Rita Procesi Rosaria Rota

ELEMENTI
DI
ALGEBRA
E
MATEMATICA DISCRETA

ACCADEMICA

Prof.ssa Rita Procesi
Dipartimento di Matematica “Guido Castelnuovo” Università di Roma “La Sapienza”
Piazzale Aldo Moro. 5 - 00185 Roma

Prof.ssa Rosaria Rota
Dipartimento di Matematica
Università di Roma Tre
Largo Murialdo, 2 - 00146 Roma

www.accademica.it

e-ISBN 978-88-85929-64-7 ISBN 978-88-85929-11-7

Procesi, Rita – Rota, Rosaria: Elementi di Algebra e Matematica discreta

Prefazione

Lo scopo di questo testo è quello di fornire allo studente alcune nozioni di base di algebra moderna e di matematica discreta.

Vengono innanzitutto presentate le prime nozioni di logica matematica; in seguito, dopo aver esaminato alcune delle più importanti proprietà degli insiemi numerici, si passa allo studio delle principali strutture algebriche.

Il libro si conclude con un capitolo dedicato all'esame dei concetti fondamentali di teoria dei grafi.

LISTA DEI SIMBOLI

alfa= α, A	beta= β, B	gamma= γ, Γ	delta= δ, Δ
epsilon= ϵ, E	zeta = ζ, Z	eta= η, H	teta= $\vartheta = \theta, \Theta$
iota= ι, I	kappa= κ, K	lambda=λ, Λ	mi(mu)=μ, M
ni(nu)=ν, N	csi= ξ, Ξ	omicron=o,O	pi=π, Π
ro=ρ, P	sigma = σ, Σ	tau= τ, T	upsilon= υ, Υ
fi=φ, Φ	chi= χ, X	psi= ψ, Ψ	omega= ω, Ω

$\Rightarrow$	implica	$\Leftrightarrow$	se e solo se
/	tale che	:	tale che
$\exists$	esiste	$\exists!$	esiste unico
$\forall$	per ogni	$\emptyset$	insieme vuoto
$-$	differenza fra insiemi	$\in$	appartenente
$\notin$	non appartenente	$\ni$	contenente
$\subseteq$	sottoinsieme	$\subset$	sottoinsieme proprio
$\geq$	maggiore o eguale	$\leq$	minore o eguale
$\neq$	diverso		
$\mathbb{N}$	numeri naturali	$\mathbb{Z}$	numeri interi relativi
$\mathbb{Q}$	numeri razionali	$\mathbb{R}$	numeri reali
$\mathbb{C}$	numeri complessi		
A^+	positivi in A (A=$\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$)	A^-	negativi in A (A=$\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$)
A^*	$A\backslash\{0\}$	$m\mathbb{Z}$	multipli interi di m
$a \mid b$	a divide b		
$a \equiv b \bmod(m)$ ($a \equiv_m b$)	a congruo a b modulo m		
$\mathbb{Z}_m$	classi resto modulo m		

Indice

CAPITOLO 1

ELEMENTI DI LOGICA

1.1

In questo capitolo fisseremo la nostra attenzione sui metodi e sui principi usati per ragionare correttamente. Partiremo considerando espressioni per le quali ha senso dire se siano vere o false; queste espressioni sono dette *proposizioni* o *enunciati*. A queste proposizioni si associano i simboli V o F, *vero* o *falso*, detti *valori di verità*.

Ad esempio la proposizione "Parigi è in Francia" è vera, mentre la proposizione "3+5=10" è falsa.

Abbiamo già visto che si possono eseguire operazioni con i numeri e con gli insiemi, per esempio $+, \cdot, \cup, \times$; facciamo vedere come si possa operare anche con le proposizioni. Si può operare su un solo enunciato o connettere due o più proposizioni tramite *connettivi* ed ottenere nuove proposizioni dette *proposizioni composte* o *funzioni proposizionali*.

