \iff (p \wedge \text{vero})$$
$$\text{vero} \iff (p \vee \text{vero})$$

Introduzione (Non c'è per falso)

Eliminazione Un'ipotesi falso consente di concludere immediatamente la dimostrazione, qualunque sia la tesi t .

$$\frac{\Gamma \quad IP1 : \text{falso}}{\text{tesi} : t} \quad \checkmark \quad \text{Fine della dimostrazione}$$

Esercizio: dimostrare

$$p \iff (p \vee \text{falso})$$
$$\text{falso} \iff (p \wedge \text{falso})$$

Negazione

FUORI
ESAME

La negazione $\neg p$ è definibile come

$$p \iff \text{falso}$$

Siccome $\text{falso} \implies p$ vale sempre, possiamo equivalentemente definire $\neg p$ come

$$p \implies \text{falso}$$

Spesso l'introduzione è resa come:

Dobbiamo fare vedere che vale $\neg p$. Assumiamo p e ricaviamo un assurdo. ... C.V.D.

Esercizi

Esercizio. Dimostrare che $\neg(p \wedge \neg p)$.

Esercizio. Dimostrare che

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

La seconda implicazione è la “contrapositiva” della prima.

Il “Taglio”

FUORI
ESAME

Nelle dimostrazioni è possibile introdurre dei risultati intermedi prima di procedere a dimostrare la tesi.

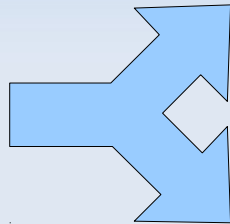
Taglio Alle ipotesi Γ possiamo aggiungere qualunque formula p che si derivi da esse, e continuare a dimostrare la tesi t .

Dobbiamo dimostrare t . Facciamo intanto vedere che p vale. ... quindi p vale. Sfruttando questo, proseguiamo a dimostrare t

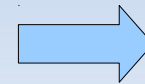
Il “Taglio”

FUORI
ESAME

$$\frac{\Gamma}{\text{tesi} : t}$$

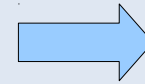


$$\frac{\Gamma}{\text{tesi} : p}$$



...

$$\frac{\Gamma}{\text{IP1} : p}$$
$$\frac{\text{IP1} : p}{\text{tesi} : t}$$



...

Terzo Escluso

FUORI
ESAME

Terzo Escluso In una dimostrazione possiamo sempre aggiungere $p \vee \neg p$ tra le ipotesi.

Questa regola ci consente di prendere una qualunque proprietà p e considerare i casi “ p vera” e “ p falsa”.

$$\frac{\Gamma}{\text{tesi} : t} \quad \longrightarrow \quad \frac{\Gamma}{\text{IP1} : p \vee \neg p} \quad \longrightarrow \quad \dots$$

Curiosità: le regole del connettivo \vee viste prima non sono sufficienti a dimostrare la legge del terzo escluso.

Esercizi

Esercizio. Dimostrare $\neg\neg p \iff p$

Esercizio. Dimostrare che

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

Da questo e dall'analogo esercizio precedente segue che ogni implicazione è equivalente alla sua contrappositiva.

Esercizi

Esercizio. Dimostrare le seguenti (anche in modo più informale rispetto alle regole viste prima).

$$\neg(p \vee q) \iff (\neg p \wedge \neg q) \quad \text{DeMorgan}$$

$$\neg(p \wedge q) \iff (\neg p \vee \neg q) \quad \text{DeMorgan}$$

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

$$\neg(p \implies q) \iff (p \wedge \neg q)$$

$$((p \vee q) \wedge r) \iff ((p \wedge r) \vee (q \wedge r)) \quad \text{distributiva}$$

$$((p \wedge q) \vee r) \iff ((p \vee r) \wedge (q \vee r)) \quad \text{distributiva}$$

Riscrittura di formule

Quando $p \iff q$ vale, è possibile rimpiazzare p con q (e viceversa) all'interno di formule più grandi, mantenendole equivalenti. Infatti in tal caso si ha (esercizio):

$$\begin{aligned}(p \wedge r) &\iff (q \wedge r) \\(p \vee r) &\iff (q \vee r) \\(p \implies r) &\iff (q \implies r) \\(r \implies p) &\iff (r \implies q) \\&\dots\end{aligned}$$

A volte, per dimostrare una formula, è comodo potere alternare passaggi di “riscrittura equivalente” a passaggi di introduzione/eliminazione.

Tabelle di verità

I connettivi logici si possono anche definire in base alla loro *tabella di verità*, che associa ad essi un valore di verità vero o falso, in base a quello dei loro argomenti.

p	q	$p \wedge q$	$p \vee q$	$p \implies q$	$\neg p$
F	F	F	F	V	V
F	V	F	V	V	V
V	F	F	V	F	F
V	V	V	V	V	F

Queste tabelle vengono usate dai calcolatori, ma sono pressoché inutilizzate nelle dimostrazioni, in quanto piuttosto scomode da usare.

Uguaglianza

FUORI
ESAME

Introduzione Se la tesi ha la forma $a = a$, dove a è un'espressione arbitraria, possiamo concludere la dimostrazione.

