

# Note del Corso di Analisi Matematica 1\*

Alberto Berretti

*Numero pondere et mensura Deus omnia condidit* - Isaac Newton, 1643 – 1727.

## Parte I.

### Fondamenti

In questo capitolo introduciamo gli oggetti fondamentali che ci serviranno per lavorare: sostanzialmente i numeri, dai naturali ai reali. Prima richiameremo alcune nozioni fondamentali di logica e di teoria degli insiemi che sono indispensabili per proseguire.

#### 1. Richiami di Logica e di Teoria degli Insiemi

##### 1.1. I simboli della logica formale

Una proposizione è una affermazione che può essere vera o falsa. A partire da proposizioni date si possono costruire delle proposizioni più complesse la cui verità o falsità dipende ad quella delle proposizioni con le quali sono costruite: in altri termini, possiamo introdurre delle vere e proprie “operazioni” sulle proposizioni, il che conduce ad un vero e proprio “calcolo proposizionale”. Nella tabella seguente introduciamo i simboli per le principali operazioni sulle proposizioni.

---

\*Quest'opera è distribuita con licenza “Creative Commons - Attribuzione - Non commerciale - Non opere derivate 3.0 Italia (CC BY-NC-ND 3.0)” (v. <http://creativecommons.org/licenses/by-nc-nd/3.0/it/deed.it>). Ringrazio il Prof. Roberto Zanasi (<http://prooof.blogspot.com/>) per molti utili suggerimenti volti a migliorare la qualità di questo testo.

non $p$	$\neg p$	è vera se e solo se $p$ è falsa
$p$ e $q$	$p \wedge q$	è vera se e solo se sia $p$ che $q$ sono vere
$p$ o $q$	$p \vee q$	è vera se almeno una di $p$ o $q$ è vera
se $p$ allora $q$	$p \Rightarrow q$	è vera se ogni volta che $p$ è vera allora anche $q$ è vera
$p$ se e solo se $q$	$p \Leftrightarrow q$	è vera se $p$ e $q$ sono vere e false insieme

Nella tabella seguente sono elencate le principali “equivalenze” fra operazioni logiche, tutte piuttosto ovvie anche al senso comune.

$\neg(p \wedge q)$	equivale a	$\neg p \vee \neg q$
$\neg(p \vee q)$	equivale a	$\neg p \wedge \neg q$
$p \Rightarrow q$	equivale a	$\neg(p \wedge \neg q)$
	ovvero	$\neg p \vee q$
$p \Leftrightarrow q$	equivale a	$(p \Rightarrow q) \wedge (q \Rightarrow p)$

Le proposizioni possono dipendere da più variabili: in tal caso si parla di PREDICATI. Se una proposizione dipende da variabili, allora può essere vera o falsa a seconda del valore delle variabili: può essere sempre vera, può essere talvolta vera, può non essere mai vera. Per indicare tali situazioni, si introducono i QUANTIFICATORI:

Quantificatore universale	$\forall x P(x)$	“per ogni” valore della variabile $x$ $P(x)$ è vera
Quantificatore esistenziale	$\exists x P(x)$	“per qualche” valore della variabile $x$ $P(x)$ è vera ovvero “esiste almeno un” valore della variabile $x$ per cui $P(x)$ vera

“Ovviamente”:

$\neg(\forall x P(x))$	equivale a	$\exists x \neg P(x)$
$\neg(\exists x P(x))$	equivale a	$\forall x \neg P(x)$

Infatti se non è vero che per ogni  $x$   $P(x)$  è vera, deve essere falsa per qualche  $x$ , e se non esiste un  $x$  per cui  $P(x)$  è vera, deve essere falsa per ogni  $x$ .

A volte sono comode le seguenti notazioni:

$\nexists x P(x)$	come abbreviazione di	$\neg(\exists x P(x))$
$\exists! x P(x)$	vuol dire	esiste esattamente un $x$ tale che $P(x)$ vera

Inoltre, nelle formule, la frase “tale che” viene scritta spesso con il simbolo “|” (barra verticale).

## 1.2. Insiemi ed operazioni sugli insiemi

Lungi dal voler introdurre la definizione assiomatica di insieme, ci appoggiamo sul concetto intuitivo di insieme, consci del limite di tale posizione.

