

Logica Matematica

1.1 – Teoremi e dimostrazioni

Docenti: Alessandro Andretta e Luca Motto Ros

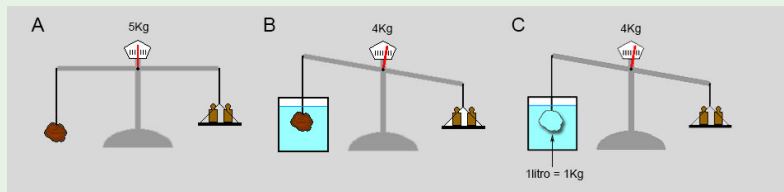
Dipartimento di Matematica
Università di Torino

Esperimenti e dimostrazioni

Nella maggior parte delle discipline scientifiche (ad esempio fisica, chimica, biologia...) per stabilire la verità di un'affermazione si ricorre a **misurazioni**, **esperimenti** o **simulazioni**: se gli esperimenti, magari fatti più volte e da più persone, confermano l'affermazione questa viene accettata (almeno temporaneamente), altrimenti viene rifiutata.

Esempio: il principio di Archimede

Ogni corpo immerso parzialmente o completamente in un fluido riceve una spinta verticale dal basso verso l'alto, uguale per intensità al peso del volume del fluido spostato.



In matematica (ma anche in informatica), questo “metodo scientifico” **non funziona!**

Ad esempio, nessun esperimento potrà mai stabilire se $\sqrt{2}$ sia un numero razionale (ovvero se $\sqrt{2} = \frac{n}{m}$ con n ed m numeri interi).

Controllare alcuni casi specifici (= **misurazioni**, **esperimenti** o **simulazioni**) può essere utile per avere **indizi** sulla verità o meno di un'affermazione, ma a volte questi indizi possono anche essere fuorvianti. Vediamo un esempio...

Esempio

Congettura: $991 \cdot n^2 + 1$ non è mai un quadrato perfetto (ovvero la sua radice quadrata non è un numero intero).

Si è dimostrato che tale congettura è falsa, anzi ci sono infiniti numeri del tipo $991 \cdot n^2 + 1$ che sono quadrati perfetti. Tuttavia, il più piccolo di tali numeri è

12055735790331359447442538767 $\approx 1,2 \cdot 10^{28} >$ diametro terra

Quanto è grande questo numero?

Diametro terra: $\approx 6,371 \cdot 10^6$ m

Esempio

Congettura: $991 \cdot n^2 + 1$ non è mai un quadrato perfetto (ovvero la sua radice quadrata non è un numero intero).

Si è dimostrato che tale congettura è falsa, anzi ci sono infiniti numeri del tipo $991 \cdot n^2 + 1$ che sono quadrati perfetti. Tuttavia, il più piccolo di tali numeri è

12055735790331359447442538767 $\approx 1,2 \cdot 10^{28} >$ diametro sole

Quanto è grande questo numero?

Diametro sole: $\approx 1,39 \cdot 10^9$ m

Esempio

Congettura: $991 \cdot n^2 + 1$ non è mai un quadrato perfetto (ovvero la sua radice quadrata non è un numero intero).

Si è dimostrato che tale congettura è falsa, anzi ci sono infiniti numeri del tipo $991 \cdot n^2 + 1$ che sono quadrati perfetti. Tuttavia, il più piccolo di tali numeri è

12055735790331359447442538767 $\approx 1,2 \cdot 10^{28}$ > distanza terra-sole

Quanto è grande questo numero?

Distanza terra-sole: $\approx 1,5 \cdot 10^{11}$ m

Esempio

Congettura: $991 \cdot n^2 + 1$ non è mai un quadrato perfetto (ovvero la sua radice quadrata non è un numero intero).

Si è dimostrato che tale congettura è falsa, anzi ci sono infiniti numeri del tipo $991 \cdot n^2 + 1$ che sono quadrati perfetti. Tuttavia, il più piccolo di tali numeri è

12055735790331359447442538767 $\approx 1,2 \cdot 10^{28} >$ età dell'universo

Quanto è grande questo numero?

