Lezione 1

Insiemi

Donato A. Ciampa

In questa prima lezione introdurremo i simboli fondamentali del linguaggio matematico, quali l'implicazione logica $\Longrightarrow$ e la doppia implicazione $\Longleftrightarrow$, e i concetti di Teorema e Proposizione matematica, nonché le tipologie di dimostrazione. In seguito, definiremo il concetto di insieme e le sue proprietà generali e studieremo, come esempi, alcuni fondamentali insiemi numerici quali $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

1. Il Linguaggio Della Matematica

Un *linguaggio* è una terna $(\mathcal{P}, \mathcal{A}, \mathcal{L})$ di tre strutture dette *proposizioni, assiomi, leggi* rispettivamente. Le proposizioni $\mathcal{P}$ costituiscono le frasi del linguaggio, gli assiomi $\mathcal{A}$ sono particolari frasi non deducibili da altre all'interno del linguaggio dato e le leggi $\mathcal{L}$ sono le regole che permettono di combinare tra loro assiomi e proposizioni al fine di generare nuove frasi.
Nelle varie branche della matematica, ognuna delle quali costituisce un linguaggio, vi sono proposizioni, assiomi e leggi diverse: ad esempio in Geometria Euclidea è noto che gli assiomi più comuni sono quelli di concetto di punto e retta, che una tipica proposizione sia il Teorema di Pitagora e che le regole siano ad esempio le leggi di congruenza o le leggi delle rette parallele.

In genere, in matematica le proposizioni si dividono in due classi distinte: le *Definizioni*, le quali servono appunto a definire gli oggetti argomento di studio e gli *Asserti*, i quali si dividono a loro volta in *Lemmi, Proposizioni, Teoremi, Corollari*. Questi ultimi sono costituiti da due frasi: *l'ipotesi* I, che raccoglie una serie di oggetti e proprietà definite in partenza, e *la tesi* T, una frase che determina una ulteriore proprietà di tali oggetti e che si può dedurre logicamente dall'ipotesi attraverso la *dimostrazione*. La struttura formale di un asserto risulta quindi la seguente

$$I \Longrightarrow T, \qquad I \Longleftrightarrow T. \tag{1.1}$$

Nel primo caso, il simbolo $\Longrightarrow$ di *implicazione logica* sta ad indicare che dall'ipotesi I si può pervenire, adoperando le leggi del linguaggio per costruire una dimostrazione, alla tesi T. Nel secondo caso, il simbolo $\Longleftrightarrow$ di *doppia implicazione*, indica che le due frasi I e T sono tra loro *logicamente equivalenti*: ciò vuol dire che non solo da I si può pervenire a T, ma i ruoli di tali frasi può essere scambiato cosicché T divenga l'ipotesi da cui si può dimostrare la tesi I[1].
Ma come si può ricavare, con passaggi logici, la tesi partendo da una ipotesi? I

[1]Le due frasi in (1.1) vanno lette: *se I allora T; I se e solo se T.*

metodi di dimostrazione sono i più svariati e cambiano da argomento ad argomento. In generale, tuttavia, le dimostrazioni si suddividono in due grandi classi:

(i) *dimostrazioni dirette*: sono quelle nelle quali, utilizzando varie proprietà degli oggetti in esame e partendo dalle proprietà enunciate nelle ipotesi, attraverso una catena di ragionamenti logici, si perviene direttamente alla tesi;

(ii) *dimostrazione per assurdo*: si suppone che la tesi possa essere falsa e, attraverso una serie di procedimenti logici, si perviene ad un assurdo, ovvero a determinare che l'ipotesi non possa essere correta. Dal momento che l'ipotesi è una assunzione che facciamo liberamente, e che quindi non è soggetta a dimostrazioni e risulta sempre vera, ciò ci porta ad affermare che l'aver supposto falsa la tesi è il motivo di tale assurdo e, quindi, la tesi deve essere vera.

Diamo una spiegazione logica della dimostrazione per assurdo. Supponiamo di voler dimostrare l'asserto $I \Longrightarrow T$ per assurdo. Quindi assumiamo che T sia falsa: se ciò accade, la negazione di T, che indichiamo con $\neg T$, risulta vera. A questo punto, si applica una legge fondamentale dei linguaggi, detta della *controimplicazione*

$$(I \Longrightarrow T) \Longleftrightarrow (\neg T \Longrightarrow \neg I). \tag{1.2}$$

Tale legge afferma che se la frase I implica la T, allora è anche vero che la frase $\neg T$ implica la $\neg I$. Un esempio banale di questo fatto è il seguente asserto vero:

Se Q è un quadrato allora i suoi lati sono uguali

la cui negazione

Se i lati **non** sono uguali allora Q **non** è un quadrato

è ancora un'asserto vero.
Utilizzando la (1.2), possiamo allora dedurre che il fatto che $\neg T$ sia vera deve implicare necessariamente che anche $\neg I$ sia vera, ma allora I è falsa, ma ciò non può essere in quanto I essendo la nostra ipotesi, deve essere necessariamente vera. L'assurdo, come si può facilmente vedere nasce dall'aver supposto T falsa e quindi si può concludere che T deve essere vera.