Un INSIEME è un aggregato piú o meno qualsiasi di oggetti detti ELEMENTI.

Che c'è qualcosa che non va in tale (pseudo-) definizione è quasi ovvio e ben noto sin dalla fine del XIX secolo. Infatti, se ammettiamo che un insieme possa essere una collezione *arbitraria* di oggetti, allora cadiamo in una serie di paradossi logici di cui il seguente è il piú semplice: basta chiedersi se l'insieme di tutti gli insiemi che non contengono se stessi contenga o no se stesso; se contiene se stesso, allora non può contenere se stesso perché contiene se stesso, mentre se non contiene se stesso allora per definizione contiene se stesso. La migliore via di uscita da tale pantano logico consiste nel *non definire* gli insiemi, bensí nell'enunciare degli assiomi che permettano di parlarne in modo rigoroso, senza porsi il problema di cosa un insieme effettivamente sia.

Per indicare che l'oggetto  $x$  è un elemento dell'insieme  $S$  (ovvero che  $x$  “appartiene” ad  $S$ ) si scrive  $x \in S$ . La sua negazione ( $x$  non è elemento di  $S$ , ovvero  $x$  non appartiene ad  $S$ ) si scrive  $x \notin S$ .

Se due insiemi hanno gli stessi elementi, allora sono lo stesso insieme (questo in effetti sarebbe il primo assioma nella teoria degli insiemi, l'*assioma di estensionalità*).

Un insieme privo di elementi (ed ovviamente esiste solo *un* insieme privo di elementi!) è detto INSIEME VUOTO ed è indicato con il simbolo  $\emptyset$  (la sua esistenza è il secondo assioma nella teoria degli insiemi).

Si noti la differenza fra un oggetto  $a$  e l'insieme  $\{a\}$ : il secondo *non è*  $a$ , ma l'insieme il cui unico elemento è  $a$ ; sono due cose diverse.

Se tutti gli elementi di  $A$  sono anche elementi di  $B$  (ma in  $B$  ci possono essere elementi che non sono anche in  $A$ ) allora si dice che  $A$  è un SOTTOINSIEME di  $B$  e si scrive  $A \subseteq B$  oppure  $B \supseteq A$ . Se ogni elemento di  $A$  è contenuto in  $B$  e ci sono elementi di  $B$  che non sono in  $A$  allora si dice che  $A$  un SOTTOINSIEME PROPRIO di  $B$  e si scrive  $A \subset B$  oppure  $B \supset A$  (oppure, se si vuole sottolineare il fatto che  $A$  è effettivamente proprio, si può scrivere  $A \subsetneq B$  oppure  $B \supsetneq A$ ). Ovviamente l'insieme vuoto è un sottoinsieme di qualsiasi insieme.

L'insieme di tutti i sottoinsiemi di  $A$  viene detto **INSIEME POTENZA** o **INSIEME DELLE PARTI** di  $A$  ed indicato con  $\mathcal{P}(A)$  oppure con la notazione (apparentemente bizzarra)  $2^A$ . Ad es., se  $A = \{0, 1, 2\}$ , allora abbiamo:

$$\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{2, 3\}, \{1, 3\}, \{1, 2\}, \{1, 2, 3\}\}.$$

La ragione per cui l'insieme delle parti viene anche detto *insieme potenza* ed indicato come una potenza di 2 è che l'insieme delle parti di un insieme di  $n$  elementi è formato da esattamente  $2^n$  elementi, come un semplice calcolo che potrebbe essere fatto più avanti dimostra.

Le principali operazioni che possiamo eseguire sugli insiemi riflettono le operazioni logiche.

Dati due insiemi  $A$  e  $B$ ,  $A \cup B$  è l'**UNIONE** degli insiemi  $A$  e  $B$ , ovvero l'insieme i cui elementi sono elementi di  $A$  o elementi di  $B$ ;  $A \cap B$  è l'**INTERSEZIONE** degli insiemi  $A$  e  $B$ , ovvero l'insieme i cui elementi sono elementi sia di  $A$  che di  $B$ . La **DIFFERENZA** di due insiemi  $A$  e  $B$ , indicata con  $A \setminus B$ , è l'insieme degli elementi di  $A$  che non appartengono a  $B$ :

$$x \in A \setminus B \Leftrightarrow x \in A \wedge x \notin B. \quad (1)$$

Definiamo anche la **DIFFERENZA SIMMETRICA** tra due insiemi:

$$A \Delta B = (A \setminus B) \cup (B \setminus A), \quad (2)$$

per cui un elemento appartiene a  $A \Delta B$  se appartiene a  $A$  o a  $B$  ma non ad entrambe.