Eliminazione Se un'ipotesi ha la forma $a = b$, dove a, b sono espressioni arbitrarie, possiamo sostituire una qualunque occorrenza di a con b , sia nelle altre ipotesi che nella tesi.

Esercizio. Dimostrate che l'uguaglianza è transitiva attenendovi precisamente alle regole di sopra.

Esercizio

Esercizio. L'equazione

$$x = \begin{cases} 5 & \text{se } y = 0 \\ 7 & \text{se } y \neq 0 \end{cases}$$

si può anche esprimere come

$$(y = 0 \implies x = 5) \wedge (y \neq 0 \implies x = 7)$$

e anche come

$$(y = 0 \wedge x = 5) \vee (y \neq 0 \wedge x = 7)$$

Dimostrare (informalmente) che sono due modi equivalenti.

Logica di base: quantificatori e dimostrazioni

Quantificatori

\forall “per ogni”

$$\forall x. x > 5 \implies x \neq 0$$

\exists “esiste almeno un”

$$\exists x. x > 5 \wedge x < 10$$

Notazione “compatta” per i quantificatori ripetuti:

$$(\forall a, \dots, z. p(a, \dots, z)) \iff (\forall a. \dots (\forall z. p(a, \dots, z)))$$

e analoga per \exists .

Per ogni - Introduzione

FUORI
ESAME

Introduzione Per dimostrare una tesi $\forall x. p(x)$, è sufficiente prendere una variabile non usata altrove y e dimostrare la nuova tesi $p(y)$.

Dobbiamo dimostrare $\forall x. p(x)$. Dato y un valore arbitrario, facciamo vedere che $p(y)$ vale.
...C.V.D.

(Spesso si sceglie x stessa come variabile “non usata”)

$$\frac{\Gamma}{\text{tesi : } \forall x. p(x)} \quad \longrightarrow \quad \frac{\Gamma}{\text{tesi : } p(y)} \quad \longrightarrow \quad \dots$$

Per ogni - Eliminazione

FUORI
ESAME

Eliminazione Per usare un'ipotesi $\forall x. p(x)$, si aggiunge $p(e)$ alle ipotesi, dove e è un'espressione scelta a piacere.

Sappiamo che vale $\forall x. p(x)$ per ipotesi. Quindi possiamo dedurre che $p(n + 2 - k)$. Sfruttando ciò, si ha che la tesi t segue da ...

$$\frac{\Gamma \quad IP1 : \forall x. p(x)}{\text{tesi} : t} \quad \Rightarrow \quad \frac{\Gamma \quad IP1 : \forall x. p(x) \quad IP2 : p(n + 2 - k)}{\text{tesi} : t} \quad \Rightarrow \quad \dots$$

Esercizi

Sia p un predicato (una proprietà) e f una funzione.

Esercizio. Dimostrare che

$$(\forall x. p(x)) \wedge q \implies (\forall x. p(x) \wedge q)$$

Esercizio. Dimostrare che

$$(\forall x. p(x) \implies p(f(x))) \implies (\forall x. p(x) \implies p(f(f(x))))$$

Esempi

$$(\forall x. \forall y. p(x, y)) \iff (\forall y. \forall x. p(x, y))$$

$$(\forall x. p(x) \wedge q(x)) \iff (\forall x. p(x)) \wedge (\forall x. q(x))$$

$$(\forall x. p(x) \vee q(x)) \not\Rightarrow (\forall x. p(x)) \vee (\forall x. q(x))$$

Esiste - Introduzione

FUORI
ESAME

Introduzione Per dimostrare una tesi $\exists x. p(x)$, è sufficiente dimostrare $p(e)$, dove e è un'espressione scelta a piacere.

Dobbiamo dimostrare $\exists x. p(x)$. Per farlo, facciamo vedere che $p(n^2 - k)$ vale. ... C.V.D.

$$\frac{\Gamma}{\text{tesi : } \exists x. p(x)} \quad \longrightarrow \quad \frac{\Gamma}{\text{tesi : } p(n^2 - k)} \quad \longrightarrow \quad \dots$$

Esiste - Eliminazione

FUORI
ESAME

Eliminazione Per usare un'ipotesi $\exists x. p(x)$, si aggiunge $p(y)$ alle ipotesi, dove y è una variabile non usata altrove.

Sappiamo che vale $\exists x. p(x)$ per ipotesi. Quindi possiamo supporre che $p(y)$ per un y opportuno. Sfruttando ciò, si ha che la tesi t segue da ...

