Rita Procesi Ciampi

LEZIONI DI ALGEBRA

un primo modulo

ACCADEMICA

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

Copyright © 2003 by Accademica S.r.l., Roma
Quest'opera è soggetta a copyright. I diritti di traduzione, di memorizzazione elettronica, di riproduzione e di adattamento totale o parziale con qualsiasi mezzo (compresi i microfilm e le copie fotostatiche) sono riservati per tutti i paesi.

sito web: www.accademica.it

e-ISBN 978-88-85929-68-5

Procesi Ciampi, Rita: Lezioni di Algebra - un primo modulo

a Marta

Prefazione

Con la riforma universitaria è stato necessario rivedere l'organizzazione dei corsi e la natura stessa di ciascun corso ha subito profonde modifiche; molti dei libri che si utilizzavano si sono quindi rivelati non del tutto rispondenti alle nuove esigenze.

Lo scopo di questo testo è quello di fornire allo studente che affronta un primo corso di Algebra uno strumento che sia contemporaneamente accurato e semplice. Di conseguenza alcuni argomenti non sono stati trattati in maniera completa e di alcuni teoremi manca la dimostrazione; d'altra parte si fa a volte riferimento ad alcune nozioni di Algebra Lineare e Calcolo supponendo che il corso di Algebra segua i corsi relativi.

Sono molto grata ai colleghi Valentina Barucci, Giulio Campanella, Anna Franchetta e Rosaria Rota per i suggerimenti e le correzioni; ringrazio anche Daniele Gewurz per i disegni.

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
$\setminus$	differenza fra insiemi	$\in$	appartenente
$\notin$	non appartenente	$\ni$	contenente
$\subseteq$	sottoinsieme	$\subset$	sottoinsieme proprio
$\mathcal{C}_A(B)$	complementare di B in A	$C \times D$	prodotto cartesiano di C e D
$\geq$	maggiore o eguale	$\leq$	minore o eguale
$\neq$	diverso	$\aleph$	aleph
$\mathbb{N}$	numeri naturali	$\mathbb{Z}$	numeri interi relativi
$\mathbb{Q}$	numeri razionali	$\mathbb{R}$	numeri reali
$\mathbb{C}$	numeri complessi	A^*	$A\setminus\{0\}$ (A=$\mathbb{N}$,$\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$,$\mathbb{C}$)
A^+	positivi in A (A=$\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$)	A^-	negativi in A (A=$\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$)
n!	n fattoriale	$\binom{n}{k}$	coefficiente binomiale
$a \mid b$	a divide b	$m\mathbb{Z}$	multipli interi di m
$a \equiv b \bmod m$	a congruo a b modulo m	$\mathbb{Z}_m$	classi resto modulo m
$A[x]$	anello dei polinomi a coefficienti in A	$\mathbb{Z}[i]$	interi di Gauss
$N < G$	N sottogruppo di G	$N \lhd G$	N sottogruppo normale di G
A/ρ	insieme quoziente	G/N	gruppo quoziente

Indice

1 TEORIA DEGLI INSIEMI **1**
1.1 OPERAZIONI FRA INSIEMI 1
1.2 APPLICAZIONI FRA INSIEMI 8
1.3 RELAZIONI DI EQUIVALENZA 17
1.4 RELAZIONI D'ORDINE 22

2 CARDINALITÀ **27**
2.1 FINITO, NUMERABILE E CONTINUO 27

3 INSIEMI NUMERICI **37**
3.1 I NATURALI E L'INDUZIONE 37
3.2 INTERI RELATIVI E DIVISIBILITA' 40
3.3 CONGRUENZE 50
3.4 CLASSI RESTO 61
3.5 I NUMERI RAZIONALI 70
3.6 I NUMERI COMPLESSI 72
3.7 I QUATERNIONI 76
3.8 NUMERAZIONE IN BASI DIVERSE 78

4 L'ANELLO DEI POLINOMI **83**
4.1 ANELLI 83
4.2 POLINOMI 87
4.3 CONGRUENZE FRA POLINOMI 100
4.4 RADICI DELL'UNITÀ 108

5 GRUPPI **115**
5.1 GRUPPI - PRIME PROPRIETÀ 115
5.2 GRUPPI CICLICI 131
5.3 GRUPPI DI PERMUTAZIONI 133
5.4 GRUPPI DIEDRALI 145
5.5 OMOMORFISMI FRA GRUPPI 149

CAPITOLO 1

TEORIA DEGLI INSIEMI

1.1 OPERAZIONI FRA INSIEMI

Ricordiamo innanzitutto alcuni simboli di uso comune, che sono anche presentati nella lista dei simboli.

Nel definire un insieme o una proprietà utilizzeremo i due punti ":" o la barra "/" al posto dell'espressione "tale che"; nello stesso ambito la virgola e il punto e virgola conservano il loro significato usuale.

Come è già noto nel caso dei simboli "$=$" e "$\neq$", barrare un simbolo equivale a negarne il significato; ne vedremo immediatamente degli esempi.

Sottolineiamo poi l'importanza dei "quantificatori", ovvero $\forall$, $\exists$ e $\exists!$; il primo si legge "per ogni", il secondo "esiste almeno uno", il terzo "esiste esattamente uno".

Gli insiemi numerici classici, alcuni dei quali verranno poi studiati in maggior dettaglio, li indicheremo al modo seguente:

$\mathbb{N}$ l'insieme dei numeri naturali
$\mathbb{Z}$ l'insieme dei numeri interi relativi
$\mathbb{Q}$ l'insieme dei numeri razionali
$\mathbb{R}$ l'insieme dei numeri reali
$\mathbb{C}$ l'insieme dei numeri complessi

Se A indica uno di questi insiemi, o un qualunque insieme che contenga lo zero, il simbolo A^* indicherà l'insieme stesso privato dello zero.

Chiariamo infine l'uso dei simboli $\Rightarrow$ e $\Leftrightarrow$, ovvero dei simboli di implicazione.

Se F_1 e F_2 sono due formule, due affermazioni, due proposizioni, etc... la scrittura $F_1 \Rightarrow F_2$ si legge "F_1 implica F_2" e significa che, se vale la F_1 allora vale anche la F_2.

Analogamente la scrittura $F_1 \Leftrightarrow F_2$ equivale a dire che "F_1 vale se, e solo se, vale F_2".

Chiariamo con un esempio, siano F_1 l'affermazione "n è un intero relativo multiplo di sei" e F_2 l'affermazione "n è un intero relativo multiplo di due"; allora risulta:

$$F_1 \Rightarrow F_2 \quad \text{e} \quad F_1 \not\Leftarrow F_2 \, .$$

In quasto corso non possiamo trattare rigorosamente la teoria degli insiemi; intuitivamente diremo che un *insieme* è una collezione di oggetti o elementi, denoteremo gli insiemi con lettere maiuscole.

Se A è un insieme, per indicare che un elemento x appartiene all'insieme A scriveremo $x \in A$; analogamente scriveremo $y \notin A$ se l'elemento y non appartiene all'insieme A.

Per descrivere un insieme se ne possono elencare gli elementi, e in tal caso si scriverà per esempio $A = \{1, 3, 5, 7\}$; se gli elementi dell'insieme sono tutti e soli quelli soddisfacenti ad una proprietà P l'insieme potrà essere descritto al modo seguente $A = \{\ x : P(x) \text{ è vera }\}$ e potremo allora scrivere:

$$A = \{1, 3, 5, 7\} = \{\ x \in \mathbb{N} : x \text{ è dispari, } 1 \leq x \leq 7\}.$$

Definizione 1.1.1 Un insieme S si dice *sottoinsieme* di un insieme A, e si scrive $S \subseteq A$, se ogni elemento di S è anche elemento di A; in tal caso diremo anche che S è *contenuto* in A.

Diremo poi che due insiemi A e B sono *uguali*, e scriveremo $A = B$, se $A \subseteq B$ e $B \subseteq A$, ovvero se ogni elemento di A è anche elemento di B ed ogni elemento di B appartiene anche ad A.

La definizione precedente può essere scritta in modo sintetico come segue:

$$S \subseteq A \iff \forall\, s \in S \Longrightarrow s \in A$$

e

$$A = B \iff [\forall\, a \in A \Longrightarrow a \in B \text{ e } \forall\, b \in B \Longrightarrow b \in A\ ].$$

Definizione 1.1.2 Diciamo che un insieme S è un *sottoinsieme proprio* di A, ovvero che S è *contenuto propriamente* in A, e si scrive $S \subset A$, se ogni elemento di S è anche elemento di A ed esiste almeno un elemento di A che non appartiene ad S, ovvero $S \subseteq A$ e $S \neq A$.

Esempio 1.1.1 Siano $A = \{3, -2\}$ e $B = \{b \in \mathbb{Z} \,/\, b^3 - b^2 - 6b = 0\}$; A è un sottoinsieme di B poiché 3 e -2 sono radici dell'equazione $x^3 - x^2 - 6x = 0$ e quindi $3, -2 \in B$. Inoltre A è un sottoinsieme proprio di B poiché $0 \in B$, ma $0 \notin A$.