Dato un *insieme contesto*  $\mathcal{U}$  di cui  $A$  è sottoinsieme, il suo **COMPLEMENTO RISPETTO AD  $\mathcal{U}$**  indicato con  $\complement_{\mathcal{U}}A$  (o brevemente  $\complement A$  se l'insieme contesto  $\mathcal{U}$  è ovvio) è la differenza  $\mathcal{U} \setminus A$ , cioè l'insieme degli elementi di  $\mathcal{U}$  che non appartengono a  $A$ . Lo scopo dell'insieme contesto è quello di far sí che il complemento non contenga *troppe cose*.

Le proprietà di tali operazioni sugli insiemi sono piuttosto ovvie e dipendono da quelle della logica formale. Nella tabella seguente riassumiamo le principali tali proprietà: si tratta di cose piuttosto ovvie e ben note perlomeno dalle scuole superiori.

---

$A \cup A = A \cap A = A$	idempotenza
$A \cup B = B \cup A$	commutatività dell'unione
$A \cap B = B \cap A$	commutatività dell'intersezione
$A \cup (B \cup C) = (A \cup B) \cup C$	associatività dell'unione
$A \cap (B \cap C) = (A \cap B) \cap C$	associatività dell'intersezione
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	distributività di $\cup$ rispetto a $\cap$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	distributività di $\cap$ rispetto a $\cup$
$A \cup \emptyset = A \quad A \cap \emptyset = \emptyset$	
$\complement(\complement A) = A; \quad A \cup \complement A = \mathcal{U}; \quad A \cap \complement A = \emptyset$	
$\complement(A \cup B) = \complement A \cap \complement B$	prima legge di De Morgan
$\complement(A \cap B) = \complement A \cup \complement B$	seconda legge di De Morgan

---

### 1.3. Insiemi complessi, relazioni, funzioni

Dati due insiemi  $A$  e  $B$  il **PRODOTTO CARTESIANO**  $A \times B$  è l'insieme delle coppie *ordinate*  $(a, b)$  tali che  $a \in A$  e  $b \in B$ . È importante sottolineare che  $(a, b)$  è *molto* diverso dall'insieme  $\{a, b\}$ : infatti, ad es.  $\{a, b\} = \{b, a\}$  mentre invece  $(a, b) \neq (b, a)$ .

Questa è una definizione informale. Una definizione formale di  $A \times B$  è, ad es., la seguente:

$$A \times B = \{\{a, b\}, a, a \in A, b \in B\},$$

cioè l'insieme formato da coppie di oggetti: il primo è a sua volta un insieme di due elementi formato da un elemento del primo insieme ed uno del secondo, mentre il secondo è l'elemento che deve essere considerato il primo nella coppia ordinata. Sottolineiamo che non vi è nulla di "magico" in questa definizione, semplicemente occorre introdurre il concetto di "primo elemento di due" in qualche modo e tale definizione lo fa in modo semplice.

Analogamente possiamo definire terne, quaterne, ed in generale  $n$ -uple *ordinate* di elementi di tre, quattro ed in generale  $n$  insiemi  $A_i$ . Se  $A \neq B$  i due insiemi  $A \times B$  e  $B \times A$  sono ovviamente diversi. Se  $A = B$ , si scrive  $A^2$  invece che  $A \times A$ , e così via per terne, quaterne etc.