(Spesso si sceglie x stessa come variabile “non usata”)

$$\frac{\Gamma \quad IP1 : \exists x. p(x)}{\text{tesi} : t} \quad \longrightarrow \quad \frac{\Gamma \quad IP1 : \exists x. p(x) \quad IP2 : p(y)}{\text{tesi} : t} \quad \longrightarrow \quad \dots$$

Esercizi

Esercizio Usando liberamente le proprietà usuali dell'aritmetica, dimostrare che: (sotto, x, y sono numeri naturali)

$$\forall x. \exists y. y > x$$

$$\nexists y. \forall x. y > x$$

$$\exists x. \forall y. x = y \vee y > x$$

Potete usare, per esempio, che

$$\forall x. (x \neq 0 \iff x > 0)$$

$$\forall x. \neg(x > x)$$

Esercizi

Esercizio Osservate che in una dimostrazione di

$$(\exists x. p(x)) \implies (\exists y. q(y))$$

il valore di y viene scelto da chi dimostra, ma il valore di x no. Infatti, $\exists y$ viene introdotto mentre $\exists x$ viene eliminato. “Scegliere” anche il valore di x è un errore grave, da evitare con cura.

Come vengono scelte x, y quando si dimostra la seguente?

$$(\forall x. p(x)) \implies (\forall y. q(y))$$

Quantificatori: esempi

De Morgan:

$$\begin{aligned}\neg(\forall x. p(x)) &\iff (\exists x. \neg p(x)) \\ \neg(\exists x. p(x)) &\iff (\forall x. \neg p(x))\end{aligned}$$

Quantificatori: esempi

Esercizio. Dimostrate che, se vale

$$\forall x. p(x) \iff q(x)$$

allora valgono

$$\begin{array}{l} 1) \quad (\forall x.p(x)) \iff (\forall x.q(x)) \\ 2) \quad (\exists x.p(x)) \iff (\exists x.q(x)) \end{array}$$

Questa proprietà consente di riscrivere le formule in modo equivalente sotto i quantificatori.

Quantificatori: esempi

Esercizio. Giustificare informalmente.

(p non dipende da x)

$$(p \vee (\forall x. q(x))) \iff (\forall x. p \vee q(x))$$

$$(p \wedge (\forall x. q(x))) \iff (\forall x. p \wedge q(x))$$

$$(p \vee (\exists x. q(x))) \iff (\exists x. p \vee q(x))$$

$$(p \wedge (\exists x. q(x))) \iff (\exists x. p \wedge q(x))$$

Suggerimento: se p è vero..., se è falso...

Quantificatori: esempi

Esercizio. Giustificare riscrivendo \implies usando \forall .

$$(p \implies (\forall x. q(x))) \iff (\forall x. p \implies q(x))$$

$$(p \implies (\exists x. q(x))) \iff (\exists x. p \implies q(x))$$

$$((\forall x. p(x)) \implies q) \iff (\exists x. p(x) \implies q)$$

$$((\exists x. p(x)) \implies q) \iff (\forall x. p(x) \implies q)$$

Notate come negli ultimi due casi \forall e \exists si “scambiano”. Intuitivamente, questo è legato al fatto che $a \implies b$ è equivalente a $(\neg a) \vee b$, quindi l’antecedente di una implicazione è “sotto una negazione”, che per De Morgan scambia i quantificatori.

Esercizio

Questa formula (o una sua generalizzazione con più variabili) verrà usata frequentemente nel resto del corso.

Esercizio Dimostrate che la formula

$$\forall x, y, z. p(x, y) \wedge q(y, z) \implies r(x, y, z)$$

si può riscrivere in modo equivalente come

$$\forall x, y. p(x, y) \implies (\forall z. q(y, z) \implies r(x, y, z))$$

“Esiste un unico ...”

$\exists!$ “esiste esattamente un”

$$\exists!x. x \geq 4 \wedge x \leq 4$$

Quantificatori

Esercizio. Convincetevi che $\exists!x. p(x)$ si può formalizzare come

$$(\exists x. p(x)) \wedge (\forall x, y. p(x) \wedge p(y) \implies x = y)$$

La prima parte garantisce l'*esistenza*, la seconda l'*unicità*.

Dimostrate (in modo informale ma preciso) che la formula di sopra è equivalente a

$$\exists x. \forall y. (p(y) \iff y = x)$$

Esercizi

Esercizio. Formalizzate gli asserti

“quando gioca Mario facciamo sempre 3 reti”

“ho 2 chiavi ma nessuna apre la porta”

“tutte le volte che premo il tasto 1 con la spia rossa spenta, tale spia si accende”

Insiemistica di base

Insiemistica (“ingenua”)

Notazione per gli insiemi

$$A = \{x \mid x \text{ soddisfa una qualche proprietà}\}$$

Appartenenza: un valore appartiene all’insieme se e solo se ne soddisfa la proprietà

$$a \in \{x \mid p(x)\} \iff p(a)$$

Estensionalità: due insiemi con gli stessi elementi sono ugali

$$(\forall x. x \in A \iff x \in B) \implies A = B$$

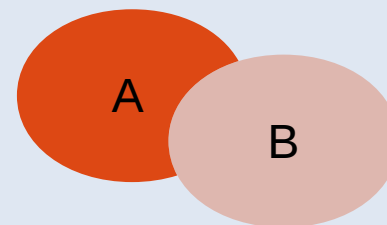
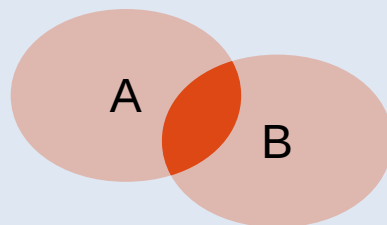
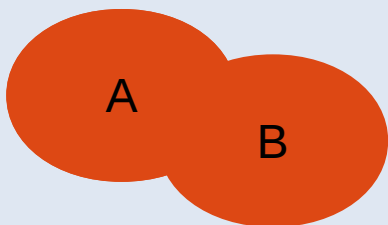
Operazioni su Insiemi