Innanzitutto possiamo considerare *l'operatore di negazione*, che opera su di un enunciato e, ad esso, fa corrispondere la sua negazione; tale operatore si denota con il simbolo $\neg$. Ad esempio, se p è la proposizione "Parigi è in Francia", la proposizione $\neg p$ è "Parigi non è in Francia". Inoltre due o più enunciati possono essere collegati fra loro mediante i connettivi: "e", "o", "se ... allora", "se e solo se". Questi connettivi sono detti rispettivamente *congiunzione*, *disgiunzione*, *implicazione*, *doppia implicazione* e vengono denotati con i simboli $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$.

Esempi di proposizioni ottenute operando con i seguenti connettivi sono:

1) Francesco studia Analisi Matematica "e" Lorella studia Geometria.

2) Francesco studia Analisi Matematica "o" Lorella studia Geometria.

3) Se un numero naturale è divisibile per 4 "allora" è pari.

4) Il numero naturale p è primo "se, e solo se," esso è divisibile soltanto per 1 e per se stesso.

La parte della logica che si occupa delle operazioni fra proposizioni si dice *calcolo delle proposizioni*; il problema di cui si occupa il calcolo delle proposizioni è quello di stabilire il valore di verità delle proposizioni composte a partire dal valore di verità delle proposizioni che le costituiscono. Studiamo ora più dettagliatamente le operazioni fra enunciati; denoteremo con $\mathcal{P}$ l'insieme delle proposizioni.

Definizione 1.1.1 Si definisce *congiunzione* l'operazione $\wedge : \mathcal{P} \times \mathcal{P} \to \mathcal{P}$ che associa, alla coppia (p, q) di proposizioni, la proposizione composta $p \wedge q$ che è vera se p e q sono vere e falsa in ogni altro caso.

Esempio 1.1.1 La proposizione $p \wedge q$ "Francesco studia Analisi Matematica e Lorella studia Geometria", composta delle due proposizioni p "Francesco studia Analisi Matematica" e q "Lorella studia Geometria" è vera se contemporaneamente Francesco studia Analisi Matematica e Lorella studia Geometria, mentre è falsa sia se Francesco studia Analisi Matematica, ma Lorella non studia Geometria, sia se Francesco non studia Analisi Matematica e Lorella studia Geometria, sia se Francesco non studia Analisi Matematica e Lorella non studia Geometria.

Per visualizzare questo caso lo studente può pensare a due interruttori messi in serie, in questa situazione la corrente può passare solamente se entrambi gli interruttori sono aperti.

I valori di verità delle proposizioni composte vengono schematizzati con tabelle, dette *tavole di verità*; nel caso della congiunzione, dalla definizione segue che la sua tavola di verità è:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

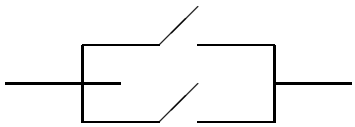
Definizione 1.1.2 Si definisce *disgiunzione* l'operazione $\vee : \mathcal{P} \times \mathcal{P} \to \mathcal{P}$ che associa, alla coppia (p, q) di proposizioni, la proposizione composta $p \vee q$ che è vera se almeno una delle due proposizioni p e q è vera.

In base a tale definizione, la tavola di verità della disgiunzione è:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Esempio 1.1.2 Sia p la proposizione "25 è un multiplo di 5" e sia q la proposizione "25 è un numero pari"; la proposizione composta $p \vee q$ "25 è un multiplo di 5 o 25 è un numero pari" è vera in quanto la proposizione p è vera.

Ripetendo l'esempio degli interruttori in questo caso lo studente può pensare a due interruttori messi in parallelo; in questa situazione la corrente può passare purché almeno uno degli interruttori risulti essere aperto.