Età dell'universo: $\approx 13,83 \cdot 10^9$ m

Esempio

Congettura: $991 \cdot n^2 + 1$ non è mai un quadrato perfetto (ovvero la sua radice quadrata non è un numero intero).

Si è dimostrato che tale congettura è falsa, anzi ci sono infiniti numeri del tipo $991 \cdot n^2 + 1$ che sono quadrati perfetti. Tuttavia, il più piccolo di tali numeri è

12055735790331359447442538767 $\approx 1,2 \cdot 10^{28}$ > numero di stelle

Quanto è grande questo numero?

Numero di stelle nell'universo osservabile: $\approx 3 \cdot 10^{23}$ m

Esempio

Congettura: $991 \cdot n^2 + 1$ non è mai un quadrato perfetto (ovvero la sua radice quadrata non è un numero intero).

Si è dimostrato che tale congettura è falsa, anzi ci sono infiniti numeri del tipo $991 \cdot n^2 + 1$ che sono quadrati perfetti. Tuttavia, il più piccolo di tali numeri è

12055735790331359447442538767 $\approx 1,2 \cdot 10^{28}$ > cellule umane

Quanto è grande questo numero?

Cellule che compongono tutti gli esseri umani messi insieme: $\approx 10^{24}$ m

Esempio

Congettura: $991 \cdot n^2 + 1$ non è mai un quadrato perfetto (ovvero la sua radice quadrata non è un numero intero).

Si è dimostrato che tale congettura è falsa, anzi ci sono infiniti numeri del tipo $991 \cdot n^2 + 1$ che sono quadrati perfetti. Tuttavia, il più piccolo di tali numeri è

12055735790331359447442538767 $\approx 1,2 \cdot 10^{28}$

Quanto è grande questo numero? Confrontatelo con il *numero di stelle nell'universo osservabile*, ovvero: $\approx 3 \cdot 10^{23}$. Il nostro numero è enorme!

Quindi controllare a mano la congettura con degli esempi (anche moltissimi!) ci avrebbe erroneamente indotti a crederla vera...

In matematica, per stabilire la verità di un'affermazione (= **teorema**) si deve ricorrere a una **dimostrazione**.

Teorema: è l'affermazione (riguardante numeri, funzioni, enti geometrici, o altri oggetti matematici) che si vuole dimostrare. Di solito è della forma

“Se valgono certe **ipotesi**, allora anche la **tesi** del teorema è vera.”

Esempio: Se **p e q sono numeri negativi**, allora **$p \cdot q$ è un numero positivo**.

Dimostrazione: catena di ragionamenti che ci permette di concludere che la tesi del teorema deve essere vera partendo dall'assunzione che le ipotesi del teorema siano vere.

La stessa cosa vale in informatica. Supponiamo di aver scritto il programma che controlla la ventilazione di una sonda spaziale. Verificare con un certo numero (anche elevatissimo!) di **esperimenti** o **simulazioni** che il programma non va in crash ed esegue correttamente tutte le operazioni che deve svolgere non è sufficiente...

Come si può garantire che una volta in funzione sulla sonda spaziale non si verifichi proprio una situazione, mai incontrata nelle simulazioni, che porti al blocco del sistema (per la gioia degli astronauti presenti a bordo, che morirebbero soffocati)?

L'unico modo è fornire una **dimostrazione** del fatto che il programma funziona, ovvero della sua **correttezza**. Pur parlando di programmi e non di numeri, il concetto di dimostrazione è esattamente lo stesso usato in matematica quando si parla di teoremi. In questo caso il teorema sarà

Teorema

Il programma è corretto.

Cos'è un teorema?

Un **teorema** è un enunciato della forma

Se valgono P_1 e P_2 e ... P_n , allora vale anche Q .

Le affermazioni P_1, \dots, P_n sono dette **ipotesi** del teorema, mentre Q è detta **tesi** del teorema.

Un esempio di teorema è il seguente:

Teorema

Se n è un numero naturale dispari ed m è un numero naturale pari, allora $n + m$ è dispari.

Teorema

Se n è un numero naturale dispari ed m è un numero naturale pari, allora $n + m$ è dispari.