Unione, intersezione, differenza

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}$$



Enumerazioni

Insieme vuoto

$$\emptyset = \{x \mid \text{falso}\} = \{x \mid x \neq x\} = \{x \mid 5 < 4\}$$

Insieme singolo

$$\{a\} = \{x \mid x = a\}$$

Insieme enumerato

$$\{a_1, \dots, a_n\} = \{x \mid x = a_1 \vee \dots \vee x = a_n\} = \{a_1\} \cup \dots \cup \{a_n\}$$

Esercizio. È vera la seguente?

$$\exists a, b, c. \{a, b\} = \{c\}$$

Quantificatori

Altre forme:

$$\begin{aligned}(\forall x \in A. p(x)) &\iff (\forall x. x \in A \implies p(x)) \\(\exists x \in A. p(x)) &\iff (\exists x. x \in A \wedge p(x))\end{aligned}$$

Conseguentemente:

$$\begin{aligned}(\forall x \in \emptyset. p(x)) &\iff \text{vero} \\(\exists x \in \emptyset. p(x)) &\iff \text{falso}\end{aligned}$$

Immagine

La notazione

$$A = \{f(x) \mid p(x)\}$$

indica

$$A = \{z \mid \exists x. z = f(x) \wedge p(x)\}$$

Esempio.

$$A = \{x^2 \mid x \in \mathbb{Z} \wedge -2 \leq x \leq 4\} = \{0, 1, 4, 9, 16\}$$

Notate che i numeri $1, 4 \in A$ sono “generati” da due valori di x ciascuno, ovvero $\pm 1, \pm 2$, mentre i numeri $0, 9, 16$ sono “generati” da solo un valore di x , ovvero $0, 3, 4$.

Immagine

Esercizio. Sia A un insieme arbitrario.

Sono vere le seguenti?

$$f(a) \in \{f(x) \mid x \in A\} \implies a \in A$$

$$f(a) \notin \{f(x) \mid x \in A\} \implies a \notin A$$

Sottoinsieme

Relazione di sottoinsieme

$$A \subseteq B \iff (\forall x. x \in A \implies x \in B)$$

Insieme delle parti

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

Esempio

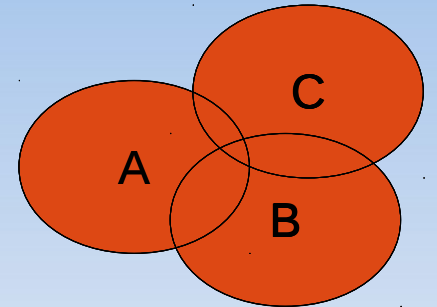
$$\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$$

Questo è un “insieme di insiemi”, a volte anche chiamato “famiglia di insiemi”.

Unioni arbitrarie

Unione di un insieme di insiemi \mathcal{X}

$$\bigcup \mathcal{X} = \{x \mid \exists X. X \in \mathcal{X} \wedge x \in X\}$$



Concettualmente: \mathcal{X} è un insieme di insiemi, X è un insieme, mentre x è un elemento.

Esempio:

$$\bigcup \{\{1, 2\}, \{2, 3\}, \{3, 4\}\} = \{1, 2, 3, 4\}$$

Unioni arbitrarie

Notare che:

$$A \cup B = \bigcup \{A, B\}$$

Altra notazione: usando un insieme di “indici” I

$$\bigcup_{i \in I} A_i = \bigcup \{A_i \mid i \in I\}$$

Intersezioni arbitrarie

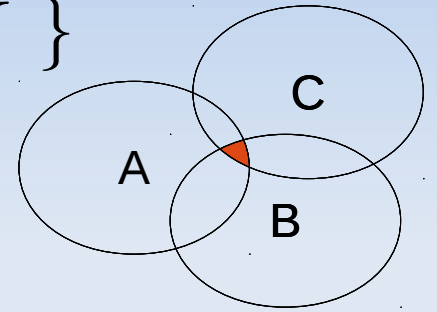
L'intersezione di un insieme di insiemi \mathcal{X} è analoga

$$\bigcap \mathcal{X} = \{x \mid \forall X. X \in \mathcal{X} \implies x \in X\}$$

Esercizio. Semplificare le seguenti:

$$\bigcup \{\{n, n + 1, n + 2\} \mid n \in \mathbb{N}\}$$

$$\bigcap \{\{m \mid m \in \mathbb{N} \wedge m \geq n\} \mid n \in \mathbb{N}\}$$



Esercizio

Esercizio. Dimostrare che, se l'insieme Y appartiene alla famiglia \mathcal{X} :

$$\bigcap \mathcal{X} \subseteq Y \subseteq \bigcup \mathcal{X}$$

Unioni arbitrarie

FUORI
ESAME

L'operatore di unione arbitraria si può pensare come un operatore

$$\bigcup : \mathcal{P}(\mathcal{P}(A)) \rightarrow \mathcal{P}(A)$$

che quindi prende un insieme di insiemi (di elementi di A) e restituisce un insieme (di elementi di A).