2. Teoria Degli Insiemi

Un insieme è una collezione di oggetti *a priori* non specificata. Denotiamo un insieme con le lettere maiuscole latine $A, B, C, \cdots$. Dato un insieme A, gli oggetti che si trovano in A si chiamano *elementi* di A, e vengono elencati con lettere minuscole dell'alfabeto latino. Se a è un elemento di A, scriveremo $a \in A$, mentre se a non è un elemento di A scriveremo $a \notin A$.
Siano A, B due insiemi: se accade che tutti gli elementi di A si trovano anche in B, allora diremo che A è *incluso* in B e scriveremo $A \subseteq B$. Se A è incluso in B ma B contiene elementi che non si trovano in A, diremo che A è *incluso strettamente* in B e scriveremo $A \subset B$. Se in particolare tutti gli elementi di A e B coincidono, allora diremo che A e B sono *uguali* e scriveremo $A = B$.

Teorema 2.1. *Siano A e B due insiemi. Allora $A = B$ se e solo se $A \subseteq B$ e $B \subseteq A$.*

Dimostrazione. Supponiamo che $A = B$: allora gli elementi dei due insiemi sono gli stessi. Ciò implica che $A \subseteq B$ e che $B \subseteq A$, poiché ciascuno dei due insiemi contiene tutti gli elementi dell'altro.
Viceversa, supponiamo che valgano le due inclusioni e ragioniamo per assurdo. Supponiamo che allora $A \neq B$: ciò vuol dire che esiste almeno un elemento $a \in A$ tale che $a \notin B$ e che esiste almeno un lemento $b \in B$ tale che $b \notin A$. Ma allora né A è incluso in B, né B è incluso in A, cosa assurda visto che siamo partiti da tale ipotesi. Ne segue che deve essere necessariamente $A = B$. □

Il Teorema 2.1 si dice *Teorema della doppia inclusione*. Esso costituisce un importante risultato in quanto asserisce che, al fine di dimostrare l'uguaglianza tra due insiemi, è necessario e sufficiente far vedere che i due insiemi sono uno incluso nell'altro reciprocamente.

Definiremo ora, in maniera formale, alcune operazioni tra insiemi. Innanzitutto, vediamo che possiamo definire un insieme in maniera analitica nel modo seguente

$$A = \{x \in X : x \text{ soddisfa la proprietà } \mathcal{P}\}.$$

Vediamo cosa significa la precedente scrittura:

(*i*) A è l'insieme che si vuole definire;

(*ii*) X rappresenta un insieme grande, detto *insieme Universo*, all'interno del quale si trovano gli elementi che vogliamo includere nell'insieme A (ed in generale $A \subseteq X$);

(*iii*) $\mathcal{P}$ indica una proprietà che tutti gli elementi x dell'insieme A devono soddisfare.

Ad esempio, se $X = \{1, 2, 3, \ldots, 99, 100\}$ è l'universo dei primi 100 numeri naturali, allora possiamo definire gli insiemi

$$A = \{x \in X : x \text{ è pari}\},$$

$$B = \{x \in X : x \text{ è dispari}\},$$

$$C = \{x \in X : x \text{ è multiplo di } 5\},$$

oppure se Y è l'insieme di tutti gli studenti dell'Università, possiamo definire gli insiemi

$$D = \{x \in Y : x \text{ è donna}\},$$

$$E = \{x \in X : x \text{ è uno studente di ingegneria}\},$$

e così via.
A questo punto possiamo dare le seguenti definizioni.

Definizione 2.2. Siano A, B due insiemi nell'universo X. Si chiama *unione* di A e B l'insieme[2]

$$A \cup B = \{x \in X : x \in A \vee x \in B\}. \tag{2.1}$$

e si chiama *intersezione* di A e B l'insieme

$$A \cap B = \{x \in X : x \in A \wedge x \in B\}. \tag{2.2}$$

[2]I connettivi logici $\vee$ e $\wedge$ si dicono rispettivamente *disgiunzione* e *congiunzione* e sostituiscono in linguaggio matematico le congiunzioni "o"ed "e"rispettivamente.