$\underbrace{\hspace{15em}}_{P_1}$ $\underbrace{\hspace{15em}}_{P_2}$

$\underbrace{\hspace{10em}}_Q$

In questo caso le ipotesi sono

- n è un numero naturale dispari,
- m è un numero naturale pari,

mentre la tesi è

- $n + m$ è dispari.

In matematica sono di uso comune anche altri sinonimi di “*Teorema*”, ad esempio “*Proposizione*”, “*Lemma*” e così via.

Dal punto di vista tecnico, tutti questi termini vogliono dire esattamente la stessa cosa, ovvero che quel che si sta affermando è un teorema.

La differenza tra le varie espressioni è l'importanza (del tutto soggettiva!) che chi scrive o parla vuole attribuire all'affermazione che si sta dimostrando: solitamente si riserva il termine “Teorema” per quelle che si ritengono veramente importanti e significative, “Proposizione” per quelle che sono un po' meno importanti ma pur sempre abbastanza significative e “Lemma” per quelle affermazioni che di per sé non sarebbero molto significative, ma che servono poi per dimostrare altri fatti più importanti.

Quando si analizza il ragionamento matematico, come faremo noi in questo corso, non si tiene conto di queste distinzioni e si parla sempre di **teorema**.

Il teorema

Se valgono P_1, P_2, \dots, P_n , allora vale anche Q .

intende asserire che:

In qualunque contesto o situazione le affermazioni P_1, P_2, \dots, P_n sono verificate, anche l'affermazione Q risulta essere vera.

Utilizzeremo la scrittura

$$P_1, \dots, P_n \models Q$$

(che si legge “ Q è **conseguenza logica** di P_1, \dots, P_n ”) per tradurre in un linguaggio simbolico il teorema con ipotesi P_1, \dots, P_n e tesi Q .

Ci sono anche affermazioni Q che sono valide in qualunque contesto, ossia enunciati per i quali

$$\vDash Q$$

è un teorema che non ha bisogno di ipotesi.

Ad esempio

Lo zero è il più piccolo tra i numeri naturali.

Un'affermazione Q di questo tipo viene detta **tautologia**.

Stabilire che cosa sia un *contesto/situazione* in cui sia possibile valutare se una data affermazione P sia vera o falsa è molto delicato (buona parte del corso sarà dedicata a dare una formulazione rigorosa di cosa siano questi “contesti”).

Negli esempi seguenti tutti le affermazioni P che considereremo parleranno di numeri n, m, x : i “contesti” possibili saranno allora tutti i possibili valori che questi numeri possono assumere.

Esempio

L'affermazione “ n è un numero naturale dispari” è vera nella situazione in cui n vale 3, ma falsa quando n vale 4.

Dimostrazioni

Come possiamo organizzare in modo rigoroso un ragionamento e stabilire che esso costituisce la dimostrazione di un teorema?

Ci sono diverse strategie dimostrative variamente utilizzate (spesso in combinazione tra loro). Nel seguito presenteremo le più comuni ossia:

- la **dimostrazione diretta**,
- la **dimostrazione per assurdo**,
- la **dimostrazione per contrapposizione**,
- la **dimostrazione per composizione** (o interpolazione),
- la **dimostrazione per casi**.

Vedremo nella Sezione 1.3 che la correttezza di tutte queste strategie dimostrative può essere verificata in maniera rigorosa utilizzando la logica proposizionale.

Dimostrazione diretta

La dimostrazione diretta è la strategia più semplice e naturale per stabilire un teorema del tipo

$$P_1, \dots, P_n \models Q.$$

La dimostrazione diretta assume di trovarsi in un qualunque contesto in cui siano verificate le ipotesi P_1, \dots, P_n e sulla base di semplici e rigorosi ragionamenti stabilisce che in tale contesto anche la tesi Q è verificata.

Dimostrazione diretta: un esempio

Se n è un numero intero dispari e m è un numero intero pari, allora $n + m$ è un numero intero dispari.

Dimostrazione.