Esempio 1.1.2 Siano $A = \{x/x \in \mathbb{N},\ x \text{ è un numero primo, } 2 \leq x \leq 8\}$ e $B = \{2, 3, 5, 7\}$; si verifica, utilizzando la doppia inclusione $A \subseteq B$ e $B \subseteq A$, che $A = B$.

La definizione che segue è forse poco intuitiva, ma ne vedremo l'utilità nel seguito.

Definizione 1.1.3 Si dice *insieme vuoto* e si denota con il simbolo $\emptyset$ l'insieme privo di elementi; si assume che $\emptyset \subseteq A$ per ogni insieme A.

Esempio 1.1.3 Sia $A = \{x \,/\, x \in \mathbb{N},\ 3x = 8\}$; poiché ovviamente non esiste alcun numero naturale x tale che $3x = 8$, risulta $A = \emptyset$.

Osserviamo che non si deve confondere l'elemento x di un insieme A con il sottoinsieme $\{x\}$ di A costituito dal solo elemento x.

Definizione 1.1.4 Definiamo *insieme delle parti* di un insieme A l'insieme i cui elementi sono tutti i sottoinsiemi di A, ovvero $\mathcal{P}(A) = \{X : X \subseteq A\}$.

Esempio 1.1.4 Se $A = \{a, b, c\}$, allora risulta $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}$.

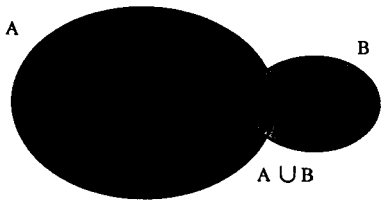
L'esempio precedente mostra che, nel caso di un insieme con tre elementi, il suo insieme delle parti ha otto elementi; ciò non è casuale poiché sussiste la seguente proposizione, la cui dimostrazione verrà data nel paragrafo seguente.

Proposizione 1.1.1 *Se A è un insieme con n elementi, $\mathcal{P}(A)$ ha 2^n elementi.*

Dopo queste prime definizioni cominciamo con lo studio delle operazioni fra gli insiemi.

Definizione 1.1.5 Se A e B sono due insiemi, si definisce *unione* dei due insiemi A e B, e si denota $A \cup B$, l'insieme degli elementi che appartengono ad A o a B, ovvero:

$$A \cup B \;=\; \{x \,/\, x \in A \text{ o } x \in B\}\,.$$



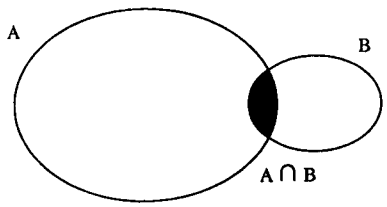
Osserviamo che la 'o' che compare nella definizione di unione è la traduzione del 'vel' latino e non di 'aut', poiché non si esclude il caso che l'elemento x possa appartenere sia ad A che a B; nel caso in cui l'elemento x appartenga ad entrambi gli insiemi, in $A \cup B$ lo considereremo come elemento una volta sola.

Esempio 1.1.5 Siano $A = \{1, 2\}$ e $B = \{x/x \in \mathbb{N},\ 0 \leq x \leq 1\}$; risulta allora: $A \cup B = \{0, 1, 2\}$.

Esempio 1.1.6 Siano $A = \{1, 2, 5, 7, 9\}$ e $B = \{2, 4, 6, 7, 8, \}$; allora risulta che $A \cup B = \{1, 2, 5, 7, 9, 4, 6, 8\}$.

Definizione 1.1.6 Si definisce *intersezione* di due insiemi A e B, e si denota $A \cap B$, l'insieme degli elementi che appartengono ad A e a B, ovvero:

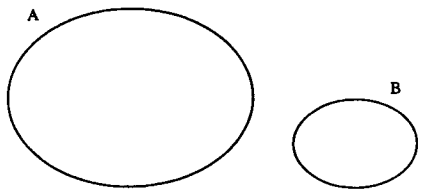
$$A \cap B = \{x \ / \ x \in A \text{ e } x \in B\}.$$



Esempio 1.1.7 Se A e B sono gli insiemi descritti nell'esempio 1.1.6, risulta $A \cap B = \{2, 7\}$.

Esempio 1.1.8 Siano $A = \{-4, -1, 3\}$ e $B = \{x \ / \ x^4 - 2x^3 - 3x^2 = 0\}$; poiché -1 e 3 sono radici dell'equazione $x^4 - 2x^3 - 3x^2 = 0$ mentre $-4 \notin B$, risulta $A \cap B = \{-1, 3\}$.

Definizione 1.1.7 Due insiemi A e B si dicono *disgiunti* se $A \cap B = \emptyset$.



Esempio 1.1.9 Siano $A = \mathbb{R}$ e $B = \{x \ / \ x^2 + 1 = 0\}$; poiché non esiste alcun numero reale x tale che $x^2 + 1 = 0$, si ha che $A \cap B = \emptyset$ ovvero A e B sono disgiunti.

Per quanto riguarda le proprietà soddisfatte dalle operazioni di unione e di intersezione di insiemi, vale la seguente proposizione:

Proposizione 1.1.2 *Se A, B e C sono tre insiemi, si ha:*

1) $A \cup A = A$, $A \cap A = A$ *idempotenza*

2) $A \cup B = B \cup A$, $A \cap B = B \cap A$ *proprietà commutativa*

3) $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$ *proprietà associativa*

4) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *proprietà distributive*

5) $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$.

Dimostrazione - Verifichiamo una delle precedenti proprietà, ad esempio la seconda delle 4), lasciando allo studente la dimostrazione delle altre.

Per verificare che $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ occorre dimostrare, per la definizione di uguaglianza di due insiemi, che valgono le due inclusioni:

i) $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

ii) $A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$.

Allo scopo di dimostrare la i), occorre dimostrare che ogni elemento dell'insieme a primo membro è anche elemento dell'insieme a secondo membro; sia quindi x un elemento generico dell'insieme $A \cap (B \cup C)$.

Per definizione di intersezione, l'elemento x appartiene sia ad A che a $B \cup C$, ovvero sia ad A che a B o a C. Pertanto l'elemento x appartiene ad $A \cap B$ o ad $A \cap C$ e quindi all'unione dei due insiemi $A \cap B$ e $A \cap C$; la dimostrazione appena fatta può essere scritta in maniera sintetica come segue:

$x \in A \cap (B \cup C) \Rightarrow (x \in A)$ e $(x \in B \cup C) \Rightarrow (x \in A)$ e $(x \in B$ o $x \in C)$

$\Rightarrow (x \in A$ e $x \in B)$ o $(x \in A$ e $x \in C) \Rightarrow x \in A \cap B$ o $x \in A \cap C$

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

Per quanto riguarda la verifica della ii), in modo analogo risulta:

$x \in (A \cap B) \cup (A \cap C) \Rightarrow x \in A \cap B$ o $x \in A \cap C \Rightarrow (x \in A$ e $x \in B)$ o

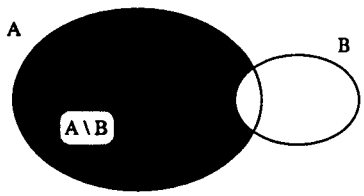
$(x \in A$ e $x \in C) \Rightarrow (x \in A)$ e $(x \in B$ o $x \in C) \Rightarrow (x \in A)$ e $(x \in B \cup C)$

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

Come si può osservare, la dimostrazione della ii) si effettua invertendo le frecce nella dimostrazione della i). ■

Definizione 1.1.8 Dati due insiemi A e B si definisce *differenza* dei due insiemi A e B, e si denota $A \backslash B$, l'insieme degli elementi che appartengono ad A, ma non appartengono a B, ovvero:

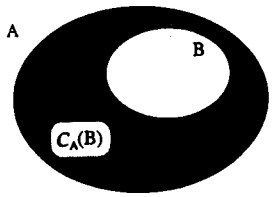
$$A \backslash B = \{ x \ / \ x \in A, \ x \notin B \} .$$



Esempio 1.1.10 Se A e B sono gli insiemi descritti nell'esercizio 1.1.6, risulta $A \backslash B = \{1, 5, 9\}$.

Esempio 1.1.11 Siano $A = \{x \ / \ x \in \mathbb{N}, 0 \leq x \leq 8\}$ e $B = \{x \ / \ x^3 - 8x^2 + 17x - 10 = 0\}$; poiché gli elementi 1,2 e 5 di A sono radici dell'equazione che definisce B, si ha che $A \backslash B = \{0, 3, 4, 6, 7, 8\}$.

Definizione 1.1.9 Se l'insieme B è un sottoinsieme dell'insieme A, l'insieme differenza $A \backslash B$ si dice *complementare* di B in A e si denota $\mathcal{C}_A(B)$.



Esempio 1.1.12 Siano $A = \{x \ / \ x \in \mathbb{N},\ x \text{ primo},\ x \leq 17\}$ e $B = \{7, 11, 13\}$; risulta allora $B \subseteq A$ ed inoltre $\mathcal{C}_A(B) = \{2, 3, 5, 17\}$.