Definizione 1.1.3 Si definisce *negazione* l'operazione $\neg : \mathcal{P} \to \mathcal{P}$ che alla proposizione p associa la proposizione $\neg p$ che è vera se p è falsa ed è falsa se p è vera. Si tratta quindi della proposizione la cui tavola di verità risulta essere:

p	$\neg p$
V	F
F	V

Osserviamo che, mentre la congiunzione e la disgiunzione sono operazioni binarie (ovvero operano su due proposizioni), la negazione è un'operazione che opera su una sola proposizione (operazione unaria).

Esempio 1.1.3 Siano p la proposizione "un quadrato è un poligono regolare" e q la proposizione "Napoleone Bonaparte è nato a Roma"; queste due proposizioni sono una vera e una falsa. La proposizione composta $p \wedge q$, ovvero "un quadrato è un poligono regolare e Napoleone Bonaparte è nato a Roma", è falsa, mentre la proposizione composta $p \vee q$, ovvero "un quadrato è un poligono regolare o Napoleone Bonaparte è nato a Roma", è vera. Osserviamo inoltre che le proposizioni $\neg p$ e $\neg q$ sono rispettivamente falsa e vera.

Vogliamo a questo punto notare che il significato di "e", "o" e "non" in logica vengono usati in modo molto rigoroso, mentre nel linguaggio comune si accettano sfumature e imprecisioni. Ad esempio la frase "Luca studia Geometria e va al cinema" ha un evidente significato di "eventi in successione" prima Luca studia Geometria e poi va al cinema, mentre la "e" logica ha cempre un significato di "e contemporaneamente". In logica $\neg(\neg p) = p$, mentre nel linguaggio comune il senso della frase "non ho nessuna fretta" è equivalente (o addirittura è un rafforzativo) a quello della frase "non ho fretta".

Prendiamo ora in esame altri due modi di comporre due proposizioni.

Definizione 1.1.4 Si definisce *implicazione* di due proposizioni p e q, l'operazione binaria $\rightarrow$: $\mathcal{P} \times \mathcal{P} \rightarrow \mathcal{P}$ che, alla coppia (p, q) di proposizioni, associa la proposizione composta $p \rightarrow q$ (p implica q) che è falsa soltanto se p è vera e q è falsa, ovvero la cui tavola di verità è:

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

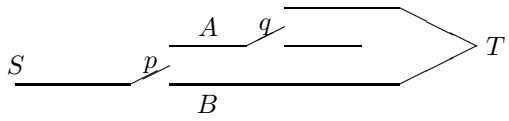
In questo caso si nota maggiormente la differenza fra l'uso che si fa, nel linguaggio comune, di questo tipo di connettivo e la definizione appena data, come ben si vede nel seguente esempio.

Esempio 1.1.4 Sia p la proposizione "2 è un numero dispari" e sia q la proposizione "Roma è la capitale d'Italia"; queste due proposizioni sono una falsa e una vera; pertanto la proposizione composta $p \rightarrow q$, è vera.

Ovviamente nel linguaggio ordinario l'affermazione "se 2 è un numero dispari allora Roma è la capitale d'Italia" è completamente priva di senso. Non dobbiamo quindi confondere l'implicazione $p \rightarrow q$ con l'implicazione logica, che si denota con il simbolo $\Rightarrow$ e che richiede una effettiva dipendenza fra le proposizioni coinvolte; di tale implicazione parleremo successivamente.

Possiamo provare a schematizzare la situazione con uno scambio ferroviario; pensiamo ad un binario che, partendo da una stazione S, ad un certo punto si divide in due binari A e B con uno scambio, la proposizione p. Supponiamo inoltre che sulla tratta A sia presente un ulteriore scambio, la proposizione q, che in una posizione (q vera schematizzata con l'interruttore aperto) porti a confluire, senza alcuno scambio, con la tratta B in un unico

binario fino a giungere alla stazione T. In tale situazione un treno che parte da S non arriva a T soltanto se imbocca, sulla tratta A, lo scambio q falsa.