Lo stesso vale per \bigcap .

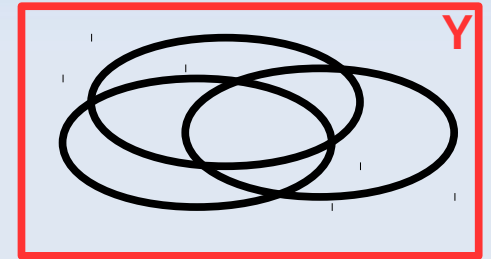
Esercizio. (Impegnativo) Sia $\mathcal{X} \in \mathcal{P}(\mathcal{P}(A))$. Dimostrare che

$$\bigcup \mathcal{X} = \left(A \setminus \bigcap \{A \setminus X \mid X \in \mathcal{X}\} \right)$$

Proprietà dell'Unione/Intersez.

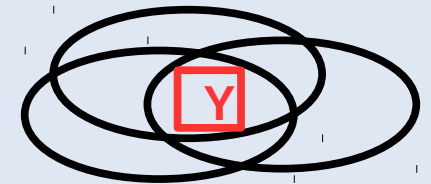
Lemma. Sia \mathcal{X} una famiglia di insiemi, e Y un insieme.
Vale la seguente:

$$\bigcup \mathcal{X} \subseteq Y \quad \iff \quad \forall X \in \mathcal{X}. X \subseteq Y$$



Analogamente per l'intersezione:

$$Y \subseteq \bigcap \mathcal{X} \quad \iff \quad \forall X \in \mathcal{X}. Y \subseteq X$$



Proprietà dell'Unione

Dim. Dimostriamo solo la prima parte (unione), lasciando la seconda (intersezione) per esercizio.

(\Rightarrow) Assumiamo *IP1* : $\bigcup \mathcal{X} \subseteq Y$ e dimostriamo che per ogni $X \in \mathcal{X}$ si ha $X \subseteq Y$.

Prendiamo quindi un arbitrario $X \in \mathcal{X}$ e dimostriamo $X \subseteq Y$.

Vale l'inclusione $X \subseteq \bigcup \mathcal{X}$: infatti, $\bigcup \mathcal{X}$ include qualunque insieme nella famiglia.

Da questo e *IP1* ricaviamo la tesi:

$$X \subseteq \bigcup \mathcal{X} \subseteq Y$$

Proprietà dell'Unione

(\Leftarrow) Per ipotesi assumiamo che $X \subseteq Y$ per ogni $X \in \mathcal{X}$ (*IP1*), e dimostriamo che $\bigcup \mathcal{X} \subseteq Y$.

Per dimostrare tale inclusione, consideriamo un elemento arbitrario $x \in \bigcup \mathcal{X}$ (*IP2*) e dimostriamo $x \in Y$.

Da *IP2* ricaviamo che esiste un insieme $X \in \mathcal{X}$ (*IP3*) tale per cui $x \in X$ (*IP4*).

Da *IP1*, *IP3* ricaviamo che $X \subseteq Y$. Da questo e *IP4*, si ha

$$x \in X \subseteq Y$$

da cui la tesi $x \in Y$.

Q.E.D.

L'insieme più piccolo tale che ...

Def. Data una famiglia di insiemi \mathcal{X} il *più piccolo* insieme M in \mathcal{X} , detto anche il *minimo* di \mathcal{X} , è quell'insieme che soddisfa

- 1) $M \in \mathcal{X}$
- 2) $\forall Y \in \mathcal{X}. M \subseteq Y$

In altre parole, il minimo insieme in \mathcal{X} è un insieme che appartiene alla famiglia che è incluso in tutti gli altri.

Si noti che il minimo non sempre esiste.

Esempi

La famiglia $\{\{1, 2\}, \{2, 3\}\}$ non ha minimo.

La famiglia $\{\{1, 2, 3, 4\}, \{2, 3\}\}$ ha come minimo $\{2, 3\}$.

La famiglia di intervalli reali $\{[-x, x] \mid x > 3\}$ non ha minimo, mentre $\{[-x, x] \mid x \geq 3\}$ ha minimo $[-3, 3]$.

La famiglia $\mathcal{P}(\mathbb{N})$ ha minimo \emptyset . La famiglia $\mathcal{P}^\infty(\mathbb{N})$ che contiene solo i sottoinsiemi *infiniti* di \mathbb{N} (come i numeri pari, i numeri primi, i numeri maggiori di 42, etc.) non ha minimo.

Lemma dell'insieme minimo (1)

Lemma. Sia \mathcal{X} una famiglia di insiemi. Se ammette un minimo M , allora deve essere $M = \bigcap \mathcal{X}$.

Dim. Siccome M è minimo, per definizione abbiamo che $IP1 : M \in \mathcal{X}$ e $IP2 : M \subseteq Y$ per ogni $Y \in \mathcal{X}$.