Siano n ed m interi qualsiasi, e assumiamo che n sia dispari ed m pari, ovvero che $n = 2l + 1$ per qualche intero l , mentre $m = 2k$ per qualche intero k . Bisogna dimostrare che $n + m$ è dispari. Effettuando i calcoli si ha

$$\begin{aligned}n + m &= (2l + 1) + 2k \\ &= (2l + 2k) + 1 \\ &= 2(l + k) + 1.\end{aligned}$$

Questo dimostra che $n + m$ è dispari perché ha la forma $2j + 1$ (basta prendere $j = l + k$). □

Dimostrazione per assurdo

Una **dimostrazione per assurdo** di una proposizione Q a partire dalle ipotesi P_1, \dots, P_n è una dimostrazione in cui si assume che Q sia falsa e da questa assunzione si deriva (utilizzando anche le ipotesi P_1, \dots, P_n) una **contraddizione**, ovvero una proposizione della forma

$$R \text{ e non } R$$

che asserisce che una qualche affermazione R è al contempo sia vera che falsa. Poiché una contraddizione è necessariamente falsa (una proposizione in un dato contesto può essere vera o falsa, ma non entrambe contemporaneamente!), questo prova che assumere che Q sia falsa porta a conclusioni assurde, e quindi Q non può che essere vera. In altre parole: si dimostra che se le premesse P_1, \dots, P_n sono vere non è possibile che Q sia falsa.

Una dimostrazione con questa struttura viene anche chiamata una **dimostrazione indiretta**.

Concretamente, in una dimostrazione per assurdo di un teorema del tipo

$$P_1, \dots, P_n \models Q$$

si assume che le ipotesi P_1, \dots, P_n siano vere ma che, per assurdo, la tesi Q sia falsa, e da questa assunzione si deriva una contraddizione.

Quando invece il teorema è del tipo

$$\models Q,$$

ovvero quando si deve dimostrare Q senza partire da alcuna ipotesi (cioè quando bisogna mostrare che Q è una tautologia), allora una dimostrazione per assurdo consiste semplicemente nell'assumere per assurdo che Q sia falsa, e poi dimostrare che da quest'assunzione deriva una contraddizione.

Dimostrazione per assurdo: un esempio

Per tutti i numeri reali x, y , se $\underbrace{x + y \geq 2}_P$ allora $\underbrace{x \geq 1 \text{ oppure } y \geq 1}_Q$.

Dimostrazione.

Siano x e y numeri reali qualsiasi, e supponiamo per assurdo che P sia vera ma Q sia falsa, ovvero che valgano $x + y \geq 2$ e $x, y < 1$. (Si osservi che assumere che “ $x \geq 1$ oppure $y \geq 1$ ” sia falsa è equivalente ad assumere che “ $x < 1$ e $y < 1$ ” sia vera.)

Dalla negazione di Q segue che $x + y < 1 + 1$, ovvero $x + y < 2$. Ma questo contraddice l'assunzione P , ovvero si avrebbe che $x + y \geq 2$ e non $x + y \geq 2$.

Questo dimostra (per assurdo) che se vale P allora Q non può essere falsa. In altre parole, è vero che se vale P allora deve valere anche Q , quindi il teorema è dimostrato. □

Dimostriamo ora l'enunciato:

Per ogni numero intero n , se $\underbrace{n^2 \text{ è pari}}_P$, allora $\underbrace{n \text{ è pari}}_Q$.

Dimostrazione.

Supponiamo per assurdo che P sia vera ma Q sia falsa (ovvero che n sia dispari) e facciamo vedere che queste assunzioni portano ad una contraddizione. Sia n dispari, ovvero $n = 2m + 1$ per qualche intero m . Allora possiamo calcolare:

$$\begin{aligned}n^2 &= (2m + 1)^2 \\ &= 4m^2 + 4m + 1 \\ &= 2(2m^2 + 2m) + 1,\end{aligned}$$

per cui n^2 è dispari (essendo della forma $2j + 1$). Quindi abbiamo che
“ n^2 è pari” e non “ n^2 è pari”,
contraddizione! Quindi se vale P deve valere anche Q . □

Dimostrazione per contrapposizione

Introduciamo una tecnica che può essere utilizzata per semplificare la dimostrazione che abbiamo appena visto.