Tali definizioni hanno senso quando, tra gli insiemi possibili, si considerano anche tutto l'universo X e *l'insieme vuoto* $\emptyset$: tale insieme può essere pensato come un contenitore all'interno del quale non vi sia nulla (e non come se fosse nulla, errore abbastanza comune per altro!). In particolare, risulta che se A e B non hanno elementi in comune, allora $A \cap B = \emptyset$. Inoltre

$$A \cup B = \emptyset \Longleftrightarrow A = \emptyset \text{ e } B = \emptyset,$$

cioè l'unione di due insiemi è vuota se e solo se entrambi gli insiemi sono vuoti. Vale il seguente

Teorema 2.3. *Siano A, B, C insiemi nell'universo X. Allora*[3]

$$\begin{aligned} A \cup B = B \cup A, &\quad A \cap B = B \cap A \\ A \cup (B \cup C) = (A \cup B) \cup C, &\quad A \cap (B \cap C) = (A \cap B) \cap C, \\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C), &\quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\ A \cup \emptyset = A, &\quad A \cap \emptyset = \emptyset \\ A \cup X = X, &\quad A \cap X = A. \end{aligned}$$

Dimostrazione. Useremo come metodo di dimostrazione il Teorema della doppia inclusione, facendo vedere che preso un elemento qualsiasi in uno degli insiemi che appare nelle uguaglianze, esso compare anche nell'insieme all'altro membro.
Per le proprietà nella prima riga abbiamo

$$1)\ x \in A \cup B \Leftrightarrow x \in A \vee x \in B \Leftrightarrow x \in B \vee x \in A \Leftrightarrow x \in B \cup A.$$

$$2)\ x \in A \cap B \Leftrightarrow x \in A \wedge x \in B \Leftrightarrow x \in B \wedge x \in A \Leftrightarrow x \in B \cap A.$$

Per quelle della seconda riga si ha

$$3)\ x \in A \cup (B \cup C) \Leftrightarrow x \in A \ \vee \ x \in (B \cup C) \Leftrightarrow x \in A \ \vee \ x \in B \ \vee \ x \in C \Leftrightarrow$$
$$\Leftrightarrow x \in (A \cup B) \ \vee \ x \in C \Leftrightarrow x \in (A \cup B) \cup C.$$

$$4)\ x \in A \cap (B \cap C) \Leftrightarrow x \in A \ \wedge \ x \in (B \cap C) \Leftrightarrow x \in A \ \wedge \ x \in B \ \wedge \ x \in C \Leftrightarrow$$
$$\Leftrightarrow x \in (A \cap B) \ \wedge \ x \in C \Leftrightarrow x \in (A \cap B) \cap C.$$

Per la terza riga abbiamo

$$5)\ x \in A \cup (B \cap C) \Leftrightarrow x \in A \ \vee \ x \in (B \cap C) \Leftrightarrow$$
$$\Leftrightarrow (x \in A \ \wedge \ x \notin (B \cap C)) \ \vee \ (x \notin A \ \wedge \ x \in (B \cap C)) \ \vee \ (x \in A \ \wedge \ x \in (B \cap C)) \Leftrightarrow$$
$$\Leftrightarrow (x \in A \wedge x \notin B \wedge x \notin C)) \vee (x \notin A \wedge x \in B \wedge x \in C)) \vee (x \in A \wedge x \in B \wedge x \in C)) \Leftrightarrow$$
$$\Leftrightarrow (x \in (A \cup B) \wedge x \in (A \cup C)) \vee (x \in (A \cup B) \wedge x \in (A \cup C)) \vee (x \in (A \cup B) \wedge x \in (A \cup C)) \Leftrightarrow$$
$$\Leftrightarrow x \in (A \cup B) \cap (A \cup C).$$

$$6) x \in A \cap (B \cup C) \Leftrightarrow x \in A \ \wedge \ x \in (B \cup C) \Leftrightarrow$$
$$\Leftrightarrow (x \in A \wedge x \in B \wedge x \notin C) \vee (x \in A \wedge x \notin B \wedge x \in C) \vee (x \in A \wedge x \in B \wedge x \in C) \Leftrightarrow$$
$$\Leftrightarrow (x \in (A \cap B) \wedge x \notin (A \cap C)) \vee (x \notin (A \cap B) \wedge x \in (A \cap C)) \vee (x \in (A \cap B) \wedge x \in (A \cap C)) \Leftrightarrow$$

[3] Le proprietà della prima riga dicono che le operazioni di $\cup$ e $\cap$ sono *commutative*. La seconda riga riguarda la proprietà *assoiativa*, la terza quella *distributiva* dell'una rispetto all'altra, la quarta il fatto che $\emptyset$ sia *elemento neutro* dell'unione ed elemento *assorbente* dell'intersezione, la quinta che X sia elemento assorbente dell'unione ed elemento neutro dell'intersezione.

$$\Leftrightarrow x \in (A \cap B) \cup (A \cap C).$$

Per le ultime due righe osserviamo che in generale se $A \subseteq B$ allora

$$A \cup B = B, \qquad A \cap B = A.$$

Infatti

$$x \in A \cup B \Leftrightarrow x \in A \ \vee x \in B \Leftrightarrow$$
$$\Leftrightarrow (x \notin A \ \wedge \ x \in B) \ \vee \ (x \in A \ \wedge \ x \in B) \Leftrightarrow x \in B.$$

$$x \in A \cap B \Leftrightarrow x \in A \ \wedge \ x \in B \Leftrightarrow x \in A.$$