Osservazione 1.1.1 Osserviamo che l'operazione di implicazione $p \to q$ ha la stessa tavola di verità dell'operazione $p \vee \neg q$; infatti risulta:

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

Definizione 1.1.5 Si definisce *doppia implicazione* di due proposizioni p e q, l'operazione binaria $\leftrightarrow$: $\mathcal{P} \times \mathcal{P} \to \mathcal{P}$ che, alla coppia (p, q) di proposizioni, associa la proposizione composta $p \leftrightarrow q$ (p se e solo se q) che è falsa se p e q hanno valori di verità diversi. La tavola di verità dell'operazione $\leftrightarrow$ è quindi:

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Osserviamo che, al contrario dell'implicazione $\to$, la doppia implicazione gode della proprietà commutativa.

Operando tra più proposizioni, sia semplici che composte, si ottengono nuove proposizioni il cui valore di verità dipende dai valori di verità delle singole proposizioni.

Esempio 1.1.5 Si considerino le proposizioni p e q e la proposizione composta $p \vee q$; vogliamo stabilire il valore di verità della seguente proposizione: $(p \vee q) \wedge q$. A tal fine costruiamo la sua tavola di verità che è la seguente:

p	q	$p \vee q$	$(p \vee q) \wedge q$
V	V	V	V
V	F	V	F
F	V	V	V
F	F	F	F

Definizione 1.1.6 Si dice *tautologia* una proposizione composta che è vera sempre, indipendentemente dai valori di verità delle proposizioni che la compongono.

Esempio 1.1.6 Si considerino le proposizioni p, q e $p \wedge q$; allora la proposizione $p \wedge q \rightarrow p$ è una tautologia come mostra la sua tavola di verità:

p	q	$p \wedge q$	$(p \wedge q) \rightarrow p$
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	V

Definizione 1.1.7 Si dice *contraddizione* una proposizione che è sempre falsa, indipendentemente dai valori di verità delle proposizioni che la compongono.

Esempio 1.1.7 Se si considera una qualunque proposizione p, la formula proposizionale $p \wedge (\neg p)$ è una contraddizione; infatti la sua tavola di verità è:

p	$\neg p$	$p \wedge (\neg p)$
V	F	F
F	V	F

Osservazione 1.1.2 Se consideriamo una proposizione composta, nella quale compaiono n proposizioni semplici, la sua tavola di verità sarà composta da 2^n righe; poiché sull'ultima colonna, quella che fornisce il valore di verità della proposizione composta, si possono avere due valori per ogni riga le possibili tavole di verità della proposizione sono 2^{2^n}.

Consideriamo ora un insieme non vuoto E; per indicare che un elemento $a \in E$ gode della proprietà p scriveremo $p(a)$, ovvero diremo che l'elemento a gode della proprietà p se, e solo se, la proposizione $p(a)$ è vera.

Se consideriamo l'espressione $p(x)$, con x variabile in E, non ha senso chiedersi se sia vera o falsa perché non si sa chi è x; pertanto $p(x)$ non è un enunciato, ma un *predicato* ovvero una *forma proposizionale* su E.

Una forma proposizionale diventa un enunciato sostituendo alla variabile x un determinato elemento di E; ad esempio, se come insieme E consideriamo l'insieme $\mathbb{Z}$ degli interi relativi, l'espressione $x^2 - 12 \geq 0$ non è un enunciato, ma una forma proposizionale, mentre $3^2 - 12 \geq 0$ e $4^2 - 12 \geq 0$ sono due proposizioni, una falsa e una vera.