Per dimostrare un teorema del tipo $P \models Q$, si può anche dimostrare (in modo diretto) il teorema:

$$\text{non } Q \models \text{non } P.$$

Infatti, supponiamo di aver stabilito la correttezza del teorema “ $\text{non } Q \models \text{non } P$ ” e di essere in un contesto in cui vale l’ipotesi P . Allora in tale contesto anche Q deve essere vera, perché se fosse falsa (ovvero se valesse “non Q ”) allora si avrebbe che sia P (per ipotesi) che “non P ” (per il teorema $\text{non } Q \models \text{non } P$) sarebbero vere, contraddizione!

Posto di sapere che $\text{non } Q \models \text{non } P$, questo argomento mostra che in ogni contesto in cui valga P deve valere anche Q , ossia che $P \models Q$.

Dimostrazione per contrapposizione: un esempio

Per esempio, si può dimostrare per contrapposizione l'enunciato:

Se n^2 è un numero intero pari allora n è un numero intero pari.

dimostrando (in modo diretto) l'enunciato:

Se n è un numero intero dispari allora n^2 è dispari.

$(n$ non è pari) $(n^2$ non è pari)

Se n è un numero intero dispari allora n^2 è dispari.

$(n$ **non** è pari)

$(n^2$ **non** è pari)

Dimostrazione.

Assumiamo che n sia dispari, ovvero che $n = 2k + 1$ per qualche intero k : bisogna dimostrare allora che anche n^2 è dispari. Svolgendo i calcoli si ha che

$$\begin{aligned}n^2 &= (2k + 1)^2 \\ &= (4k^2 + 4k + 1) \\ &= 2(2k^2 + 2k) + 1\end{aligned}$$

quindi n^2 è dispari (poiché è della forma $2j + 1$). □

Dimostrazione per composizione o interpolazione

Se abbiamo dimostrato il teorema

$$P_1, \dots, P_n \models Q$$

ed il teorema

$$Q \models R,$$

allora possiamo comporre le due dimostrazioni in una dimostrazione di

$$P_1, \dots, P_n \models R$$

nel modo seguente:

In ogni contesto in cui valgano le ipotesi P_1, \dots, P_n deve valere anche Q , dato che $P_1, \dots, P_n \models Q$. Ma allora in tale contesto deve valere anche R poiché $Q \models R$. Quindi abbiamo stabilito che in ogni contesto in cui valgano P_1, \dots, P_n anche R deve valere, ossia che $P_1, \dots, P_n \models R$.

Dimostrazione per composizione: un esempio

Se $\underbrace{n \text{ è un numero intero dispari}}_{P_1}$ e $\underbrace{m \text{ è un numero intero pari}}_{P_2}$ allora
 $\underbrace{(n + m)^2 \text{ è un numero intero dispari.}}_R$

Dimostrazione.

Abbiamo visto in precedenza che considerando

$\underbrace{(n + m) \text{ è un numero intero dispari,}}_Q$

si ha che $P_1, P_2 \models Q$ e $Q \models R$. Componendo le dimostrazioni dei due teoremi otteniamo quindi una dimostrazione di $P_1, P_2 \models R$. □

Dimostrazione per casi

Quando si deve dimostrare un teorema della forma $P \models Q$ dove P è una disgiunzione di enunciati della forma

$$P_1 \text{ oppure } P_2 \text{ oppure } \dots \text{ oppure } P_n,$$

conviene dimostrare separatamente i teoremi

$$\begin{aligned} P_1 &\models Q \\ P_2 &\models Q \\ &\vdots \\ P_n &\models Q. \end{aligned}$$

Infatti, supponiamo di aver dimostrato ciascuno dei teoremi sopra elencati. Se in un contesto vale P , in questo contesto almeno un P_j tra i P_1, \dots, P_n sarà vero, per cui avendo dimostrato che $P_j \models Q$ possiamo concludere che in tale contesto anche Q è vero.