Relativamente all'operazione appena definita, sussistono le seguenti due proprietà, dette formule di de Morgan:

Proposizione 1.1.3 *Se B e C sono due sottoinsiemi di un insieme A risulta allora:*

1) $\mathcal{C}_A(B \cup C) = \mathcal{C}_A(B) \cap \mathcal{C}_A(C)$

2) $\mathcal{C}_A(B \cap C) = \mathcal{C}_A(B) \cup \mathcal{C}_A(C)$.

Dimostrazione - Dimostriamo la 1), lasciando allo studente la dimostrazione, del tutto analoga, della 2); a tal fine verifichiamo che:

i) $\mathcal{C}_A(B \cup C) \subseteq \mathcal{C}_A(B) \cap \mathcal{C}_A(C)$

ii) $\mathcal{C}_A(B) \cap \mathcal{C}_A(C) \subseteq \mathcal{C}_A(B \cup C)$.

Cominciamo con il dimostrare la i); sia $x \in \mathcal{C}_A(B \cup C)$ ovvero $x \notin B \cup C$.

Poiché $x \notin B \cup C$, x non può appartenere né a B né a C, ovvero x appartiene sia al complementare di B che al complementare di C, da ciò segue che x appartiene a $\mathcal{C}_A(B) \cap \mathcal{C}_A(C)$.

Per quanto riguarda la ii), sia $x \in \mathcal{C}_A(B) \cap \mathcal{C}_A(C)$ ovvero $x \in \mathcal{C}_A(B)$ e $x \in \mathcal{C}_A(C)$; allora $x \notin B$ e $x \notin C$, onde x non può appartenere a $B \cup C$ e quindi $x \in \mathcal{C}_A(B \cup C)$.

Abbiamo così dimostrato che vale la doppia inclusione e quindi l'uguaglianza dei due insiemi espressa nella formula 1). Affinché lo studente familiarizzi con il linguaggio simbolico, riscriviamo la dimostrazione appena fatta utilizzando soltanto simboli matematici:

$$x \in \mathcal{C}_A(B \cup C) \Leftrightarrow x \in A,\ x \notin B \cup C \Leftrightarrow x \in A\ ,\ x \notin B \text{ e } x \notin C \Leftrightarrow$$

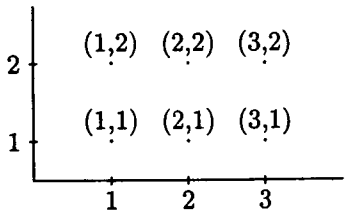
$$\Leftrightarrow x \in \mathcal{C}_A(B) \text{ e } x \in \mathcal{C}_A(C) \Leftrightarrow x \in \mathcal{C}_A(B) \cap \mathcal{C}_A(C). \blacksquare$$

Definizione 1.1.10 Dati due insiemi A e B, si definisce *prodotto cartesiano* dei due insiemi A e B, e si denota $A \times B$, l'insieme delle coppie ordinate in cui il primo elemento è in A ed il secondo in B, ovvero:

$$A \times B \ = \ \{\ (x, y)\ /\ x \in A,\ y \in B\ \}\ .$$

Descriviamo il prodotto cartesiano $A \times B$ dove $A = \{1,2,3\}$ e $B = \{1,2\}$; tale insieme risulta essere costituito da tutte le coppie il cui primo elemento è in A e il secondo in B.

Se descriviamo tale insieme nel piano, seguendo lo stesso metodo che si usa per scrivere le coordinate cartesiane di un punto, otteniamo il seguente grafico:

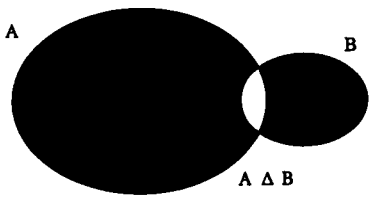


Esempio 1.1.13 Osserviamo che il prodotto cartesiano non è commutativo; infatti, se $A = \{a,b\}$ e $B = \{1,2,3\}$, si ha $A \times B = \{(a,1),(a,2),(a,3),(b,1),(b,2),(b,3)\}$, mentre $B \times A = \{(1,a),(2,a),(3,a),(1,b),(2,b),(3,b)\}$.

Vogliamo sottolineare il fatto che due coppie (x,y) e (x',y') coincidono se, e solo se, $x = x'$ e $y = y'$.

Definizione 1.1.11 Dati due insiemi A e B, si definisce *differenza simmetrica* dei due insiemi A e B, e si denota $A\Delta B$, l'unione dei due insiemi $A\backslash B$ e $B\backslash A$, ovvero:

$$A\Delta B = (A\backslash B) \cup (B\backslash A) = \{x \ / \ (x \in A,\ x \notin B) \text{ o } (x \in B,\ x \notin A)\}.$$



Si verifica facilmente che:

Proposizione 1.1.4 *Dati due insiemi A e B risulta:*

$$A\Delta B = (A \cup B)\backslash(A \cap B).$$

Dimostrazione - Dimostriamo, con una serie di doppie implicazioni, l'uguaglianza dei due insiemi $A\Delta B$ e $(A \cup B)\backslash(A \cap B)$; si ha:

$$x \in A\Delta B \Longleftrightarrow x \in A\backslash B \text{ oppure } x \in B\backslash A \Longleftrightarrow$$

$$\Longleftrightarrow (x \in A,\ x \notin B) \text{ oppure } (x \in B, x \notin A)$$

Pertanto l'elemento x appartiene ad $A\Delta B$ se, e solo se, appartenendo ad A non appartiene anche a B e, appartenendo a B, non appartiene anche ad A.

Da ciò segue che l'elemento x, che appartiene o ad A o a B, non può appartenere ad entrambi gli insiemi, e quindi non appartiene all'intersezione; onde

$$x \in A\Delta B \Leftrightarrow x \in (A \cup B)\backslash(A \cap B),$$

da cui l'uguaglianza richiesta. ■

Esempio 1.1.14 Siano $A = \{a, b, c, d\}$ e $B = \{b, d, e, f, g\}$; risulta allora:

$$A\Delta B = (A\backslash B) \cup (B\backslash A) = \{a, c\} \cup \{e, f, g\} = \{a, c, e, f, g\} =$$
$$= \{a, b, c, d, e, f, g\}\backslash\{b, d\} = (A \cup B)\backslash(A \cap B).$$

1.2 APPLICAZIONI FRA INSIEMI

Definizione 1.2.1 Siano A e B due insiemi; si dice *applicazione* o *funzione* di A in B una legge che associa ad ogni elemento di A un ben determinato elemento di B; per denotare un'applicazione f di A in B si usa il simbolismo $f : A \to B$. Gli insiemi A e B si dicono rispettivamente *dominio* e *codominio* di f. Inoltre due applicazioni $f : A \to B$ e $g : C \to D$ sono *uguali* se $A = C$, $B = D$ e $f(x) = g(x)\ \forall\ x \in$A.

Definizione 1.2.2 Se $A = B$ si può definire una particolare applicazione i_A di A in A ponendo, $\forall\ x \in A$, $i_A(x) = x$; tale applicazione viene detta *applicazione identica* ~~di~~ A o *identità* di A.

Esempio 1.2.1 Un esempio di applicazione di dominio $\mathbb{Z}$ e codominio $\mathbb{N}$ si ottiene associando ad ogni intero x il suo quadrato; in tal caso, per denotare tale applicazione, si scriverà $f : \mathbb{Z} \to \mathbb{N}$ tale che, $\forall\ x \in \mathbb{Z}$, $f(x) = x^2$, ovvero:

$$\begin{array}{rcl} f : \mathbb{Z} & \to & \mathbb{N} \\ x & \to & x^2 \ . \end{array}$$

Esempio 1.2.2 Per denotare l'applicazione f di dominio $\mathbb{Z}$ e codominio $\mathbb{R}$ che associa all'intero n la sua radice cubica si scrive:

$$\begin{array}{rcl} f : \mathbb{Z} & \to & \mathbb{R} \\ n & \to & \sqrt[3]{n} \ . \end{array}$$

Definizione 1.2.3 Data l'applicazione $f : A \to B$, l'elemento $f(x) \in B$, $x \in A$, prende il nome di *immagine* di x tramite f. Se $y \in B$, si dice *controimmagine* di y tramite f, e si denota $f^{-1}(y)$, l'insieme degli elementi x di A tali che $f(x) = y$, ovvero:

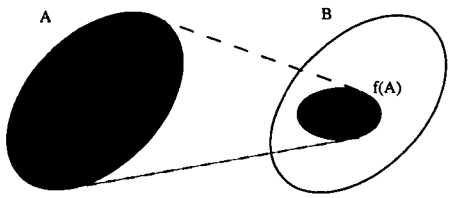
$$f^{-1}(y) = \{x \in A \ / \ f(x) = y\} \ .$$

Osservazione 1.2.1 Osserviamo che la controimmagine di un elemento può anche essere l'insieme vuoto; infatti, se si considera l'applicazione f descritta nell'esempio 1.2.1, risulta $f^{-1}(9) = \{-3, +3\}$, mentre $f^{-1}(7) = \emptyset$, poiché non esistono interi relativi il cui quadrato è 7.