Un particolare modo per trasformare una forma proposizionale in un enunciato si ottiene affermando che ogni elemento di E gode della proprietà p. Per indicare che tutti gli elementi di E godono della proprietà p si scrive: $\forall\ x \in E : p(x)$; per indicare che esiste almeno un x che gode della proprietà p si scrive: $\exists\ x \in E\ /\ p(x)$. I due simboli $\forall$ e $\exists$ prendono il nome di *quantificatori* ; in particolare $\forall$ viene detto *quantificatore universale*, $\exists$ *quantificatore esistenziale.*

Esempio 1.1.8 Se nell'insieme $\mathbb{N}$ si considera la forma proposizionale $x^2 = 4$, essa si può trasformare in una proposizione al modo seguente: $\exists\ x \in \mathbb{N}\ /\ x^2 = 4$; tale proposizione si legge "esiste x appartenente a $\mathbb{N}$ tale che $x^2 = 4$" ed è ovviamente vera. La stessa forma proposizionale si può trasformare, con il quantificatore universale, in un'altra proposizione: $\forall\ x \in \mathbb{N} : x^2 = 4$ che si legge "per ogni x appartenente a $\mathbb{N}$ risulta $x^2 = 4$" e che è ovviamente falsa. Se si considera invece, nell'insieme $\mathbb{R}$ dei numeri reali, la forma proposizionale $\sqrt[3]{x} \in \mathbb{R}$, essa si trasforma, con entrambi i quantificatori, in una proposizione vera; infatti $\forall\ x \in \mathbb{R} : \sqrt[3]{x} \in \mathbb{R}$ ed ovviamente $\exists\ x \in \mathbb{R}\ /\ \sqrt[3]{x} \in \mathbb{R}$.

Siano ora $p(x)$ e $q(x)$ due forme proposizionali su un insieme E; si dice che $p(x)$ *implica logicamente* $q(x)$, e si scrive $p(x) \Rightarrow q(x)$, se per ogni $x \in E$ per cui $p(x)$ è vera anche $q(x)$ è vera.

Esempio 1.1.9 Sia $\mathbb{N}$ l'insieme dei numeri naturali e siano rispettivamente $p(x)$ e $q(x)$ le seguenti forme proposizionali su $\mathbb{N}$:

$$p(x) : x \text{ è un multiplo di } 21 \quad q(x) : x \text{ è un multiplo di } 7$$

Ovviamente ogni numero naturale multiplo di 21 risulta essere anche multiplo di 7 e quindi $p(x)$ implica logicamente $q(x)$, ovvero $p(x) \Rightarrow q(x)$. In questo caso questa implicazione logica si legge: "se un numero naturale è un multiplo di 21, allora esso è un multiplo di 7".

Osserviamo che in un'implicazione logica $p(x) \Rightarrow q(x)$ non possiamo scambiare le forme proposizionali, perché facendolo non è detto che si ottenga ancora un'implicazione logica.

Esempio 1.1.10 Nell'insieme $\mathbb{N}$ dei naturali, se $p(x)$ e $q(x)$ sono le forme proposizionali dell'esempio precedente, poiché ad esempio 49, che è un multiplo di 7, non è un multiplo di 21, $q(x)$ non implica logicamente $p(x)$, ovvero $p(x) \not\Rightarrow q(x)$.

Se per due forme proposizionali $p(x)$ e $q(x)$ in un insieme E risulta sia $p(x) \Rightarrow q(x)$ che $q(x) \Rightarrow p(x)$, si dice che $p(x)$ e $q(x)$ sono *logicamente equivalenti* e si scrive $p(x) \Leftrightarrow q(x)$; la scrittura $p(x) \Leftrightarrow q(x)$ si dice anche *doppia implicazione logica* e si legge "$p(x)$ è vera se, e solo se, $q(x)$ è vera".

Esempio 1.1.11 Nell'insieme $\mathbb{N}$ dei naturali, se $p(x)$ è la forma proposizionale "x è un numero pari" e $q(x)$ è la forma proposizionale "x è un multiplo di 2", risulta ovviamente che $p(x)$ e $q(x)$ sono logicamente equivalenti, ovvero $p(x) \Leftrightarrow q(x)$.