Dall'ipotesi $IP1$ segue che $\bigcap \mathcal{X} \subseteq M$ visto che l'intersezione è inclusa in un qualunque insieme della famiglia.

L'ipotesi $IP2$ per la proprietà dell'intersezione è equivalente a $M \subseteq \bigcap \mathcal{X}$.

Dalla doppia inclusione concludiamo $M = \bigcap \mathcal{X}$.

Lemma dell'insieme minimo (2)

Lemma. Sia \mathcal{X} una famiglia di insiemi e sia $M = \bigcap \mathcal{X}$. Se $M \in \mathcal{X}$, allora M è il minimo di \mathcal{X} .

Dim. Siccome $M \in \mathcal{X}$, basta solo vedere che per ogni $Y \in \mathcal{X}$ si ha $M \subseteq Y$.

Questo segue immediatamente dal fatto che l'intersezione è inclusa in un qualunque insieme della famiglia.

Coppie ordinate

Proprietà fondamentale delle coppie ordinate

$$\langle x, y \rangle = \langle x', y' \rangle \iff x = x' \wedge y = y'$$

Prodotto cartesiano:

$$A \times B = \{ \langle a, b \rangle \mid a \in A \wedge b \in B \}$$

Proiezioni:

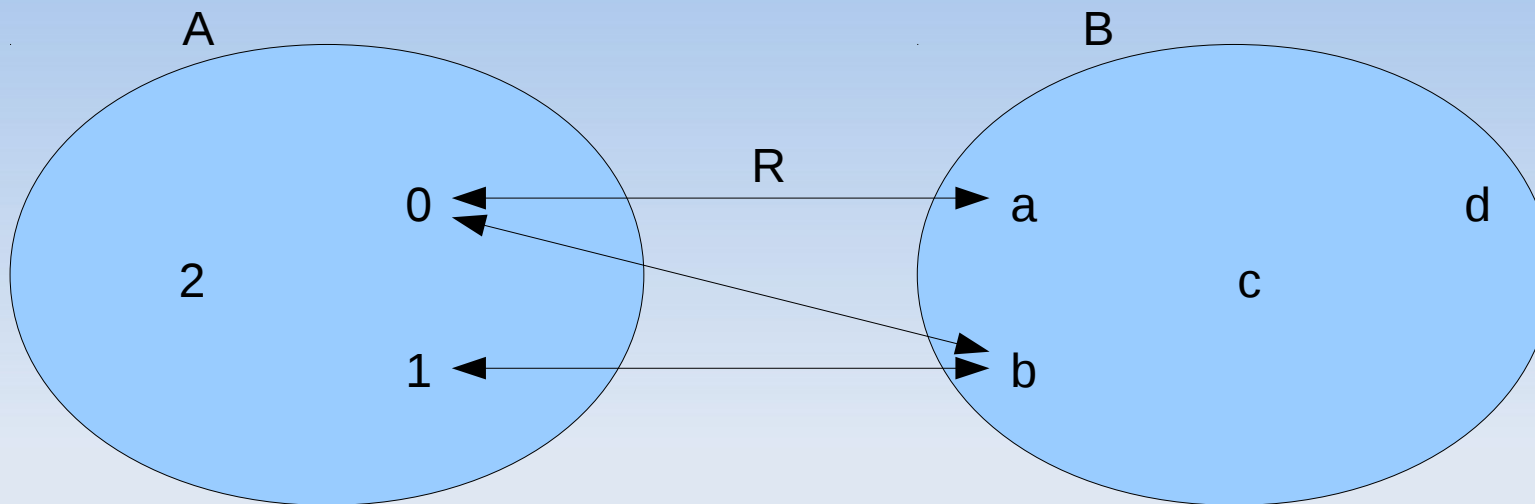
$$\pi_1 : A \times B \rightarrow A$$

$$\pi_1(\langle a, b \rangle) = a$$

$$\pi_2 : A \times B \rightarrow B$$

$$\pi_2(\langle a, b \rangle) = b$$

Relazioni



Una R relazione tra A e B si può vedere come un insieme di coppie

$$R = \{\langle 0, a \rangle, \langle 0, b \rangle, \langle 1, b \rangle\} \subseteq A \times B$$

In altri termini, l'insieme delle relazioni tra A e B è

$$\mathcal{P}(A \times B)$$

La notazione usuale per “ a e b sono associati da R ”

$$aRb \iff \langle a, b \rangle \in R$$

Composizione di relazioni $R \in \mathcal{P}(A \times B), S \in \mathcal{P}(B \times C)$

$$S \circ R = \{ \langle a, c \rangle \mid \exists b \in B. aRb \wedge bSc \} \in \mathcal{P}(A \times C)$$

(da non confondere con $R \circ S$)

Relazione inversa

$$R^{-1} = \{ \langle a, b \rangle \mid \langle b, a \rangle \in R \}$$

Esercizio. Dire se $R^{-1} \circ R = I$ dove I è la relazione identità.