Ne seguono le identità alla quarta e quinta riga, essendo $\emptyset \subseteq A \subseteq X$. □

Consideriamo due insiemi A, B nell'universo X. Definiamo la *differenza* tra A e B come l'insieme

$$A \setminus B = \{x \in X : x \in A \ \wedge \ x \notin B\}.$$

Possiamo osservare che la differenza tra due insiemi non è commutativa: infatti, se ad esempio $A = \{1, 2, 3, 4\}$ e $B = \{3, 4, 5, 6\}$, allora

$$A \setminus B = \{1, 2\}, \qquad B \setminus A = \{5, 6\}.$$

Proposizione 2.4. *Siano A e B due insiemi nell'universo X. Allora*
(*i*) $A \setminus B = A \setminus (A \cap B)$*;*
(*ii*) *Se definiamo la* differenza simmetrica

$$A \Delta B = (A \setminus B) \cup (B \setminus A)$$

allora $A \Delta B = B \Delta A$.

Dimostrazione. (*i*) Abbiamo

$$x \in A \setminus (A \cap B) \Leftrightarrow x \in A \ \wedge \ x \notin A \cap B \Leftrightarrow x \in A \ \wedge \ x \notin B \Leftrightarrow x \in A \setminus B.$$

(*ii*) Per dimostrare che la differenza simmetrica è commutativa, possiamo ancora usare il Teorema della doppia inclusione, oppure procedere al modo seguente

$$B \Delta A = (B \setminus A) \cup (A \setminus B) = (A \setminus B) \cup (B \setminus A) = A \Delta B$$

dove nell'uguaglianza centrale abbiamo sfruttato il fatto che l'unione tra due insiemi è commutativa. □

Consideriamo un insieme A in un universo X: A si dice *sottoinsieme* di X. L'insieme

$$\mathcal{P}(X) = \{A : A \subseteq X\},$$

formato da tutti i sottoinsiemi di un insieme X si dice *insieme delle parti* di X. Si osservi che tale insieme ha come elementi degli insiemi. In particolare $\emptyset$ e X appartengono a $\mathcal{P}(X)$.
Se $X = \{1, 2, 3\}$ allora

$$\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, X\}.$$

Se indichiamo con $|X|$ la *cardinalità* di X, cioè il numero di elementi che costituiscono l'insieme X, allora abbiamo il seguente teorema.

Teorema 2.5. *Sia X un insieme. Allora $|\mathcal{P}(X)| = 2^{|X|}$.*

Sia A un sottoinsieme nell'universo X. L'insieme

$$A^c = X \setminus A$$

si dice *complementare* di A in X. In particolare se $A \in \mathcal{P}(X)$ allora $A^c \in \mathcal{P}(X)$. Si osservi poi che, per la stessa definizione,

$$\emptyset^c = X, \qquad X^c = \emptyset.$$

Il seguente teorema è di fondamentale importanza in teoria degli insiemi.

Teorema 2.6. *Sia X un insieme. Allora*

$$(A \cup B)^c = A^c \cap B^c \tag{2.3}$$

$$(A \cap B)^c = A^c \cup B^c, \tag{2.4}$$

per ogni $A, B \in \mathcal{P}(X)$.

Dimostrazione. Iniziamo con la prima. Abbiamo

$$x \in (A \cup B)^c \Leftrightarrow x \notin A \cup B \Leftrightarrow x \notin A \ \wedge \ x \notin B \Leftrightarrow$$

$$\Leftrightarrow x \in A^c \ \wedge \ x \in B^c \Leftrightarrow x \in A^c \cap B^c.$$

Analogamente per la seconda si ha

$$x \in (A \cap B)^c \Leftrightarrow x \notin A \cap B \Leftrightarrow$$

$$\Leftrightarrow (x \notin A \ \wedge \ x \in B) \ \vee \ (x \in A \ \wedge \ x \notin B) \ \vee \ (x \notin A \ \wedge x \notin B) \Leftrightarrow$$

$$\Leftrightarrow (x \in A^c \ \wedge \ x \notin B^c) \ \vee \ (x \notin A^c \ \wedge \ x \in B^c) \ \vee \ (x \in A^c \ \wedge \ x \in B^c) \Leftrightarrow$$

$$\Leftrightarrow x \in A^c \cup B^c,$$

e quindi la tesi. □

Siano A e B due insiemi nell'universo X. Si chiama *prodotto cartesiano* l'insieme

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

Se $B = A$ si suole scrivere A^2 al posto di $A \times A$. Vale il seguente teorema, che non dimostriamo.