Una **RELAZIONE** tra due insiemi  $A$  e  $B$  è un predicato binario  $r(a, b)$  con  $a \in A$  e  $b \in B$ , cioè una affermazione che può essere vera o falsa e che dipende da *due* oggetti  $a \in A$  e  $b \in B$ . Il sottoinsieme di  $A \times B$  per cui  $r(a, b)$  è vera viene detto **GRAFICO** di  $r$  e si indica con  $\Gamma_r$  o  $\text{graph}(r)$ . Viceversa dato un sottoinsieme  $G \subseteq A \times B$  è automaticamente definita la relazione:

$$r_G(a, b) = \begin{cases} \text{Vero} & \text{se } (a, b) \in G, \\ \text{Falso} & \text{se } (a, b) \notin G. \end{cases}$$

Definiamo ora tre tipi importanti di relazioni.

### 1.3.1. Relazioni d'ordine

Una relazione  $r(a, b)$ , dove  $a, b \in A$ , è una RELAZIONE D'ORDINE (che indichiamo nel seguito con la notazione  $a \leq b$  ovvero  $b \geq a$ , leggi  $a$  precede  $b$  ovvero  $b$  segue  $a$ ) se:

$$\forall a \in A : a \leq a \quad (\text{proprietà riflessiva}), \quad (3a)$$

$$\forall a, b \in A : a \leq b \wedge b \leq a \Rightarrow a = b \quad (\text{proprietà antisimmetrica}), \quad (3b)$$

$$\forall a, b, c \in A : a \leq b \wedge b \leq c \Rightarrow a \leq c \quad (\text{proprietà transitiva}); \quad (3c)$$

proprietà analoghe valgono allora per  $\geq$ .

Se  $a \leq b$  ma  $a \neq b$  allora diremo che la relazione d'ordine fra i due elementi considerati è STRETTA e scriveremo  $a < b$ ; analogamente se  $a \geq b$  ma  $a \neq b$  scriveremo  $a > b$ . L'essere in relazione d'ordine stretta è una proprietà di  $a$  e  $b$ , non della relazione d'ordine  $\leq$ !

Un insieme dotato di una relazione d'ordine viene detto INSIEME ORDINATO. Se  $\forall a, b \in A$  vale o  $a \leq b$  o  $b \leq a$  (cioè se  $\forall a, b \in A$ ,  $a, b$  sono CONFRONTABILI allora la relazione d'ordine è una RELAZIONE D'ORDINE TOTALE e l'insieme  $A$  viene detto TOTALMENTE ORDINATO (altrimenti è solo PARZIALMENTE ORDINATO).

**Esempio 1.** L'insieme delle parti di un insieme dato è ordinato dalla relazione di inclusione  $\subseteq$ . Ovviamente si tratta di una relazione d'ordine parziale (due sottoinsiemi possono essere disgiunti e quindi non confrontabili).

**Esempio 2.** L'insieme dei punti che giacciono su una retta orientata è un insieme totalmente ordinato dalla relazione “ $P_1$  giace a sinistra di  $P_2$ ”.

Introduciamo ora alcuni importanti concetti che saranno centrali nel seguito, nel contesto di insiemi numerici. Poiché riguardano solo la relazione di ordinamento totale, possiamo utilmente anticiparli ora.

Sia  $A$  un insieme totalmente ordinato e  $B \subseteq A$ .  $x \in A$  è un MAGGIORANTE di  $B$  se  $\forall y \in B$   $y \leq x$ ; è un MINORANTE di  $B$  se  $\forall y \in B$   $y \geq x$ .  $B$  è LIMITATO SUPERIORMENTE se possiede almeno un maggiorante, ed è LIMITATO INFERIORMENTE se possiede almeno un minorante. È LIMITATO se è limitato sia superiormente che inferiormente.

Un maggiorante di  $B$  che fa anche parte di  $B$  è un MASSIMO di  $B$ ; un minorante di  $B$  che fa anche parte di  $B$  è un MINIMO di  $B$ .

Il lettore dovrebbe fermarsi a riflettere un attimo su queste definizioni *formali*, e comprendere che effettivamente sono la versione rigorosa dell'idea intuitiva di massimo, minimo, e di limitatezza di un insieme.