Definizione 1.2.4 Siano A e B due insiemi ed f un'applicazione di A in B; se S è un sottoinsieme di A, si dice *immagine di S tramite f*, e si denota $f(S)$, l'insieme degli elementi di B che sono immagini, tramite f, di elementi di S, ovvero:

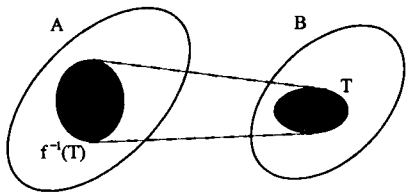
$$f(S) = \{y \in B \ / \ \exists \ x \in S : f(x) = y\} \ .$$

Se $S = A$, $f(A)$ si dice *immagine di f* e si denota $\mathrm{Im}f$.



Definizione 1.2.5 Se T è un sottoinsieme di B, si dice *controimmagine di T tramite f*, e si denota $f^{-1}(T)$, l'insieme degli elementi di A la cui immagine appartiene a T, ovvero:

$$f^{-1}(T) = \{x \in A \ / \ f(x) \in T\} \ .$$



Esempio 1.2.3 Sia $f : \mathbb{N} \to \mathbb{N}$ l'applicazione definita ponendo $f(x) = 2x$, per ogni $x \in \mathbb{N}$; allora, se $S = \{2, 3, 5, 7\}$, risulta $f(S) = \{4, 6, 10, 14\}$. Inoltre, come subito si vede, $\mathrm{Im}f$ è l'insieme dei numeri naturali pari. Considerati poi $R = \{11, 17, 25\}$ e $T = \{1, 13, 6, 7\}$, risulta $f^{-1}(S) = \{1\}$, $f^{-1}(R) = \emptyset$ e $f^{-1}(T) = \{3\}$.

Esempio 1.2.4 Sia f l'applicazione di $\mathbb{R}^3$ in $\mathbb{R}^2$ definita al modo seguente, $\forall \ (a, b, c) \in \mathbb{R}^3$, $f((a, b, c)) = (a + b, c)$; determiniamo $f^{-1}(T)$, essendo $T = \{(0, y) \ / \ y \in \mathbb{R}\}$. Poiché $f^{-1}(T)$ è l'insieme degli elementi di $\mathbb{R}^3$ che vengono trasformati da f in elementi di T, si ha che:

$$(a, b, c) \in f^{-1}(T) \Leftrightarrow f((a, b, c)) = (a + b, c) \in T \Leftrightarrow a + b = 0 \Leftrightarrow b = -a.$$

Pertanto risulta $f^{-1}(T) = \{(a, -a, c)/a, c \in \mathbb{R}\}$.

Esempio 1.2.5 Sia f l'applicazione di $\mathbb{R}^2$ in $\mathbb{R}^2$ così definita, $\forall (a,b) \in \mathbb{R}^2$, $f((a,b)) = (a+b,0)$ e siano $S = \{(-1,2),(\frac{3}{2},-4),(\sqrt{3},0)\}$ e $T = \{(\pi,0)\}$; risulta allora $f(S) = \{(1,0),(-\frac{5}{2},0),(\sqrt{3},0)\}$ e $f^{-1}(T) = \{(\pi - x, x), x \in \mathbb{R}\}$.

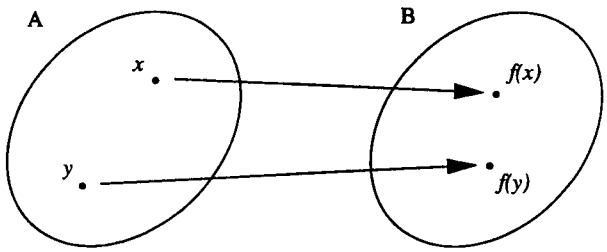
Per f ovviamente risulta $\mathrm{Im} f = \{(x,0), x \in \mathbb{R}\}$.

Definizione 1.2.6 Sia f un'applicazione di A in B; si dice che f è *iniettiva* se, $\forall\, x,y \in A$, $x \neq y$, risulta $f(x) \neq f(y)$.

La definizione appena data è equivalente alla seguente:

$$\forall\, x,y \in A,\ f(x) = f(y) \Rightarrow x = y$$

che più spesso è utilizzata per verificare che una applicazione data è iniettiva.



Esempio 1.2.6 L'applicazione di cui all'esempio 1.2.1 non è iniettiva, poiché $f(3) = f(-3) = 9$, mentre l'applicazione $g : \mathbb{Z} \to \mathbb{Z}$ tale che, $\forall\, x \in \mathbb{Z}$, $g(x) = x+4$, è evidentemente iniettiva.

Esempio 1.2.7 L'applicazione $f : \mathbb{R} \to \mathbb{R}$ tale che, $\forall\, x \in \mathbb{R}$, $f(x) = x^2 + \pi$ non è iniettiva poiché essa assume lo stesso valore per ogni coppia di valori opposti, ad esempio $f(2) = 4 + \pi = f(-2)$.

Esempio 1.2.8 L'applicazione g di dominio l'insieme $A = \{a,b,c\}$ e codominio l'insieme $B = \{1,2,3,4\}$, tale che $g(a) = 3$, $g(b) = 1$ e $g(c) = 4$ è ovviamente iniettiva poiché elementi distinti in A hanno immagini distinte in B.

Osserviamo che, nel caso in cui un'applicazione è iniettiva, la controimmagine di ogni elemento del codominio, se non è vuota, è costituita da un unico elemento.

Definizione 1.2.7 L'applicazione $f : A \to B$ si dice *suriettiva* se, $\forall\, y \in B$, esiste $x \in A$ tale che $f(x) = y$; per come è definita l'immagine di un'applicazione, f risulta essere suriettiva se, e solo se, $Imf = B$.

Esempio 1.2.9 L'applicazione $f : \mathbb{Z} \to \mathbb{Z}$, definita ponendo, $\forall\, x \in \mathbb{Z}$, $f(x) = x^2$, non è suriettiva, poiché, per esempio, l'elemento 5, non essendo il quadrato di un intero, non è immagine di alcun elemento di $\mathbb{Z}$. L'applicazione $g : \mathbb{Z} \to \mathbb{Z}$ tale che $g(x) = x + 4$ è invece suriettiva poiché l'elemento generico y di $\mathbb{Z}$ è immagine tramite g dell'elemento $y - 4$; infatti $g(y-4) = (y-4) + 4 = y$.

Definizione 1.2.8 Un'applicazione $f : A \to B$ si dice *biiettiva* o *biunivoca* se essa è sia iniettiva che suriettiva. Per le applicazioni biunivoche si usa spesso il termine *corrispondenza biunivoca.*

Esempio 1.2.10 L'applicazione $f : \mathbb{R} \to \mathbb{R}$, definita ponendo, $\forall\ x \in\mathbb{R}$, $f(x) = \sqrt[3]{x+1} - 7$, è biiettiva.

Osserviamo innanzitutto che la radice cubica reale di un numero reale esiste sempre ed è unica; pertanto l'applicazione f è definita su tutto $\mathbb{R}$.

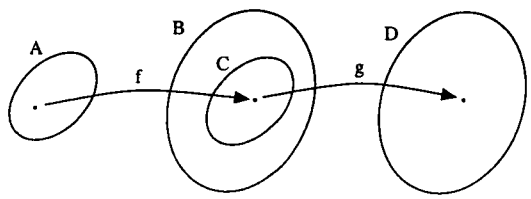
Verifichiamo ora che tale applicazione è iniettiva; a tal fine siano $x, y \in\mathbb{R}$ tali che $f(x) = f(y)$, ovvero $\sqrt[3]{x+1} - 7 = \sqrt[3]{y+1} - 7$ e quindi $\sqrt[3]{x+1} = \sqrt[3]{y+1}$. Elevando al cubo entrambi i membri dell'ultima uguaglianza, si ottiene $x + 1 = y + 1$ e quindi $x = y$; pertanto $f(x) = f(y)$ implica $x = y$ e quindi l'applicazione considerata è iniettiva.

Per quanto riguarda la suriettività sia $y \in\mathbb{R}$; ci chiediamo se esiste $x \in\mathbb{R}$ tale che $f(x) = y$, ovvero $\sqrt[3]{x+1} - 7 = y$. Dall'ultima uguaglianza segue $\sqrt[3]{x+1} = y + 7$, onde $x = (y+7)^3 - 1$; pertanto f è suriettiva, poiché, $\forall y \in\mathbb{R}$, $\exists\ [(y+7)^3 - 1] \in\mathbb{R}\ /\ f((y+7)^3 - 1) = y$.