Teorema 2.7. *Siano A_1, B_1, A, B, C degli insiemi. Allora*

$$A_1 \times B_1 \subseteq A \times B \Longleftrightarrow A_1 \subseteq A \ e \ B_1 \subseteq B,$$

$$A \times (B \cup C) = (A \times B) \cup (A \times C),$$

$$A \times (B \cap C) = (A \times B) \cap (A \times C),$$

$$(A \cup B) \times C = (A \times C) \cup (B \times C),$$

$$(A \cap B) \times C = (A \times C) \cap (B \times C).$$

3. Insiemi Numerici

3.1. **L'insieme dei numeri naturali $\mathbb{N}$.** L'insieme numerico più immediato da comprendere, nonché quello con cui veniamo a contatto nella maggioranza dei casi nella vita quotidiana, è quello dei numeri naturali $\mathbb{N}$. Lungi dal volerne dare una definizione assiomatica precisa, possiamo indicare tale insieme elencando i suoi elementi

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, \ldots\},$$

dove i puntini suggeriscono come continuare in modo ovvio tale sequenza numerica. Una descrizione completa dell'insieme dei numeri naturali non è possibile, a causa dell'infinità di elementi in esso contenuti. Infatti, supponiamo che N sia il più grande numero naturale esistente. Ma allora $N + 1$ è ancora un numero naturale[4] e quindi l'ipotesi che ne esista uno più grande di tutti gli altri è assurda: ne segue che $\mathbb{N}$ ha cardinalità infinita che indicheremo con $|\mathbb{N}|$.

Una questione fondamentale quando si opera con gli insiemi numerici è quella di definire le operazioni binarie[5] tra i suoi elementi. All'interno dei numeri naturali è pissibile definire come è noto le due operazioni seguenti:

(i) *l'addizione* $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, $(n, m) \mapsto n + m$, la quale gode delle proprietà associativa e commutativa e per la quale lo zero è l'elemento neutro ($n + 0 = n$);

(ii) *la moltiplicazione* $\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, $(n, m) \mapsto n \cdot m$, la quale gode delle proprietà associativa e commutativa e per la quale 1 è l'elemento neutro ($n \cdot 1 = n$).

Inoltre, le due operazioni qui definite, soddisfano la legge distributiva

$$(n + m) \cdot r = n \cdot r + m \cdot r.$$

Una classe molto importante di numeri naturali è quella dei *numeri primi*: come le lettere di una lingua formano le parole essenziali al linguaggio, così i numeri primi risultano essere i costituenti fondamentali di tutti i numeri.

Un numero p è primo se esso è divisibile solo per 1 e per se stesso. Un elenco dei primi numeri primi[6] è: $2, 3, 5, 7, 11, 13, 17, 19, \ldots$. Per essi vale il *Teorema Fondamentale dell'aritmetica*: *Ogni numero naturale si decompone, in modo unico, in prodotto di fattori primi.*

Mentre non dimostriamo tale risultato, vogliamo dare la dimostrazione del seguente fatto, noto già ad Euclide, la cui dimostrazione è, probabilmente, la più elegante dall'inizio della Matematica ad oggi!

Teorema 3.1 (Dei numeri Primi)**.** *I numeri primi sono infiniti.*

Dimostrazione. Proviamo questo fatto per assurdo. Supponiamo allora che i numeri primi siano in numero finito, e sia tale quantità pari a N. Indichiamo allora i numeri primi come $\{p_1, p_2, \ldots, p_N\}$. Consideriamo allora il seguente numero:

$$P = p_1 \cdot p_2 \cdot \ldots \cdot p_N + 1.$$

---

[4] In effetti, i numeri naturali si definiscono proprio a partire da 1 e aggiungendo ogni volta 1 o, come si usa dire, passando all'elemento successivo.

[5] Se A è un insieme, una *operazione binaria* su esso è una legge

$$* : A \times A \longrightarrow A, \qquad (a, b) \mapsto a * b$$

che ad ogni coppia di elementi (a, b) associa un nuovo elemento $c = a * b$ di A.

[6] Spero si perdonerà l'involontario gioco di parole!

Tale numero è ancora un numero naturale, in quanto prodotto e somme di numeri naturali. Ora, se proviamo a dividere P per qualsiasi numero primo nel nostro elenco, otterremo sempre come resto 1: ciò implica che P non è divisibile da nessun numero primo noto. Ci sono allora 2 possibilità:

(i) esiste un numero primo al di fuori del nostro elenco che divide P,

(ii) P è primo.

In entrambi i casi, risulta che i numeri primi che abbiamo elencato non sono tutti (in entrambi i casi troviamo almeno un nuovo numero primo) e ciò significa che il loro numero totale non è N. Data l'arbitrarietà della scelta del numero N, ciò implica che i numeri primi sono infiniti. □

Il Teorema fondamentale dell'aritmetica permette di definire anche i concetti di *Massimo Comune Divisore* (M.C.D.) e di *minimo comune multiplo* (m.c.m) tra due numeri naturali. Infatti, essendo ogni numero decomponibile in modo unico quale prodotto di primi distinti, il M.C.D. e il m.c.m. sono definiti al modo seguente:

(i) M.C.D.: si prendono tutti i primi comuni nelle fattorizzazioni, ciascuno con l'esponente più piccolo con cui compare nelle fattorizzazioni;

(ii) m.c.m.: si prendono tutti i fattori primi comuni e non comuni nelle fattorizzazioni, ciascuno con l'esponente più alto con cui compare nelle fattorizzazioni.