Osserviamo che, per quanto riguarda l'implicazione logica $p(x) \Rightarrow q(x)$, si dice che $p(x)$ è *condizione sufficiente* per $q(x)$ e che $q(x)$ è *condizione necessaria* per $p(x)$; nella doppia implicazione $p(x) \Leftrightarrow q(x)$ si dice che $p(x)$ è *condizione necessaria e sufficiente* per $q(x)$ (e viceversa $q(x)$ è *condizione necessaria e sufficiente* per $p(x)$).

Esempio 1.1.12 Nell'implicazione $p(x) \Rightarrow q(x)$ dove $p(x)$ è "x è un multiplo di 21" e $q(x)$ è "x è un multiplo di 7", risulta che $p(x)$ è condizione sufficiente per $q(x)$, ma non necessaria poiché $q(x)$ non implica logicamente $p(x)$.

La nozione di implicazione logica è fondamentale nella matematica; un teorema infatti è un'implicazione logica $I \Rightarrow T$ fra due proposizioni, I e T, dette *ipotesi* e *tesi* e la dimostrazione del teorema stesso è la verifica di tale implicazione. Tale dimostrazione consiste in una successione di implicazioni:

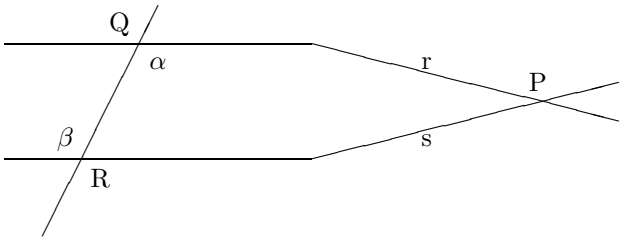
$$I_0 = I \Rightarrow I_1 \Rightarrow I_2 \Rightarrow \ldots \Rightarrow I_t = T,$$

dove I è l'ipotesi , T è la tesi e I_i è una funzione proposizionale, $\forall\ i$.

Un tipo di dimostrazione spesso usata in matematica è quella per assurdo; per dimostrare per assurdo l'implicazione $I \Rightarrow T$, oltre all'ipotesi si suppone vera la negazione della tesi, ovvero $\neg T$ e, da questo punto di partenza, si dimostra la negazione dell'ipotesi e cioè $\neg I$. Pertanto si dimostra l'implicazione $\neg T \Rightarrow \neg I$; non potendo però essere vere contemporaneamente I e $\neg I$, non può essere vera $\neg T$ e quindi deve essere vera la tesi T.

Esempio 1.1.13 Dimostriamo per assurdo che, se due rette tagliate da una trasversale formano angoli alterni interni uguali, allora sono parallele.

Dobbiamo dimostrare quindi l'implicazione $I \Rightarrow T$, dove l'ipotesi I è "$\alpha = \beta$" e la tesi T è "$r \parallel s$".



Ragioniamo per assurdo e supponiamo che le rette r e s non siano parallele e che quindi si incontrino in un punto P; allora l'angolo β esterno al triangolo di vertici P, Q e R è maggiore dell'angolo interno non adiacente α. Abbiamo così dimostrato che $\neg T \Rightarrow \neg I$, ovvero che la negazione della tesi ha portato alla negazione dell'ipotesi che si è supposta vera; pertanto non si può negare la tesi, che quindi risulta essere vera.

Terminiamo questo paragrafo con un'osservazione che mette in luce i collegamenti esistenti fra operazioni logiche e operazioni insiemistiche.