Definizione 1.2.9 Se $f : A \to B$ è biiettiva, si può definire un'applicazione, che denoteremo f^{-1}, di B in A ponendo, $\forall\ y \in B$, $f^{-1}(y) = x$, dove x è l'elemento di A tale che $f(x) = y$; osserviamo che l'elemento x esiste poiché f è suriettiva ed è unico, e quindi f^{-1} è un'applicazione, poiché f è iniettiva. L'applicazione f^{-1} appena definita si dice *applicazione inversa* di f.

Esempio 1.2.11 Negli esempi 1.2.6 e 1.2.9 abbiamo visto che l'applicazione $g : \mathbb{Z} \to\mathbb{Z}$ tale che $g(x) = x + 4$ è biiettiva; pertanto è possibile definire la funzione inversa $g^{-1} : \mathbb{Z} \to\mathbb{Z}$ e risulta $g^{-1}(y) = y - 4$, $\forall\ y \in\mathbb{Z}$.

Definizione 1.2.10 Siano $f : A \to B$ e $g : C \to D$, con $Imf \subseteq C$, due applicazioni; si definisce *prodotto operatorio* di f e g, e si denota $g \circ f$, l'applicazione di dominio A e codominio D che associa all'elemento x di A l'immagine tramite g dell'elemento $f(x)$, ovvero $(g \circ f)(x) = g(f(x))$.



Esempio 1.2.12 Siano $f : \mathbb{Z} \to \mathbb{R}$ e $g : \mathbb{R} \to \mathbb{R}$ tali che $f(x) = x^2 + 2$, $\forall\ x \in\mathbb{Z}$ e $g(x) = \sqrt[3]{x-1} + 6$, $\forall x \in\mathbb{R}$; il prodotto operatorio $g \circ f$ è un'applicazione di $\mathbb{Z}$ in $\mathbb{R}$ e sul generico elemento $x \in\mathbb{Z}$ agisce al modo seguente:

$$(g \circ f)(x) = g(f(x)) = g(x^2 + 2) = \sqrt[3]{(x^2+2) - 1} + 6 = \sqrt[3]{x^2+1} + 6.$$

Osserviamo che il prodotto operatorio $f \circ g$ non si può definire poiché f è definita su $\mathbb{Z}$ e non su $\mathbb{R}$.

Proposizione 1.2.1 *Il prodotto operatorio fra applicazioni gode della proprietà associativa.*

Dimostrazione - Se $f : A \to B$, $g : B \to C$ e $h : C \to D$ sono tre applicazioni, risulta:

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x). \blacksquare$$

Al fine di chiarire la nozione di prodotto operatorio, consideriamo alcuni esempi.

Esempio 1.2.13 Se f e g sono le applicazioni di $\mathbb{Z}$ in $\mathbb{Z}$ dell'esempio 1.2.9, è possibile definire sia $g \circ f$ che $f \circ g$ e risulta:

$$(g \circ f)(x) = g(f(x)) = g(x^2) = x^2 + 4,$$

$$(f \circ g)(x) = f(g(x)) = f(x + 4) = (x + 4)^2 .$$

Da questo esempio appare chiaro che il prodotto operatorio non gode della proprietà commutativa.

Proposizione 1.2.2 *Se $f : A \to B$ è biiettiva e $f^{-1} : B \to A$ è la sua inversa, risulta $f \circ f^{-1} = i_B$ e $f^{-1} \circ f = i_A$; inoltre, per ogni funzione h di dominio l'insieme A e codominio l'insieme B risulta: $h \circ i_A = h$ e $i_B \circ h = h$.*

Infine se $f : A \to B$ e $g : B \to A$ sono due applicazioni biiettive tali che $g \circ f = i_A$ e $f \circ g = i_B$, allora $f = g^{-1}$ e $g = f^{-1}$ e pertanto f e g sono inverse l'una dell'altra.

Dimostrazione - La prima parte della dimostrazione è conseguenza delle definizioni di prodotto operatorio, inversa e identità; per quanto riguarda la seconda parte risulta:

$$f = f \circ i_A = f \circ (g \circ g^{-1}) = (f \circ g) \circ g^{-1} = i_B \circ g^{-1} = g^{-1}.$$

In modo analogo si dimostra che $g = f^{-1}$. $\blacksquare$

Esempio 1.2.14 Verifichiamo se l'applicazione $g : \mathbb{R} \to \mathbb{R}$ tale che $g(x) = \dfrac{x^3 - 6x^2 + 12x - 1}{2}$, $\forall x \in \mathbb{R}$ è l'inversa dell'applicazione $f : \mathbb{R} \to \mathbb{R}$ definita ponendo, $\forall x \in \mathbb{R}$, $f(x) = \sqrt[3]{2x - 7} + 2$.

L'applicazione g è l'inversa di f se, e solo se, risulta $g \circ f = i_{\mathbb{R}}$ e $f \circ g = i_{\mathbb{R}}$; se verifichiamo risulta:

$$(g \circ f)(x) = g(f(x)) = g(\sqrt[3]{2x - 7} + 2) =$$

$$= \frac{(\sqrt[3]{2x-7}+2)^3 - 6(\sqrt[3]{2x-7}+2)^2 + 12(\sqrt[3]{2x-7}+2) - 1}{2} =$$

$$= \frac{2x - 7 + 6\sqrt[3]{(2x-7)^2} + 12\sqrt[3]{2x-7} + 8}{2} +$$

$$+ \frac{-6(\sqrt[3]{(2x-7)^2} + 4\sqrt[3]{2x-7} + 4) + 12\sqrt[3]{2x-7} + 24 - 1}{2} = x = i_{\mathbb{R}}(x)$$

e

$$(f \circ g)(x) = f(g(x)) = f\left(\frac{x^3 - 6x^2 + 12x - 1}{2}\right) =$$

$$= \sqrt[3]{x^3 - 6x^2 + 12x - 1 - 7} + 2 = \sqrt[3]{(x-2)^3} + 2 = x - 2 + 2 = x = i_{\mathbb{R}}(x)$$

onde f e g sono funzioni una inversa dell'altra.

Proposizione 1.2.3 *Se $f : A \to B$ e $g : B \to C$ sono due applicazioni iniettive (suriettive), allora il prodotto operatorio $g \circ f$ è un'applicazione iniettiva (suriettiva).*

Dimostrazione - Se $x, y \in A$ e $(g \circ f)(x) = (g \circ f)(y)$ allora $g(f(x)) = g(f(y))$ e, per l'iniettività di g, $f(x) = f(y)$ da cui, per l'iniettività di f, $x = y$, onde $g \circ f$ è iniettiva.

Per quanto riguarda la dimostrazione relativa alla suriettività, sia $z \in C$; essendo g suriettiva esiste $y \in B$ tale che $g(y) = z$ e, per la suriettività di f, esiste $x \in A$ tale che $f(x) = y$, onde $z = g(y) = g(f(x)) = (g \circ f)(x)$, da cui la suriettività di $g \circ f$. ■

Dalla proposizione precedente segue che se f e g sono entrambe biiettive, anche $g \circ f$ è biiettiva; in tal caso ha senso parlare dell'applicazione inversa di $g \circ f$ e risulta:

Proposizione 1.2.4 *Se $f : A \to B$ e $g : B \to C$ sono due applicazioni biiettive allora $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Dimostrazione - Si ha $(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ i_B \circ g^{-1} = g \circ g^{-1} = i_C$; in modo analogo si dimostra che $i_A = (f^{-1} \circ g^{-1}) \circ (g \circ f)$, onde, per la proposizione 1.2.2, $f^{-1} \circ g^{-1} = (g \circ f)^{-1}$. ■

Esempio 1.2.15 Per chiarire la proposizione precedente consideriamo le applicazioni $f : \mathbb{R} \to \mathbb{R}$ e $g : \mathbb{R} \to \mathbb{R}$ tali che $f(x) = x - \sqrt{2}$ e $g(x) = \sqrt[3]{x}$; pertanto si ha $(g \circ f)(x) = g(f(x)) = g(x - \sqrt{2}) = \sqrt[3]{x - \sqrt{2}}$ onde, per come è definita l'applicazione inversa, risulta $(g \circ f)^{-1}(x) = y$, dove y è il numero reale tale che $(g \circ f)(y) = \sqrt[3]{y - \sqrt{2}} = x$, e quindi $y - \sqrt{2} = x^3$ da cui $y = x^3 + \sqrt{2}$.

D'altra parte $f^{-1}(x) = x + \sqrt{2}$ e $g^{-1}(x) = x^3$ e pertanto:

$$(f^{-1} \circ g^{-1})(x) = f^{-1}(g^{-1}(x)) = f^{-1}(x^3) = x^3 + \sqrt{2}$$

abbiamo perciò verificato l'uguaglianza $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Per illustrare le proprietà precedentemente esposte, consideriamo il seguente esempio fondamentale, che sarà utilizzato anche in seguito.