Consideriamo ora su $\mathbb{N}$ una proprietà P dipendente dal numero naturale n. Il *principio di induzione* è un utile metodo di dimostrazione che permette di affermare se la proprietà in esame vale per ogni numero naturale. Esso si enuncia al modo seguente:

Supponiamo che la proprietà $P(n)$ abbia le seguenti caratteristiche:

(i) $P(0)$ è vera;

(ii) se $P(n)$ è vera, allora lo è anche $P(n+1)$.

Allora la proprietà $P(n)$ è vera per qualsiasi numero naturale.

Un esempio sull'utilità del principio di induzione è il seguente:

Vogliamo dimostrare la seguente identità

$$\sum_{k=1}^{n} k = 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}.$$

In base al principio di induzione, dimostriamo inanzitutto la validità di tale tesi per $n = 1$. Infatti

$$\sum_{k=1}^{1} k = 1 = \frac{1 \cdot (1+1)}{2},$$

e quindi la base dell'induzione è vera. Supponiamo ora che l'identità sia vera per n e dimostriamo che sia vera anche per $n+1$. Dobbiamo mostrare che

$$\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}.$$

Ora

$$\sum_{k=1}^{n+1} k = \sum_{k=1}^{n} k + (n+1) = \frac{n(n+1)}{2} + (n+1) =$$

$$= \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2},$$

che è quanto volevamo dimostrare. In base al principio di induzione possiamo concludere che l'identità vale per ogni numero naturale.

3.2. **L'insieme dei numeri interi $\mathbb{Z}$.** Nel precedente abbiamo definito le operazioni binarie in $\mathbb{N}$. Si osservi che l'operazione di sottrazione e divisione in $\mathbb{N}$ non possono essere definite: ad esempio $4-8$ e $5:2$ sono numeri che non rientrano nell'insieme dei numeri naturali. Per risolvere tale problema, è necessario "costruire"nuovi insiemi numerici di cui i precedenti siano sottoinsiemi.

Il passo successivo alla costruzione di $\mathbb{N}$ e quello di costruire i numeri interi $\mathbb{Z}$:

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \ldots\}.$$

Anche in questo caso abbiamo definito l'insieme scrivendone i primi elementi e lasciando al compito dei puntini di dare l'idea di quali siano tutti gli altri elementi. Sappiamo infatti che anche l'insieme dei numeri interi è costituito da infiniti elementi. Ma quanti sono? Sono di più dei naturali?

La risposta sorprendente a questo quesito è che

$$|\mathbb{Z}| = |\mathbb{N}|,$$

cioè i numeri interi sono tanti quanti i naturali. Per vedere questo fatto, basta considerare la seguente tabella:

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	9	10	...
$\mathbb{Z}$	0	1	-1	2	-2	3	-3	4	-4	5	-5	...

In pratica, se associamo ad ogni numero positivo un numero naturale dispari e ad ogni numero negativo un naturale pari, possiamo contare tutti i numeri interi, così come contiamo i numeri naturali. Ne segue che le cardinalità dei due insiemi sono le stesse. Definiamo la relazione seguente da $\mathbb{Z}$ a $\mathbb{N}$:

$$\phi : \mathbb{Z} \to \mathbb{N},$$

$$\phi(z) = \begin{cases} 2z-1 & \text{se } z > 0 \\ 0 & \text{se } z = 0 \\ -2z & \text{se } z < 0 \end{cases}$$

La legge ϕ rappresenta, in modo formale, la legge precedentemente enunciata nella tabella. Ritorneremo su tali tipi di leggi nella prossima lezione.

Se $z \in \mathbb{Z}$, definiamo il *valore assoluto* di z la quantità

$$|z| = \begin{cases} z & z > 0 \\ 0 & z = 0 \\ -z & z < 0 \end{cases}$$

Sull'insieme $\mathbb{Z}$ possono definirsi le stesse operazioni binarie date sui naturali: tuttavia in questo caso l'addizione gode della seguente ulteriore proprietà

(i) *per ogni $z \in \mathbb{Z}$ esiste un unico elemento $z' \in \mathbb{Z}$ tale che $z + z' = 0$; tale elemento si indica con $z' = -z$ e viene detto* opposto *di z.*

Grazie a questa proprietà è possibile definire la differenza in $\mathbb{Z}$ al modo seguente: $a - b$ vuol dire semplicemente $a + (-b)$, cioè sommare ad a l'opposto dell'elemento b.