Osservazione 1.1.3 Se consideriamo un insieme E e due predicati, $p(x)$ e $q(x)$, possiamo definire due sottoinsiemi di E: $X = \{x \in E : p(x)\}$ e $Y = \{x \in E : q(x)\}$; appare allora evidente che le operazioni di unione e intersezione di sottoinsiemi corrispondono alle operazioni logiche $\wedge$ e $\vee$ rispettivamente, mentre l'operazione di complementare corrisponde all'operazione $\neg$. Risulta infatti:

$$X \cap Y = \{x \in E : p(x) \wedge q(x)\},$$

$$X \cup Y = \{x \in E : p(x) \vee q(x)\},$$

$$\mathcal{C}_E(X) = \{x \in E : x \notin X\} = \{x \in E : \neg p(x)\}.$$

CAPITOLO 2

CARDINALITA'

2.1

In questo capitolo cercheremo di chiarire due termini di uso comune di cui intuitivamente conosciamo il significato e cioé il concetto di "numero" e di "infinito". Vedremo come, dando una definizione abbastanza rigorosa di questi due termini, potremo risolvere alcuni problemi che erano stati posti già da Galileo Galilei nel XVII secolo. Osservava infatti il grande scienziato che gli interi che sono quadrati, come 0,1,4,9... etc., sono un sottoinsieme dell'insieme dei naturali, 0,1,2,3,.... e, nello stesso tempo "per ogni naturale esiste il suo quadrato ed ogni quadrato proviene da un solo naturale"; si perveniva quindi all'affermazione, che pareva assurda, che i quadrati sono "tanti quanti i naturali" pur essendo "di meno". Osserviamo che, quando consideriamo un numero naturale, ad esempio diciamo che un insieme ha "tre" elementi, stiamo considerando un insieme che può essere messo in corrispondenza biunivoca con un insieme standard $A = \{\Box, \diamond, \triangle\}$; generalizziamo questa osservazione con la seguente definizione.

Definizione 2.1.8 Due insiemi A e B si dicono *equipotenti* se esiste una corrispondenza biunivoca $\varphi : A \leftrightarrow B$. Scriveremo, in tal caso, $|A| = |B|$ indicando con il simbolo $|X|$ la *potenza* o *cardinalità* dell'insieme X.

L'affermazione fatta all'inizio del paragrafo a proposito dei numeri naturali può allora essere espressa in modo più preciso.

Esempio 2.1.14 L'insieme dei numeri naturali $\mathbb{N}$ è equipotente ad un suo sottoinsieme proprio, l'insieme $B = \{0, 1, 4, 9, \ldots\}$ dei quadrati. Infatti

possiamo stabilire la seguente corrispondenza biunivoca:

$$\begin{array}{ccccc} \varphi & : & \mathbb{N} & \leftrightarrow & B \\ & & n & \leftrightarrow & n^2 \end{array}$$

A partire da quanto osservato finora possiamo chiarire i concetti di infinito e finito.

Definizione 2.1.9 Un insieme si dice *infinito* se può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio; un insieme si dice *finito* se non è infinito, ovvero se non può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio.

Definizione 2.1.10 Dato un insieme finito A si dice che A *possiede n elementi* se esiste una corrispondenza biunivoca tra A e il seguente sottoinsieme dell'insieme dei naturali: $I_{n-1} = \{0, 1, \ldots, n-1\}$, detto *intervallo di lunghezza n*, in tal caso si scrive $|A| = n$.

Definizione 2.1.11 Un insieme infinito B si dice *numerabile* se può essere messo in corrispondenza biunivoca con l'insieme $\mathbb{N}$ dei numeri naturali; la potenza del numerabile si indica con la prima lettera dell'alfabeto ebraico, aleph, con pedice zero, ovvero si scrive $|B| = |\mathbb{N}| = \aleph_0$.