**Proposizione 1.** *Il massimo ed il minimo di un insieme, qualora esistono, sono unici.*

*Dimostrazione.* Siano  $x_1, x_2$  massimi di  $B$ , e  $x_1 \neq x_2$ : ad es.  $x_1 < x_2$  (altrimenti basta scambiare  $x_1$  con  $x_2$ ...); quindi  $x_1$  non è un maggiorante di  $B$  (perché  $x_2 \in B$ ), contraddicendo l'ipotesi. Analogamente per il minimo. □

Sia di nuovo  $B \subseteq A$ ,  $A$  totalmente ordinato. Il massimo dei minoranti di  $B$  viene detto ESTREMO INFERIORE di  $B$ , mentre il minimo dei maggioranti viene detto ESTREMO SUPERIORE di  $B$ . Si usano le seguenti notazioni:

$\max B$	massimo di $B$
$\min B$	minimo di $B$
$\sup B$	estremo superiore di $B$
$\inf B$	estremo inferiore di $B$

Essendo gli estremi superiore/inferiore dei minimi/massimi rispettivamente, la proposizione precedente si applica per cui se essi esistono sono unici. Abbiamo inoltre la seguente proposizione.

**Proposizione 2.** *Valgono le seguenti relazioni tra estremi superiore/inferiore e massimi/minimi:*

1. Se  $x = \max B$  allora  $x = \sup B$
2. Se  $x = \sup B$  e  $x \in B$  allora  $x = \max B$
3. Se  $x = \min B$  allora  $x = \inf B$
4. Se  $x = \inf B$  e  $x \in B$  allora  $x = \min B$

*Dimostrazione.* (1) Se  $x$  è un massimo, allora appartiene a  $B$ , quindi ogni  $y < x$  non è un maggiorante; anzi, ogni  $y < x$  è un *minorante dell'insieme dei maggioranti*. Anche  $x$  è un minorante dell'insieme dei maggioranti (altrimenti non potrebbe far parte di  $B$ ! pensarci sopra un attimo!) e quindi, poiché è in quanto massimo un maggiorante di  $B$ , fa parte dell'insieme dei maggioranti di  $B$  e quindi ne è il minimo. Essendo il minimo dei maggioranti, è l'estremo superiore. (2) È praticamente la definizione di massimo. (3) e (4) Le dimostrazioni sono analoghe alle precedenti.  $\square$

**Proposizione 3.** *Se  $B \subseteq A$  è un sottoinsieme finito (non vuoto!) di un insieme totalmente ordinato  $A$ , allora  $B$  ha massimo e minimo.*

*Dimostrazione.* È ovvia e “costruttiva”: se  $B$  ha  $n$  elementi, con  $n-1$  confronti si determina il massimo (analogamente il minimo). Oppure alternativamente: supponiamo che non esista il massimo; allora se  $x_1 \in B$   $x_1$  non è un maggiorante, quindi  $\exists x_2 > x_1, x_2 \in B$ . Ma nemmeno  $x_2$  è un maggiorante per la medesima ragione, per cui esiste  $x_3 > x_2, x_3 \in B$ : e così via. Quindi  $B$  ha infiniti elementi, il che contraddice l'ipotesi che sia un insieme finito.  $\square$

Le due precedenti proposizioni possono sembrare inutili e sciocche in quanto ovvie. In realtà, il massimo ed il minimo di un insieme sono stati definiti in un modo preciso e formale e quindi il rigore vuole che tutte le proprietà del massimo e del minimo vengano dedotte formalmente da tali

definizioni, e non appellandosi al significato che tali parole hanno nel linguaggio comune (che non è formalmente rigoroso come il linguaggio matematico). A volte diremo che un certo teorema o una certa proposizione è ovvia: *ciò non significa che una dimostrazione non è necessaria perché al senso comune il fatto appare scontato*, ma vuole dire che il lettore giunto al livello di sofisticazione matematica necessario è in grado di fornire una dimostrazione formalmente rigorosa dopo qualche attimo di riflessione. A volte gli enunciati che al senso comune appaiono più ovvi in matematica sono di dimostrazione molto ardua, o comunque non banale.