Sebbene sugli interi ancora non abbia senso definire la divisione, un risultato fondamentale in tale direzione è dato dal seguente lemma.

Teorema 3.2. *(Lemma di divisione Euclidea) Siano $a, b \in \mathbb{Z}$. Allora esistono unici due elementi $q \in \mathbb{Z}$ e $0 \leqslant r < |a|$ tali che $b = qa + r$.*

Il numero q si chiama *quoziente* della divisione di b per a e il numero r *resto* della divisione di b per a.

4. L'insieme dei numeri razionali $\mathbb{Q}$

Il passo successivo è quello di definire un insieme numerico all'interno del quale abbia senso il concetto di divisione. Definiamo l'insieme dei numeri razionali $\mathbb{Q}$ come l'insieme

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z} \right\}.$$

Anche in questo caso ci chiediamo quanti siano gli elementi di tale insieme. La risposta, sorprendente come in precedenza, è che $|\mathbb{Q}| = |\mathbb{N}|$. Per far vedere questo fatto, procediamo nel modo seguente. Costruiamo la seguente tabella:

$$\begin{array}{cccccccc}
1/1 & 1/2 & 1/3 & 1/4 & 1/5 & 1/6 & \cdots \\
2/1 & 2/2 & 2/3 & 2/4 & 2/5 & 2/6 & \cdots \\
3/1 & 3/2 & 3/3 & 3/4 & 3/5 & 3/6 & \cdots \\
4/1 & 4/2 & 4/3 & 4/4 & 4/5 & 4/6 & \cdots \\
5/1 & 5/2 & 5/3 & 5/4 & 5/5 & 5/6 & \cdots \\
6/1 & 6/2 & 6/3 & 6/4 & 6/5 & 6/6 & \cdots \\
7/1 & 7/2 & 7/3 & 7/4 & 7/5 & 7/6 & \cdots
\end{array}$$

Possiamo ordinare i numeri nel modo seguente, eliminando le copie:

$$1,\ 1/2,\ 2,\ 3,\ 1/3,\ 1/4,\ 2/3,\ 3/2,\ 4,\ 5,\ 1/5,$$

$$1/6,\ 2/5,\ 3/4,\ 4/3,\ 5/2,\ 6,\ 7,\ 5/3,\ 3/5, \ldots$$

A questo punto, associando ogni numero positivo con un numero dispari e il suo corrispondente negativo con uno pari otteniamo una relazione che collega ogni numero razionale ad un numero naturale.

Anche su $\mathbb{Q}$ si definiscono le stesse leggi binarie definite in precedenza. In questo caso, tuttavia, la moltiplicazione gode di una ulteriore proprietà:

(*i*) *per ogni $x \in \mathbb{Q} \setminus \{0\}$ esiste un unico elemento $x' \in \mathbb{Q}$ tale che $xx' = 1$; tale elemento si indica con $x' = 1/x$ e si chiama* reciproco[7] *di x.*

5. L'insieme dei numeri reali $\mathbb{R}$

A questo punto, parrebbe che tutti i problemi relativi alla definizione delle operazioni aritmetiche siano conclusi. Tuttavia, sebbene non vi siano più problemi "qualitativi", ne cominciano a sorgere alcuni di natura diversa, ad esempio quelli "quantitativi". Per spiegare ciò che intendiamo, guardiamo la seguente affermazione.

Proposizione 5.1. $\sqrt{2} \notin \mathbb{Q}$.

Dimostrazione. Supponiamo per assurdo che $\sqrt{2} \in \mathbb{Q}$, cioè che esistano a, b primi tra loro ($M.C.D(a, b) = 1$) tali che $\sqrt{2} = a/b$. Ne segue che $a = \sqrt{2}b$. Abbiamo allora, supponendo anche a, b entrambi positivi

$$a = \sqrt{2}b \Leftrightarrow a^2 = 2b^2.$$

[7] E non inverso di x, come spesso si usa chiamare tale numero negli Istituti Superiori!

Ora, l'ultima uguaglianza afferma che a^2 è un numero pari. Ma ciò vuol dire che anche a è pari, poiché il quadrato di un numero dispari è dispari. Segue che esiste a_1 tale che $a = 2a_1$. Ma allora $4a_1^2 = 2b^2$ e quindi $2a_1^2 = b^2$. Quest ultima identità implica che, per lo stesso motivo precedente, anche b sia pari. Ma avevamo supposto che a, b sono primi fra loro, mentre abbiamo appena visto che, essendo entrambi pari, devono avere almeno come divisore comune 2. Quindi siamo pervenuti ad un assurdo. Ne segue che il numero $\sqrt{2}$ non si può scrivere come rapporto di due numeri interi e quindi non è razionale. □

Il fatto che $\sqrt{2}$ non sia razionale, implica che esistano numeri all'infuori dell'insieme $\mathbb{Q}$. Per includere tali numeri, si introduce l'insieme $\mathbb{R}$ dei numeri reali. Darne una costruzione assiomatica, o un elenco degli elementi, in questa sede risulta praticamente impossibile[8]. Ciò che possiamo dire, invece, è che in questo caso i numeri da aggiungere ai razionali per ottenere i reali è talmente vasto che si ha $|\mathbb{R}| = \aleph_0 > |\mathbb{N}|$. Per mostrare questo fatto, procediamo come segue.