Funzioni

Una funzione tra A e B è una relazione che associa ad ogni $a \in A$ uno ed un solo $b \in B$. Formalmente, lo spazio di tutte le funzioni è dato da

$$(A \rightarrow B) = \{f \in \mathcal{P}(A \times B) \mid \forall a \in A. \exists! b \in B. \langle a, b \rangle \in f\}$$

La notazione usuale per l'applicazione di funzione:

$$f(a) = b \iff \langle a, b \rangle \in f$$

Dominio, Immagine

Dominio ed immagine di $f \in (A \rightarrow B)$:

$$\begin{aligned} \text{dom}(f) &= \{\pi_1(c) \mid c \in f\} & \text{img}(f) &= \{\pi_2(c) \mid c \in f\} \\ \text{dom}(f) &= A & \text{img}(f) &\subseteq B \end{aligned}$$

Immagine di un insieme

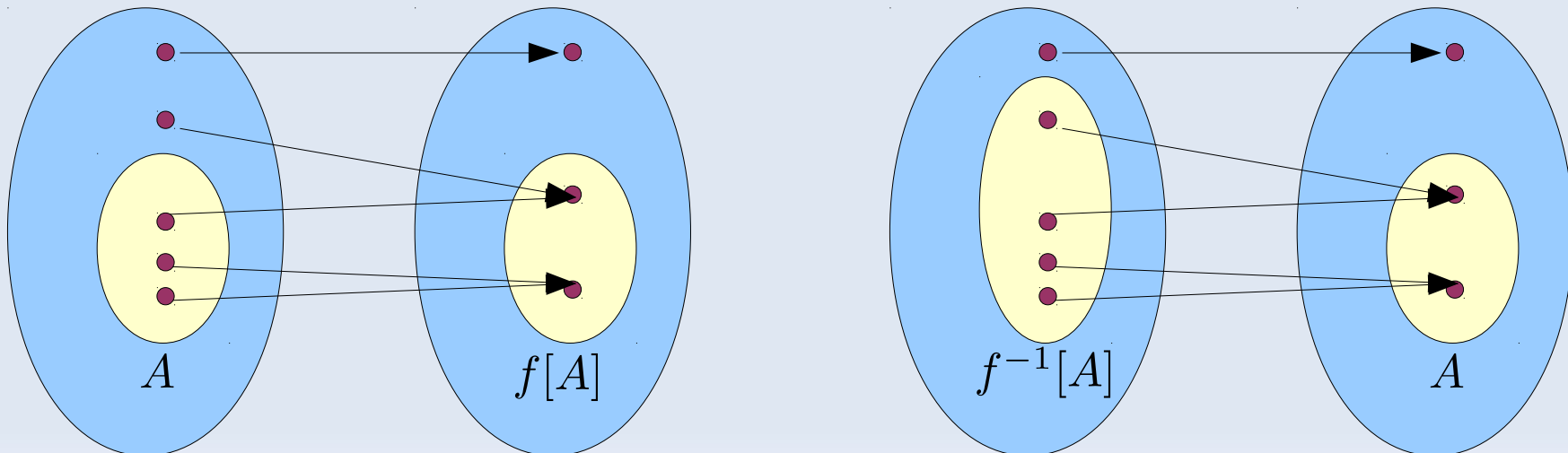
FUORI
ESAME

L'immagine di un insieme A secondo una funzione f

$$f[A] = \{f(x) \mid x \in A\}$$

La controimmagine

$$f^{-1}[A] = \{x \mid f(x) \in A\}$$



Esercizio. Sotto quali condizioni si può dire che valgono le seguenti?

$$\begin{array}{lll} f^{-1}[f[A]] \subseteq A & f^{-1}[f[A]] \supseteq A & f^{-1}[f[A]] = A \\ f[f^{-1}[A]] \subseteq A & f[f^{-1}[A]] \supseteq A & f[f^{-1}[A]] = A \end{array}$$

Immagine di un insieme

FUORI
ESAME

Esercizio. Sia $f \in (A \rightarrow B)$, $A_i \subseteq A$ e $B_i \subseteq B$.

Quali delle seguenti valgono?

$$\text{dom}(f) = f^{-1}[\text{img}(f)]$$

$$\text{img}(f) = f[\text{dom}(f)]$$

$$f[A_1 \cup A_2] = f[A_1] \cup f[A_2]$$

$$f[A_1 \cap A_2] = f[A_1] \cap f[A_2]$$

$$f^{-1}[B_1 \cup B_2] = f^{-1}[B_1] \cup f^{-1}[B_2]$$

$$f^{-1}[B_1 \cap B_2] = f^{-1}[B_1] \cap f^{-1}[B_2]$$

Cosa succede se richiedo solo \subseteq invece dell'uguaglianza? E se richiedo \supseteq ?

Iniettività, Suriettività

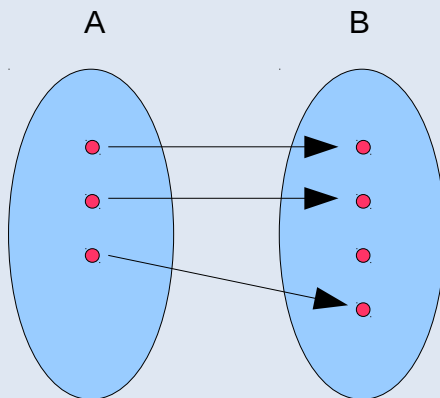
FUORI
ESAME

Sia $f \in (A \rightarrow B)$.