Esempio 2.1.15 Gli insiemi $A = \{2n : n \in \mathbb{N}\}$, $B = \{2n+1 : n \in \mathbb{N}\}$ e $C = \mathbb{Z}$, rispettivamente dei numeri naturali pari, dei numeri naturali dispari e degli interi relativi, sono numerabili. Infatti possiamo costruire le seguenti applicazioni biunivoche:

$$\begin{array}{ccccc} \alpha & : & A & \leftrightarrow & \mathbb{N} \\ & & 2n & \leftrightarrow & n \end{array} \quad , \quad \begin{array}{ccccc} \beta & : & B & \leftrightarrow & \mathbb{N} \\ & & 2n+1 & \leftrightarrow & n \end{array}$$

$$\begin{array}{ccccc} \gamma & : & \mathbb{N} & \leftrightarrow & \mathbb{Z} \\ & & 2n & \leftrightarrow & n \\ & & 2n+1 & \leftrightarrow & -(n+1) \end{array}$$

La verifica della biunivocità delle tre funzioni viene lasciata allo studente.

Proposizione 2.1.1 *Un sottoinsieme S di un insieme numerabile A è finito o numerabile.*

Dimostrazione - Osserviamo innanzitutto che dire che l'insieme A è numerabile significa dire che i suoi elementi possono essere considerati come elementi di una successione; infatti, se φ è una biiezione fra $\mathbb{N}$ e A, possiamo scrivere $\varphi(n) = a_n$ onde $A = \{\varphi(0), \varphi(1), \ldots\} = \{a_0, a_1, \ldots\}$. A questo

punto un sottoinsieme proprio S di A, se non è finito, sarà una sottosuccessione della successione $a_0, a_1, \ldots$ e quindi S risulta essere numerabile. ∎

Sappiamo bene che, nell'insieme dei numeri naturali, è definita una relazione di ordine per cui, dati comunque due naturali n, m tali che $n \neq m$, risulta sempre $n < m$ oppure $m < n$; pertanto considerati comunque due insiemi finiti A e B, $|A| = n$ e $|B| = m$, sussiste una delle seguenti tre possibilità: $|A| < |B|$, $|A| = |B|$ e $|A| > |B|$. Possiamo estendere questa relazione anche alle cardinalità infinite tramite la seguente definizione.

Definizione 2.1.12 Dati due insiemi A e B diremo che A *ha cardinalità maggiore di* B se esiste una corrispondenza biunivoca fra B ed un sottoinsieme proprio di A, ma non esiste alcuna corrispondenza biunivoca fra B e A.

Osservazione 2.1.4 Se A è un insieme finito risulta sempre $|A| < \aleph_0$.

Osserviamo ora cosa succede quando, a partire da un insieme finito, si costruisce il suo insieme delle parti.

Esempio 2.1.16 Se $A = \{a, b, c\}$ allora risulta $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$; dunque, se $|A| = 3$ allora $|\mathcal{P}(A)| = 2^3$. Lo studente può verificare su un esempio che, se $|A| = 4$, allora $|\mathcal{P}(A)| = 2^4$. In effetti si può dimostrare, in generale, la seguente proposizione.

Proposizione 2.1.2 *Se* $|A| = n$ *allora* $|\mathcal{P}(A)| = 2^n$.

Vedremo alla fine del paragrafo come, tramite l'insieme delle parti, sia possibile costruire insiemi infiniti di cardinalità crescente; enunciamo ora, senza dimostrarlo, un teorema che ci assicura che due cardinalità sono sempre confrontabili.

Teorema 2.1.1 (Teorema di Cantor-Bernstein) *Dati comunque due insiemi A e B si presenta per essi una, ed una sola, delle seguenti possibilità:*

$$|A| < |B|, \qquad |A| = |B|, \qquad |A| > |B|.$$

Dimostriamo ora due importanti teoremi relativi alla cardinalità del numerabile.

Teorema 2.1.2 (Primo teorema di Cantor) *L'unione di una quantità finita o numerabile di insiemi finiti o numerabili è un insieme di potenza al più numerabile; in particolare:*

$$\mathcal{F} = \{I_i : |I_i| = \aleph_0, \quad i \in \mathbb{N}\} \quad \Longrightarrow \quad |\cup_{i \in \mathbb{N}} I_i| = \aleph_0.$$