Supponiamo che $\mathbb{R}$ abbia la stessa cardinalità di $\mathbb{N}$ e supponiamo di aver già ordinato tutto i numeri reali di $\mathbb{R}$. Consideriamo allora la sequenza di tutti i numeri reali $\{a_1, a_2, a_3, \ldots\}$ e costruiamo il numero z la cui parte non intera è costruita al modo seguente: la cifra alla posizione k differisce dalla corrispondente del numero a_k di uno. È immediato verificare che tale numero z non appartiene alla sequenza ordinata di tutti i numeri reali, ciononostante è anch'esso un numero reale. Ne segue che l'ordinamento che abbiamo cotruito è errato e quindi che $\mathbb{R}$ ha cardinalità diversa da quella di $\mathbb{N}$.

All'interno dei numeri reali è possibile definire poi una particolare classe di insiemi detti *intervalli*. I più comuni vengono indicati con le seguenti notazioni:

$$
\begin{aligned}
[a, b] &= \{x \in \mathbb{R} : a \leqslant x \leqslant b\},\\
[a, b) &= \{x \in \mathbb{R} : a \leqslant x < b\},\\
(a, b] &= \{x \in \mathbb{R} : a < x \leqslant b\},\\
(a, b) &= \{x \in \mathbb{R} : a < x < b\},\\
[a, +\infty) &= \{x \in \mathbb{R} : a \leqslant x\},\\
(a, +\infty) &= \{x \in \mathbb{R} : a < x\},\\
(-\infty, b] &= \{x \in \mathbb{R} : x \leqslant b\},\\
(-\infty, b) &= \{x \in \mathbb{R} : x < b\}.
\end{aligned}
$$

5.1. **Quanti numeri?** I ragionamenti fin qui fatti potrebbero proseguire. In effetti è possibile costruire nuovi insiemi numerici a partire dall'insieme $\mathbb{R}$ ampliando ulteriormente questa classe[9]. Si osservi che gli insiemi qui definiti risultano uno espansione dell'altro, nel senso che

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Osserviamo che l'inclusione stretta afferma che ci sono elementi nell'insiemi a destra del simbolo non presenti nell'insiemi a sinistra del simbolo stesso. Questo ovviamente potrebbe portare ad un pensiero erroneo: significa allora che $\mathbb{Z}$ e $\mathbb{Q}$ in realtà hanno più elementi di $\mathbb{N}$ e che quindi le loro cardinalità siano diverse?

[8] Ma verrà fatto al corso di Analisi 1.

[9] Nel corso delle ultime lezioni vedremo un esempio di tale costruzione.

La risposta è abbastanza semplice: in effetti gli elementi di $\mathbb{Z}$, ad esempio, sono il doppio di quelli di $\mathbb{N}$, poiché gli interi contengono due copie di ogni numero naturale, una positiva e una negativa. Tuttavia, la cardinalità "conta"gli elementi di un insieme infinito nel senso di riuscire a determinare una procedura per poter affermare se ci sia o meno un ordinamento cardinale degli elementi, ovvero se sia possibile dire quale sia il primo, il secondo, il terzo numero e via discorrendo, così come accade in $\mathbb{N}$ in cui 1 è il primo elemento, 2 il secondo ecc. Questo non accade nei numeri reali, in quanto sebbene sia possibile determinare il maggiore tra due numeri, non è possibile decidere quale dei due occupi la posizione n-ima come all'arrivo di una gara ciclistica!

Infine, ci si può chiedere se la cardinalità di $\mathbb{R}$, che viene indicata con $\aleph_0$ (si legge *alef zero*), e viene detta *potenza del continuo*, sia la più grande possibile. Un matematico del secolo scorso, George Cantor, ipotizzò che il prodotto cartesiano di $\mathbb{R}$ per se stesso avesse cardinalità superiore, ma ciò si rivelò falso, anzi egli stesso dimostrò che

$$|\underbrace{\mathbb{R} \times \ldots \times \mathbb{R}}_{n-\text{volte}}| = |\mathbb{R}|,$$

per ogni $n \in \mathbb{N}$. Tuttavia, alcuni anni dopo, Cantor fece una sensazionale scoperta: l'insieme $\mathcal{P}(\mathbb{R})$ ha una cardinalità superiore a quella di $\mathbb{R}$ e questo permise di costruire insiemi di cardinalità infinita sempre più grande.