Esempio 1.2.16 Siano $A = \{1, 2, 3\}$ e $\mathcal{S}_3$ l'insieme delle applicazioni biiettive di A in A; allora l'insieme $\mathcal{S}_3$ è costituito dalle seguenti sei applicazioni:

$$\begin{array}{rrr} id_A : A \to A & f_1 : A \to A & f_2 : A \to A \\ 1 \to 1 & 1 \to 2 & 1 \to 3 \\ 2 \to 2 & 2 \to 3 & 2 \to 1 \\ 3 \to 3 & 3 \to 1 & 3 \to 2 \end{array}$$

$$\begin{array}{rrr} f_3 : A \to A & f_4 : A \to A & f_5 : A \to A \\ 1 \to 2 & 1 \to 3 & 1 \to 1 \\ 2 \to 1 & 2 \to 2 & 2 \to 3 \\ 3 \to 3 & 3 \to 1 & 3 \to 2 \end{array}$$

Descriviamo innanzitutto l'insieme $\mathcal{S}_3$ in modo più compatto scrivendo le applicazioni come tabelle in cui, nella seconda riga, sotto ogni elemento della prima riga scriviamo la sua immagine:

$$id_A = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \quad f_1 = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix},$$

$$f_3 = \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}, \quad f_4 = \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}.$$

Con semplici calcoli si può allora verificare che:

$$f_2 = f_1^{-1}, \quad f_3 = f_3^{-1}, \quad f_4 = f_4^{-1}, \quad f_5 = f_5^{-1};$$

inoltre, ad esempio,

$$(f_1 \circ f_3)(1) = f_1(f_3(1)) = f_1(2) = 3,$$
$$(f_1 \circ f_3)(2) = f_1(f_3(2)) = f_1(1) = 2,$$
$$(f_1 \circ f_3)(3) = f_1(f_3(3)) = f_1(3) = 1,$$

onde $f_1 \circ f_3 = f_4$.

Lo studente si eserciti a calcolare gli altri prodotti possibili.

Definizione 1.2.11 Se $A = \{1, 2, \ldots, n\}$ è un insieme con n elementi, $n > 0$, si dice *permutazione sugli n elementi di A* una biiezione di A in A; l'insieme di tutte le permutazioni su un insieme con n elementi si denota con $\mathcal{S}_n$.

Consideriamo a questo punto due insiemi A e B aventi rispettivamente n e m elementi, $n, m > 0$; indichiamo con il simbolo B^A l'insieme delle applicazioni di dominio A e codominio B, ovvero:

$$B^A = \{f : A \longrightarrow B\}$$

Il simbolismo scelto dipende dalla seguente proprietà dell'insieme stesso.

Proposizione 1.2.5 *L'insieme B^A ha m^n elementi.*

Dimostrazione - Sia $A = \{a_1, a_2, \ldots, a_n\}$ e $B = \{b_1, b_2, \ldots, b_m\}$; allora per definire una funzione di dominio A e codominio B dobbiamo scegliere un'immagine per ogni elemento di A. Poiché, per ciascuno degli n elementi di A possiamo operare m scelte, le funzioni possibili saranno esattamente:

$$\underbrace{m \cdot m \cdot \ldots \cdot m}_{n-\text{volte}} = m^n \ . \blacksquare$$

A questo punto possiamo dimostrare la proposizione 1.1.1 stabilendo una biiezione fra l'insieme delle parti di un insieme A contenente n elementi e un opportuno insieme contenente 2^n elementi.

Proposizione 1.2.6 *Per ogni insieme non vuoto A è possibile stabilire una corrispondenza biunivoca fra l'insieme $\{0,1\}^A$ e l'insieme $\mathcal{P}(A)$.*

Dimostrazione - Definiamo un'applicazione α di dominio $\{0,1\}^A$ e codominio $\mathcal{P}(A)$ al modo seguente:

$$\begin{array}{rcccl} \alpha & : & \{0,1\}^A & \longrightarrow & \mathcal{P}(A) \\ & & f & \longrightarrow & f^{-1}(\{1\}) \end{array}$$

ovvero associamo ad ogni funzione f il sottoinsieme di A costituito da quegli elementi che, tramite f, hanno per immagine l'elemento 1.

Si verifica facilmente che α è un'applicazione biunivoca; infatti, se f e g sono due funzioni di dominio A e codominio $\{0,1\}$ tali che $f \neq g$, deve esistere almeno un elemento $a \in A$ per il quale risulti $f(a) \neq g(a)$. Supponendo ad esempio che sia $f(a) = 1$ e $g(a) = 0$ risulterà che $a \in f^{-1}(\{1\}) = \alpha(f)$ e $a \notin g^{-1}(\{1\}) = \alpha(g)$; pertanto $\alpha(f) \neq \alpha(g)$ e quindi α risulta essere iniettiva.

Per quanto riguarda la suriettività, sia S un qualsiasi sottoinsieme di A; posso allora considerare la funzione $f_S : A \longrightarrow \{0,1\}$, detta *funzione caratteristica di S*, definita al modo seguente:

$$\begin{cases} f_S(a) = 1 & \text{se } a \in S \\ f_S(a) = 0 & \text{se } a \notin S \end{cases}$$

risulta allora ovviamente $\alpha(f_S) = S$, onde α è suriettiva. $\blacksquare$

Definizione 1.2.12 L'insieme $\{0,1\}^A$ viene chiamato *insieme delle funzioni caratteristiche di A* .

Se $n \leq m$ ovvero l'insieme A ha al più tanti elementi quanti l'insieme B, possiamo considerare in B^A il sottoinsieme delle funzioni iniettive di dominio A e codominio B, indichiamolo con I; possiamo allora facilmente calcolare il numero degli elementi di tale insieme.

Proposizione 1.2.7 *L'insieme I ha $m(m-1)(m-2)\ldots(m-n+1)$ elementi.*

Dimostrazione - Sia $A = \{a_1, a_2, \ldots, a_n\}$; allora quando definiamo una funzione iniettiva, di dominio A abbiamo m scelte per l'elemento a_1, ne abbiamo $m-1$ per l'elemento a_2, e così via fino ad avere $m-(n-1)$ scelte per l'elemento a_n, onde l'asserto. ■

Corollario 1.2.1 *L'insieme $\mathcal{S}_n$ contiene $n(n-1)(n-2)\ldots 2\cdot 1$ elementi.*

Definizione 1.2.13 Il numero $n(n-1)(n-2)\ldots 2\cdot 1$ si indica con il simbolo $n!$ che si legge *n fattoriale*; convenzionalmente si pone $0! = 1$.

La proposizione precedente ci permette di contare quanti sono, in un insieme $A = \{a_1, a_2, \ldots, a_n\}$, i sottoinsiemi $S = \{s_1, s_2, \ldots, s_k\}$, aventi k elementi.

Infatti, per quanto appena dimostrato, le applicazioni iniettive di dominio $K = \{1, 2, \ldots, k\}$ e codominio l'insieme A sono $n(n-1)(n-2)\ldots(n-k+1)$, inoltre ognuna di tali applicazioni definisce un sottoinsieme di A contenente k elementi; d'altra parte lo stesso sottoinsieme si può ottenere in $k!$ modi, tante quante sono le biiezioni del sottoinsieme in se stesso.

Pertanto risulta che il numero dei sottoinsiemi con k elementi in un insieme con n elementi è

$$\binom{n}{k} = \frac{n(n-1)(n-2)\ldots(n-k+1)}{k!} = \frac{n!}{k!\cdot(n-k)!}.$$

Definizione 1.2.14 Il numero $\binom{n}{k}$ viene detto *coefficiente binomiale.*

Osservazione 1.2.2 Per come è definito il coefficiente binomiale, e utilizzando nella formula la convenzione $0! = 1$, abbiamo che:

$$\binom{n}{0} = \binom{n}{n} = 1.$$

Osserviamo inoltre che il nome "coefficiente binomiale" deriva dal fatto che vale la seguente relazione, che dimostreremo nel capitolo terzo:

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n.$$

Proposizione 1.2.8 *Per i coefficienti binomiali valgono le seguenti uguaglianze:*

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k} \qquad \forall \quad 0 \le k \le n.$$

Dimostrazione - Sia A un insieme contenente $n+1$ elementi e sia $a \in A$; per quanto detto precedentemente l'insieme $B = A\backslash\{a\}$ ha n elementi e contiene $\binom{n}{k-1}$ sottoinsiemi contenenti $k-1$ elementi e $\binom{n}{k}$ sottoinsiemi contenenti k elementi.

Se $T \subseteq B$ contiene $k-1$ elementi allora $T \cup \{a\}$ è un sottoinsieme di A contenente k elementi; d'altra parte se $S \subseteq A$ contiene k elementi allora sono possibili due casi: $S \subseteq B$, se $a \notin S$ e $S \backslash \{a\} \subseteq B$ se $a \in S$.

Possiamo allora costruire la seguente corrispondenza biunivoca:

$$\psi : \{X \subset A \ / \ |X| = k\} \longrightarrow \{Y \subset B \ / \ |Y| = k-1 \text{ o } |Y| = k\}$$

tale che

$$\begin{cases} \psi(X) = X \backslash \{a\} & \text{se } a \in X \\ \psi(X) = X & \text{se } a \notin X \end{cases}$$

Pertanto, essendo poi il numero dei sottoinsiemi con k elementi di A uguale a $\binom{n+1}{k}$, si ottiene l'uguaglianza desiderata. ■

1.3 RELAZIONI DI EQUIVALENZA

Definizione 1.3.1 Se A è un insieme, si dice *relazione* su A un sottoinsieme del prodotto cartesiano $A \times A$.