A volte i “casi” P_1, \dots, P_n non sono esplicitamente dati dall’enunciato, ma possiamo comunque distinguere diversi casi nella dimostrazione (quando questo è utile).

Ad esempio, per dimostrare un teorema $\models Q$ senza nessuna ipotesi, possiamo sfruttare il fatto che l’asserzione “ P o non P ” è necessariamente vera in qualunque contesto (e indipendentemente da chi sia P : in ciascun contesto, o P è vera oppure è falsa). Quindi per dimostrare $\models Q$ ci basta considerare i due casi (P vera, oppure P falsa) e dimostrare che valgono sia $P \models Q$ che $\text{non } P \models Q$.

Esempio

Se vogliamo dimostrare che una certa proprietà vale per tutti i numeri reali, possiamo considerare separatamente diversi casi (purché ogni reale sia compreso in almeno uno di essi): ad esempio possiamo trattare separatamente il caso dei reali < 0 e quello dei reali ≥ 0 .

Dimostrazione per casi: un esempio

Dimostriamo l'enunciato:

Per ogni numero reale x si ha che $x \leq |x|$.

Il teorema è della forma $\models Q$ con $\underbrace{x \leq |x|}_Q$ e vogliamo mostrare che Q è

vera in tutti i contesti possibili, ovvero per qualunque valore di x . Siccome nella definizione di valore assoluto

$$|x| = \begin{cases} x & \text{se } x \geq 0 \\ -x & \text{se } x < 0 \end{cases}$$

si considerano i due casi $\underbrace{x < 0}_P$ e $\underbrace{x \geq 0}_{\text{non } P}$, è naturale distinguere tra tali casi anche nella dimostrazione.

(Si osservi che “ P o $\text{non } P$ ”, ovvero l'affermazione “ $x < 0$ o $x \geq 0$ ”, è vera per ogni numero reale x , ovvero in ogni contesto che dobbiamo considerare.)

Per ogni numero reale x si ha che $x \leq |x|$.

Dimostrazione.

Distinguiamo **due casi**:

- $x < 0$: in questo caso $|x| = -x$, quindi $|x| > 0 > x$, da cui $x \leq |x|$.
- $x \geq 0$: in questo caso $|x| = x$, per cui vale $x \leq |x|$.

Poiché ogni reale x o $x < 0$ oppure $x \geq 0$, si può allora concludere che $x \leq |x|$ vale per ogni reale x . □

Tecniche di dimostrazione

Riassumendo gli schemi di dimostrazione visti finora:

Dimostrazione diretta di $P_1, \dots, P_n \models Q$

Si dimostra in maniera diretta che in ogni contesto in cui le ipotesi P_1, \dots, P_n sono vere anche la tesi Q risulta vera.

Dimostrazione per assurdo di $\models Q$ o di $P_1, \dots, P_n \models Q$

Si assume (per assurdo) la negazione della tesi Q e con un ragionamento rigoroso ne si deriva una contraddizione (eventualmente utilizzando anche le ipotesi P_1, \dots, P_n).

Dimostrazione per contrapposizione di $P \models Q$

Si dimostra (in maniera diretta oppure con una delle altre tecniche di dimostrazione) il teorema *non* $Q \models \text{non } P$.

Dimostrazione per composizione (o interpolazione) di $P_1, \dots, P_n \models R$

Si trova un enunciato Q tale che $P_1, \dots, P_n \models Q$ e $Q \models R$ e si “compongono” una dopo l'altra le dimostrazioni dei due teoremi.

Dimostrazione per casi di $(P_1 \text{ oppure } \dots \text{ oppure } P_n) \models Q$

È sufficiente dimostrare separatamente i teoremi $P_1 \models Q, \dots, P_n \models Q$.

Nel caso si voglia dimostrare $\models Q$ senza alcuna ipotesi è sufficiente dimostrare separatamente $P \models Q$ e $(\text{non } P) \models Q$ per un qualche enunciato P .

Le varie tecniche di dimostrazione viste possono poi essere combinate tra loro in vario modo all'interno di una stessa dimostrazione, dando luogo ad argomenti via via più complessi ma sempre logicamente corretti.