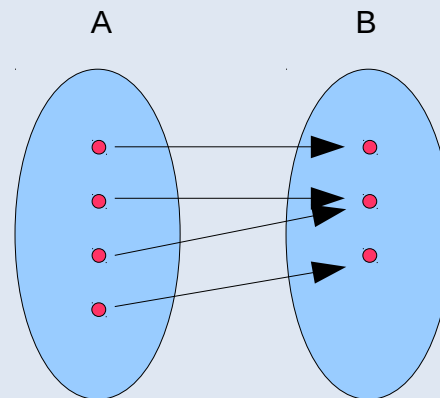
f iniettiva $\iff \forall a_1, a_2 \in A. f(a_1) = f(a_2) \implies a_1 = a_2$

f suriettiva $\iff \forall b \in B. \exists a \in A. f(a) = b$

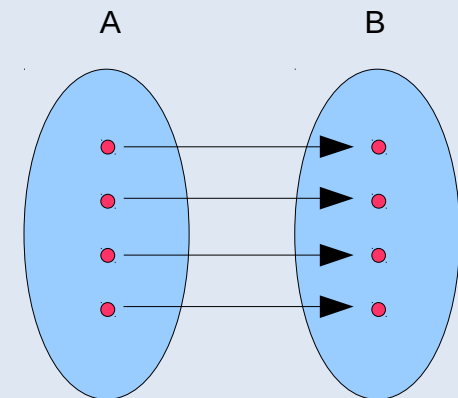
f biettiva $\iff f$ iniettiva e suriettiva



iniettiva
ma non suriettiva



suriettiva
ma non iniettiva



biettiva

Definire una biezione nei seguenti insiemi:
Sotto, A, B, C indicano insiemi arbitrari.

$$(A \times B) \quad \leftrightarrow \quad (B \times A)$$

$$(A \times (B \times C)) \quad \leftrightarrow \quad ((A \times B) \times C)$$

$$\mathcal{P}(A) \quad \leftrightarrow \quad (A \rightarrow \{0, 1\})$$

$$((A \times \{0\}) \cup (B \times \{1\})) \leftrightarrow ((B \times \{0\}) \cup (A \times \{1\}))$$

$$(A \cup B) \quad \leftrightarrow \quad ((A \times \{0\}) \cup ((B \setminus A) \times \{1\}))$$

Esercizio. Sia $f \in (A \rightarrow B)$ una funzione arbitraria, e sia f^{-1} la relazione inversa di f . Dimostrare che

$$f \text{ iniettiva} \iff f^{-1} \in (\text{img}(f) \rightarrow A)$$

facendo riferimento alle definizioni date precedentemente.

Notazione lambda

L'espressione

$$\lambda x. f(x)$$

denota la funzione che associa ad ogni x il valore $f(x)$.

Per esempio,

$$\lambda x. x^2$$

è la funzione “quadrato”.

La λ -notazione è utile quando non si vuole associare un nome alle funzioni coinvolte in un'espressione. Per esempio:

$$(\lambda x. x^3 + 1) \circ (\lambda x. x^2) = (\lambda x. x^6 + 1)$$

Notazione lambda

La λ -notazione è comoda quando si vuole specificare l'argomento di una funzione il cui dominio è un insieme di funzioni.

Per esempio

$$f \in ((\mathbb{N} \rightarrow \mathbb{N}) \rightarrow \mathbb{N})$$

$$f(g) \stackrel{def}{=} g(2)$$

$$f(\lambda x. x^3 + x) = 10$$

Esempio

Definiamo una biezione f

$$(A \rightarrow (B \times C)) \rightarrow ((A \rightarrow B) \times (A \rightarrow C))$$

Si ha:

$$\begin{aligned} f(g) &= \langle \lambda a \in A. \pi_1(g(a)), \lambda a \in A. \pi_2(g(a)) \rangle \\ &= \langle \pi_1 \circ g, \pi_2 \circ g \rangle \end{aligned}$$

con inversa

$$f^{-1}(\langle h_1, h_2 \rangle) = \lambda a \in A. \langle h_1(a), h_2(a) \rangle$$

Esempio

Definiamo una biezione f

$$((A \times B) \rightarrow C) \rightarrow (A \rightarrow (B \rightarrow C))$$

Si ha:

$$f(g) = \lambda a \in A. \lambda b \in B. g(\langle a, b \rangle)$$

con inversa

$$f^{-1}(h) = \lambda x \in A \times B. h(\pi_1(x))(\pi_2(x))$$

Si noti che $h(\pi_1(c))$ è una funzione $B \rightarrow C$.

Esercizio

FUORI
ESAME

Esercizio. Definire una biezione f (e la sua inversa)

$$((A \cup B) \rightarrow C) \rightarrow ((A \rightarrow C) \times (B \rightarrow C))$$

supponendo $A \cap B = \emptyset$