Se ρ denota una relazione su A, ovvero $\rho \subseteq A \times A$, per indicare che la coppia (x, y) appartiene al sottoinsieme ρ si scrive generalmente $x\rho y$ e si dice che x è in relazione ρ con y.

Esempio 1.3.1 Un esempio di relazione è quello che si ottiene considerando come insieme A l'insieme delle rette del piano e come sottoinsieme di $A \times A$ l'insieme $\rho = \{(r, r') \in A \times A \ / \ r \parallel r'\}$ costituito dalle coppie di rette parallele . Per denotare tale relazione scriveremo:

$$r, r' \in A, \ r\rho r' \overset{def}{\Longleftrightarrow} r \parallel r' \ .$$

Nello stesso insieme possiamo considerare anche un'altra relazione σ così definita:

$$r, r' \in A, \ r\sigma r' \overset{def}{\Longleftrightarrow} r \perp r'$$

dove la retta r è in relazione con la retta r' se, e solo se, r è perpendicolare a r'.

Le proprietà fondamentali di cui può godere una relazione su un insieme A sono le seguenti:

1) $\forall\, x \in A, \quad x\rho x$ (riflessiva),

2) $\forall\, x, y \in A, \quad x\rho y \Rightarrow y\rho x$ (simmetrica),

3) $\forall\, x, y \in A, \quad x\rho y$ e $y\rho x \Rightarrow x = y$ (antisimmetrica),

4) $\forall\, x, y, z \in A, \ x\rho y$ e $y\rho z \Rightarrow x\rho z$ (transitiva).

Per quanto riguarda le relazioni definite nell'esempio precedente possiamo dire che ρ è una relazione riflessiva simmetrica e transitiva mentre σ è solamente simmetrica.

Osservazione 1.3.1 Se ρ è una relazione su A che verifica sia la proprietà simmetrica che quella antisimmetrica, allora ρ è la relazione identica, cioè la relazione definita al modo seguente: $x\rho y \Leftrightarrow x = y$. Infatti, se $x, y \in A$ sono tali che $x\rho y$, allora per la proprietà simmetrica risulta $y\rho x$ e quindi, per la proprietà antisimmetrica, $x = y$.

Esempio 1.3.2 In $\mathbb{N}^*$ la relazione di divisibilità:

$$n, m \in \mathbb{N},\ n\rho m \quad \overset{def}{\Longleftrightarrow} \quad \exists\, k \in \mathbb{N} : m = kn.$$

gode della proprietà riflessiva poiché, $\forall\, n \in \mathbb{N}$, $n = 1 \cdot n$, della proprietà transitiva poiché $m = kn$ e $s = hm$ implica $s = hkn$ e della proprietà antisimmetrica; infatti, se $n\rho m$ e $m\rho n$, allora risulta:

$$m = kn \text{ e } n = hm \Rightarrow m = khm \Rightarrow hk = 1 \Rightarrow h = k = 1 \Rightarrow m = n$$

e pertanto tale relazione gode della proprietà antisimmetrica.

Definizione 1.3.2 Una relazione ρ su un insieme A si dice *relazione di equivalenza* se verifica le tre proprietà: riflessiva, simmetrica e transitiva.

Definizione 1.3.3 Se A è un insieme, ρ una relazione di equivalenza su A e x un elemento di A, si dice *classe di equivalenza* di x, e si denota $[x]$ o $\overline{x}$, l'insieme degli elementi di A che sono in relazione con x, ovvero:

$$[x] \;=\; \{\ y \in A \ /\ x\rho y\ \};$$

l'elemento x prende il nome di *rappresentante* della classe $[x]$.

Esempio 1.3.3 Sia $A = \mathbb{Z}$ e sia ρ la relazione definita al modo seguente:

$$x\rho y \Leftrightarrow |\ x\ | = |\ y\ |,$$

dove $|\ x\ | = x$ se $x \geq 0$, $|\ x\ | = -x$ se $x \leq 0$ e $|\ x\ |$ è chamato il *modulo* di x.

Ovviamente tale relazione gode delle proprietà riflessiva, simmetrica e transitiva e quindi è di equivalenza; se $x \in \mathbb{Z}^*$ allora $[x] = \{x, -x\}$, poiché due interi differenti hanno lo stesso modulo se, e solo se, sono uno l'opposto dell'altro. Per $x = 0$ risulta poi $[0] = \{0\}$.

Esempio 1.3.4 In $\mathbb{R} \times \mathbb{R}$ si consideri la relazione:

$$(x, y)\rho(z, w) \Leftrightarrow x = z$$

verifichiamo che ρ è una relazione di equivalenza; ρ gode ovviamente della proprietà riflessiva e della proprietà simmetrica. Per quanto riguarda la proprietà transitiva si ha che:

$$(x, y)\rho(z, w),\ (z, w)\rho(u, v) \Rightarrow x = z,\ z = u \Rightarrow x = u \Rightarrow (x, y)\rho(u, v).$$

La relazione ρ è quindi di equivalenza e la classe di equivalenza della coppia (x, y) è:

$$[(x, y)] = \{(x, k)/k \in \mathbb{R}\}.$$

Relativamente alle classi di equivalenza si dimostra la seguente proposizione:

Proposizione 1.3.1 *Sia A un insieme e ρ una relazione di equivalenza su A; si ha allora che:*

i) $\forall\, x \in A \;\Rightarrow\; x \in [x]$;

ii) $\forall\, x, y \in A \;\Rightarrow\; [\; x \in [y] \Leftrightarrow [x] = [y] \;]$;

iii) $\forall\, x, y \in A \;\Rightarrow\; [\; [x] \cap [y] \neq \emptyset \Leftrightarrow [x] = [y] \;]$.

Dimostrazione - La i) è conseguenza della proprietà riflessiva poiché, $\forall\, x \in A$, $x\rho x$ e quindi $x \in [x]$. Per quanto riguarda la ii) osserviamo che se $[x] = [y]$ dalla i) segue $x \in [y]$.

Viceversa, se $x \in [y]$, ovvero $y\rho x$, sono verificate le due inclusioni $[x] \subseteq [y]$ e $[y] \subseteq [x]$; infatti $z \in [x]$ implica $x\rho z$, dalla $y\rho x$ per la proprietà transitiva risulta $y\rho z$ ovvero $z \in [y]$ e quindi $[x] \subseteq [y]$. Analogamente si dimostra l'inclusione $[y] \subseteq [x]$.

Infine, per dimostrare la iii), dimostriamo innanzitutto che $[x] \cap [y] \neq \emptyset$ implica $[x] = [y]$. Sia dunque $z \in [x] \cap [y]$; per definizione di intersezione risulta $z \in [x]$ e $z \in [y]$, onde $x\rho z$ e $y\rho z$, da cui, per la proprietà simmetrica, $z\rho y$ e, per la transitiva, $x\rho y$ e quindi $y \in [x]$. Da ciò segue, per la ii), $[x] = [y]$; l'implicazione inversa: $[x] = [y] \Rightarrow [x] \cap [y] \neq \emptyset$ è ovvia. ■

Definizione 1.3.4 Si dice *insieme quoziente* di A rispetto alla relazione di equivalenza ρ, e si denota con A/ρ, l'insieme delle classi di equivalenza degli elementi di A, cioè:

$$A/\rho \;=\; \{[x] \;/\; x \in A\}.$$

Esempio 1.3.5 Se la relazione ρ è quella dell'esempio 1.3.3 si ha che:

$$\mathbb{Z}/\rho = \{\{x, -x\} \;/\; x \in \mathbb{Z}\}.$$

Se invece la relazione ρ è quella dell'esempio 1.3.4 allora risulta:

$$\mathbb{R} \times \mathbb{R}/\rho = \{\{(x, k) \;/\; k \in \mathbb{R}\} \;:\; x \in \mathbb{R}\}.$$

Tale esempio può essere visualizzato pensando al piano dotato di un riferimento cartesiano di assi X e Y; ogni classe di equivalenza corrisponde allora ad una retta parallela all'asse Y.

Approfondiamo ora il significato dell'insieme quoziente; diamo innanzitutto la seguente definizione.

Definizione 1.3.5 Dato un insieme A, si dice *partizione* di A una famiglia $\mathcal{F} = \{A_i\}_{i \in I}$ di sottoinsiemi non vuoti di A tali che:

i) $\displaystyle\bigcup_{i \in I} A_i \;=\; A$,

ii) $A_i \cap A_j \;=\; \emptyset$ per $i \neq j$.

Vogliamo ora mostrare il forte legame esistente tra le partizioni di un insieme A e le relazioni di equivalenza su A.