Teorema

$$\sqrt{2} \notin \mathbb{Q}.$$

Notiamo che posto $\underbrace{\sqrt{2} \notin \mathbb{Q}}_{\mathbb{Q}}$, questo è un teorema della forma $\models \mathbb{Q}$.

Dimostrazione

Supponiamo per assurdo che esistano $n, m \in \mathbb{N} \setminus \{0\}$ tali che $\left(\frac{m}{n}\right)^2 = 2$ e
 $\underbrace{\hspace{15em}}_{\text{non } \mathbb{Q}}$

cerchiamo di ottenere una contraddizione. Se n e m hanno d come massimo comun divisore, cioè $n = n_1 \cdot d$ e $m = m_1 \cdot d$, allora

$$\frac{m}{n} = \frac{m_1 \cdot d}{n_1 \cdot d} = \frac{m_1}{n_1},$$

quindi si ha che $\left(\frac{m_1}{n_1}\right)^2 = 2$ e che n_1 ed m_1 sono relativamente primi (ovvero il loro massimo comun divisore è 1).

(continua)

Dimostrazione (continua)

Da

$$\underbrace{\text{Esistono } m, n \text{ tali che } \left(\frac{m}{n}\right)^2 = 2}_{\text{non } Q}$$

abbiamo quindi dedotto (in maniera diretta) l'esistenza di numeri interi m_1, n_1 tali che

$$\underbrace{n_1 \text{ e } m_1 \text{ sono relativamente primi}}_P$$

e

$$\underbrace{\left(\frac{m_1}{n_1}\right)^2 = 2.}_R$$

Vogliamo ora ottenere una contraddizione. Per fare questo da R dedurremo $\text{non } P$, cosicché alla fine si avrà che da $\text{non } Q$ segue “ P e $\text{non } P$ ”.

(continua)

Dimostrazione (continua)

Siccome $\underbrace{\left(\frac{m_1}{n_1}\right)^2}_R = 2$, si ha che $\frac{m_1^2}{n_1^2} = 2$, da cui $m_1^2 = 2n_1^2$. Questo mostra

m_1^2 è pari, quindi, per quanto dimostrato nelle slides precedenti, m_1 è pari, cioè è della forma $m_1 = 2k$ per qualche k . Quindi $m_1^2 = 4k^2$ e sostituendo questo valore nell'equazione $m_1^2 = 2n_1^2$ si ottiene $4k^2 = 2n_1^2$, da cui $n_1^2 = 2k^2$. Quindi anche n_1^2 è pari, e per quanto visto in precedenza questo implica che n_1 sia pari. Ma poiché sono entrambi pari, questo vuol dire che n_1 ed m_1 non sono relativamente primi, contraddizione!

$\underbrace{\hspace{15em}}_{\text{non P}}$



La struttura della dimostrazione precedente è quindi:

- 1 Si assume (per assurdo) che la tesi del teorema Q sia falsa, ovvero si assume $\text{non } Q$.
- 2 Si dimostra in maniera diretta che " $\text{non } Q \models P$ ".
- 3 Si dimostra in maniera diretta che " $\text{non } Q \models R$ " e " $R \models \text{non } P$ ", da cui per composizione " $\text{non } Q \models \text{non } P$ ".

(Si noti però che durante questa dimostrazione diretta abbiamo usato due volte il fatto che "*se j^2 è pari allora j è anch'esso pari*", che era stato dimostrato per contrapposizione: quindi in realtà si tratta della composizione di alcune dimostrazioni dirette, come ad esempio quella di " $\text{non } Q \models m^2 \text{ è pari}$ " oppure quella di " $m \text{ è pari} \models n^2 \text{ è pari}$ ", con la dimostrazione per contrapposizione del risultato menzionato.)

- 4 Si conclude quindi che " $\text{non } Q \models P \text{ e } \text{non } P$ ", cosicché si è dimostrato che dall'ipotesi (assurda) $\text{non } Q$ seguirebbe una contraddizione.
- 5 Utilizzando il metodo della dimostrazione per assurdo, si conclude allora che Q deve essere vera.

Dimostrazione alternativa di $\sqrt{2} \notin \mathbb{Q}$.

Come prima, ragioniamo per assurdo. Supponiamo che esistano $n, m \in \mathbb{N} \setminus \{0\}$ tali che $\left(\frac{m}{n}\right)^2 = 2$ (ovvero tali che $m^2 = 2n^2$; in particolare $\frac{m}{2} < n < m$) e supponiamo che m sia il più piccolo numero siffatto.

Allora $m^2 = n^2 + n^2 + 2(m - n)^2 - k^2$, da cui (tenendo conto che $m^2 = 2n^2$) si ha $0 = 2(m - n)^2 - k^2$, cioè $k^2 = 2(m - n)^2$, ovvero $\left(\frac{k}{m-n}\right)^2 = 2$.

Ma $k = m - 2(m - n) < m$, contraddizione! □

Equivalenza

Può talvolta accadere di avere due affermazioni P e Q tali che

$P \models Q$ e $Q \models P$.

Se questo accade vuol dire che in ogni contesto in cui vale P deve valere anche Q e, viceversa, in ogni contesto in cui vale Q deve valere anche P ; quindi P e Q valgono esattamente negli stessi contesti, ovvero sono equivalenti.

Scriviamo

$$P \equiv Q$$

(che si legge “ P e Q sono **logicamente equivalenti**”) per dire che in ogni contesto in cui si possono valutare P e Q

P è vera se e solo se Q è vera.

In altre parole: in ogni possibile contesto, o P e Q sono entrambe vere, oppure sono entrambe false e sono pertanto “indistinguibili” per quel che riguarda l’essere vere o meno.

Un esempio

Consideriamo le seguenti affermazioni riguardanti un numero reale x :

$$\begin{aligned} P: & \quad x \geq 0; \\ Q: & \quad x = y^2 \text{ per qualche numero reale } y. \end{aligned}$$

Dato un qualunque numero reale x , se $x \geq 0$ allora basta porre $y = \sqrt{x}$ per avere $x = y^2$. Quindi

$$P \models Q.$$

D'altra parte, se $x = y^2$ per qualche numero reale y allora $x \geq 0$ perché il quadrato di un numero reale è sempre un numero non negativo. Quindi

$$Q \models P.$$

Abbiamo perciò verificato che per ogni possibile valore di x , la proprietà P è vera se e solo se Q è vera. Questo vuole dire che P e Q sono affermazioni equivalenti, ovvero

$$P \equiv Q.$$

Alcune proprietà fondamentali di \models ed \equiv

Vediamo infine alcune proprietà di base dei concetti appena introdotti. Alcune di esse sono ovvie, ma è bene comunque tenerle a mente perché torneranno utili in seguito.

Date tre affermazioni P , Q ed R qualsiasi, si ha che

$$\textcircled{1} \quad P \models P \qquad \qquad \qquad \text{(Riflessività)}$$

$$\textcircled{2} \quad \text{se } P \models Q \text{ e } Q \models R, \text{ allora } P \models R \qquad \qquad \text{(Transitività)}$$

La prima proprietà è del tutto ovvia. La seconda segue dal fatto che $P \models R$ può essere dimostrato componendo le dimostrazioni di $P \models Q$ e $Q \models R$ (*dimostrazione per composizione o interpolazione*).

Date tre affermazioni P , Q ed R qualsiasi, si ha che

- 1 $P \equiv P$ *(Riflessività)*
- 2 se $P \equiv Q$ allora anche $Q \equiv P$ *(Simmetria)*
- 3 se $P \equiv Q$ e $Q \equiv R$, allora $P \equiv R$ *(Transitività)*

La prima e la seconda proprietà sono del tutto ovvie. La terza segue dalla transitività di \models . Infatti, se $P \equiv Q$ e $Q \equiv R$, allora in particolare $P \models Q$ e $Q \models R$, da cui $P \models R$ per la transitività di \models . Viceversa, da $P \equiv Q$ e $Q \equiv R$ segue anche che $Q \models P$ e $R \models Q$, da cui $R \models P$ sempre per transitività di \models . Quindi $P \equiv R$.