Proposizione 1.3.2 *Sia A un insieme e sia ρ una relazione di equivalenza su A; allora l'insieme quoziente $A/\rho = \{[x] \ / \ x \in A\}$ è una partizione di A.*

Dimostrazione - La dimostrazione utilizza i risultati della proposizione 1.3.1; innanzitutto ogni classe di equivalenza è non vuota poiché $x \in [x]$, $\forall\ x \in A$. Inoltre, per questo stesso motivo, risulta $\bigcup_{x \in A}[x] = A$; infine due classi di equivalenza coincidono o sono disgiunte, onde l'asserto. ■

In effetti possiamo dimostrare che i concetti di relazione di equivalenza e di partizione sono fra loro intercambiabili, come mostra la seguente proposizione.

Proposizione 1.3.3 *Sia A un insieme e sia $\mathcal{F} = \{A_i\}_{i \in I}$ una partizione di A; allora la relazione ρ su A definita al modo seguente:*

$$x\rho y \Leftrightarrow \exists\ i \in I : x, y \in A_i$$

è una relazione di equivalenza, che prende il nome di equivalenza associata alla partizione $\mathcal{F}$.

Dimostrazione - Innanzitutto, $\forall\ x \in A$, $x\rho x$ poiché $A = \bigcup_{i \in I} A_i$, onde $\exists\ i \in I$ tale che $x \in A_i$; inoltre, se $x\rho y$, allora $x, y \in A_j$ per qualche $j \in I$ e quindi risulta ovviamente che $y\rho x$. Per quanto riguarda la proprietà transitiva, se $x\rho y$ e $y\rho z$ allora $\exists\ i, j \in I$ tali che $x, y \in A_i$ e $y, z \in A_j$; poiché $A_i \cap A_j = \emptyset$ se $i \neq j$, A_i e A_j, contenendo entrambi l'elemento y, coincidono e pertanto $x, z \in A_i = A_j$, onde $x\rho z$. ■

Osservazione 1.3.2 Osserviamo che, dato un insieme A e una relazione ρ su A, la relazione associata alla partizione A/ρ di A coincide con ρ, come si verifica facilmente; analogamente, se si considera una partizione $\mathcal{F}$ di A, la partizione ottenuta con le classi di equivalenza della relazione definita su A a partire da $\mathcal{F}$ coincide con $\mathcal{F}$.

Per questo motivo è assolutamente equivalente assegnare su di un insieme una relazione di equivalenza o una partizione.

Oltre che con le partizioni, il concetto di relazione di equivalenza è anche strettamente collegato con il concetto di applicazione, cerchiamo di capire bene in che modo.

Innanzitutto a partire da una relazione di equivalenza su un insieme A possiamo definire una particolare funzione di dominio A.

Definizione 1.3.6 Se A è un insieme e ρ è una relazione di equivalenza su A, l'applicazione $\pi : A \to A/\rho$ definita ponendo, $\forall\ x \in A$, $\pi(x) = [x]$, ovvero l'applicazione che associa a ciascun elemento x di A la sua classe di equivalenza, è un'applicazione suriettiva, come si verifica immediatamente, che prende il nome di *proiezione canonica.*

Inoltre, a partire da una funzione di dominio un insieme A è possibile definire in A una particolare relazione di equivalenza.

Definizione 1.3.7 Sia A un insieme ed f un'applicazione avente A come dominio; definiamo la seguente relazione ρ in A:

$$x\rho y \Leftrightarrow f(x) = f(y) \ .$$

È facile convincersi che tale relazione è di equivalenza; inoltre, $\forall\ x \in A$, risulta $[x] = \{y \in A : f(x) = f(y)\}$. La relazione di equivalenza appena considerata si dice *equivalenza associata* ad f .

I concetti definiti nelle due definizioni precedenti sono strettamente legati. Si può infatti dimostrare il seguente teorema, detto *teorema di omomorfismo per gli insiemi* o *teorema di decomposizione delle applicazioni.*

Proposizione 1.3.4 *Siano A e B due insiemi e sia f un'applicazione di A in B; se ρ denota l'equivalenza associata ad f e π denota la proiezione canonica di A su A/ρ , esiste unica $\overline{f}\ :\ A/\rho \to Imf$ biiettiva tale che $j \circ \overline{f} \circ \pi = f$, dove $j : Imf \to B$ è tale che $j(x) = x$, $\forall\ x \in Imf$.*

Dimostrazione - Definiamo, $\forall\ [x] \in A/\rho$, $\overline{f}([x]) = f(x)$; dimostriamo innanzitutto che $\overline{f}$ è ben definita, cioè che non dipende dalla scelta del rappresentante nella classe. A tal fine sia $y \in [x]$; risulta allora $x\rho y$ e, per come è definita ρ , $f(x) = f(y)$, onde $\overline{f}$ è un'applicazione. La suriettività di $\overline{f}$ è ovvia proprio per come è definita; occorre quindi dimostrare che $\overline{f}$ è iniettiva.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi"'] & B \\ A/\rho \arrow[r, "\overline{f}"] & Imf \arrow[u, "j"'] \end{tikzcd}$$

Siano $[x], [y] \in A/\rho$ tali che $\overline{f}([x]) = \overline{f}([y])$, ovvero $f(x) = f(y)$; dalla definizione di ρ risulta allora $x\rho y$ e pertanto $[x] = [y]$, da cui l'iniettività di $\overline{f}$. Per dimostrare l'uguaglianza $j \circ \overline{f} \circ \pi = f$ osserviamo innanzitutto che le due funzioni, $j \circ \overline{f} \circ \pi$ e f, hanno lo stesso dominio e lo stesso codominio; risulta poi $\forall\ x \in A$:

$$(j \circ \overline{f} \circ \pi)(x) = j(\overline{f}(\pi(x))) = j(\overline{f}([x])) = j(f(x)) = f(x).$$

Dalla definizione di uguaglianza fra applicazioni segue allora che $j \circ \overline{f} \circ \pi = f$. Rimane da dimostrare che l'applicazione $\overline{f}$, tale che $j \circ \overline{f} \circ \pi = f$, è unica; a tal fine sia $\tilde{f}$ un'applicazione di A/ρ in Imf tale che $j \circ \tilde{f} \circ \pi = f$. Risulta allora, $\forall\ [x] \in A/\rho$:

$j \circ \tilde{f} \circ \pi(x) = j(\tilde{f}([x])) = f(x)$ ovvero, per come è definita j, $\tilde{f}([x]) = f(x)$,

e quindi $\tilde{f} = \overline{f}$. ■

Esempio 1.3.6 Siano $A = \{2, 3, \ldots, 30\}$, $B = \{1, 2, 3, \ldots, 100\}$ e f l'applicazione di dominio A e codominio B definita al modo seguente:

$$f(a) = p \text{ dove } p \text{ è il più grande fra i primi che dividono } a$$

ad esempio $f(14) = 7$, $f(30) = 5$.

Risulta allora che la relazione di equivalenza ρ associata a f è quella individuata dalla seguente partizione di A:

$$\mathcal{F} = \{\{2,4,8,16\}, \{3,6,9,12,18,24,27\}, \{5,10,15,20,25,30\}, \{7,14,21,28\},$$

$$\{11,22\}, \{13,26\}, \{17\}, \{19\}, \{23\}, \{29\}\}$$

e quindi, ad esempio, $12\rho 24$ e $12 \not\rho 15$.

Infine $Imf = \{2,3,5,7,11,13,17,19,23,29\}$, $A/\rho = \mathcal{F}$ e la biiezione $\overline{f}$ di cui alla proposizione precedente è la seguente:

$$\begin{array}{lcll}
\overline{f} & : & A/\rho & \longrightarrow & Imf \\
 & & \{2,4,8,16\} & \longrightarrow & 2 \\
 & & \{3,6,9,12,18,24,27\} & \longrightarrow & 3 \\
 & & \{5,10,15,20,25,30\} & \longrightarrow & 5 \\
 & & \{7,14,21,28\} & \longrightarrow & 7 \\
 & & \{11,22\} & \longrightarrow & 11 \\
 & & \{13,26\} & \longrightarrow & 13 \\
 & & \{17\} & \longrightarrow & 17 \\
 & & \{19\} & \longrightarrow & 19 \\
 & & \{23\} & \longrightarrow & 23 \\
 & & \{29\} & \longrightarrow & 29
\end{array}$$

come si verifica immediatamente.

1.4 RELAZIONI D'ORDINE

Nell'insieme $\mathbb{N}$ dei numeri naturali la relazione $\leq$ gode delle proprietà riflessiva, antisimmetrica e transitiva; le stesse proprietà valgono, ad esempio, nell'insieme delle parole di un dizionario, ordinate secondo l'ordine lessicografico. In generale si può dare la seguente definizione.

Definizione 1.4.1 Se A è un insieme, una relazione ρ su A si dice *relazione d'ordine* se verifica le seguenti tre proprietà:

$\forall\, a \in A$	,	$a\rho a$	proprietà riflessiva,
$\forall\, a, b \in A$	,	$a\rho b$ e $b\rho a \Rightarrow a = b$	proprietà antisimmetrica,
$\forall\, a, b, c \in A$	,	$a\rho b$ e $b\rho c \Rightarrow a\rho c$	proprietà transitiva.