### 1.3.2. Funzioni

Una FUNZIONE è una relazione  $r$  tra due insiemi  $A$  e  $B$  tale che:

$$\forall a \in A \exists b \in B : r(a, b), \quad (4a)$$

$$\forall a \in A \forall b_1, b_2 \in B : r(a, b_1) \wedge r(a, b_2) \Rightarrow b_1 = b_2. \quad (4b)$$

**Nota.** Una funzione viene detta talvolta APPLICAZIONE. “Applicazione” è sinonimo di funzione.

Cosa vuol dire questa definizione? (4a) vuol dire che *ad ogni*  $a \in A$  corrisponde un elemento di  $B$  che è in relazione con  $a$ , e (4b) vuol dire che se  $b_1, b_2$  sono in relazione con  $a$  allora  $b_1 = b_2$ , cioè che *l'elemento di  $B$  con cui  $a \in A$  è in relazione è unico*. Visto che ciascun elemento di  $A$  è in relazione con un *unico* elemento di  $B$ , possiamo pensare alla funzione come ad una “regola” che, dato  $a \in A$ , genera un ben definito  $b \in B$ . Se indichiamo tale “regola” con  $f$ , allora scriviamo la funzione come  $b = f(a)$  invece che  $r(a, b)$ , *dove  $f$  indica la funzione*, e l'unico elemento di  $B$  che è in relazione con  $a \in A$  viene quindi indicato con  $f(a)$ . È importante sottolineare che *non dobbiamo pensare ad una funzione come ad una ricetta di calcolo esplicitamente data*: una *qualunque* relazione che soddisfa le condizioni (4a) e (4b) è una funzione, anche se una formula nel senso tradizionale del termine non è data. *Definire una funzione è una cosa, sapere come calcolarla grazie ad una formula o altro è completamente un altro problema.*

Per scrivere che  $f$  è una funzione dall'insieme  $A$  all'insieme  $B$  si può scrivere nel modo seguente:

$$f : A \mapsto B \quad \text{oppure} \quad A \xrightarrow{f} B.$$

**Esempio 3.** La funzione che fa corrispondere ad ogni numero reale (da definire più avanti!) il suo quadrato è una funzione, perché possiamo calcolare il quadrato di ogni numero e perché il quadrato di un numero è unico.

**Esempio 4.** La “funzione” che fa corrispondere ad ogni numero reale positivo o nullo le sue radici quadrate *non è una funzione*, perché appunto ogni numero positivo ha *due* radici quadrate (viene violata la (4b)).

L'insieme  $A$  viene detto **DOMINIO** della funzione, e si scrive  $A = \text{dom}(f)$ . Si osservi che il dominio è parte integrante della definizione di una funzione!

Il **CODOMINIO** (“range” in inglese) è il sottoinsieme degli elementi di  $B$  che sono in relazione funzionale con qualche elemento di  $A$ , ovvero è l'insieme di tutti gli elementi di  $B$  che possono essere scritti come  $f(a)$  per qualche  $a \in A$ , ovvero è l'insieme dei valori che può assumere  $f$ . Viene indicato con il simbolo  $\text{ran}(f)$ .

Se  $\text{ran}(f) = B$ , cioè se il codominio di  $f$  consiste nell'intero  $B$ , si dice che  $f$  è **SURIETTIVA**. Se inoltre:

$$\forall a_1, a_2 \in A \quad f(a_1) = f(a_2) \Rightarrow a_1 = a_2, \quad (5)$$

cioè se ogni valore di  $f(a)$  può essere ottenuto solo a partire da un unico elemento di  $A$  (leggere la formula precedente: se  $a_1$  e  $a_2$  danno lo stesso valore di  $f$ , allora  $a_1$  e  $a_2$  sono uguali) allora si dice che la  $f$  è **INIETTIVA**. Una funzione  $f$  iniettiva e suriettiva allo stesso tempo viene detta **BIETTIVA** o **CORRISPONDENZA BIUNIVOCA**: fa infatti corrispondere ad ogni elemento di  $A$  un unico elemento di  $B$  e viceversa. Se esiste una corrispondenza biunivoca fra due insiemi allora si dice che i due insiemi sono **EQUIPOTENTI** OVVERO che hanno la medesima **CARDINALITÀ**. È ovvio che due insiemi finiti equipotenti hanno lo stesso numero di elementi (in realtà questa è – quasi! – la definizione di quelli che in teoria degli insiemi si chiamano **NUMERI CARDINALI**; ma noi non ci vogliamo addentrare in simili problematiche).

Data una funzione  $f : A \mapsto B$  ed una funzione  $g : B \mapsto C$ , possiamo definire la **FUNZIONE COMPOSTA**  $h : A \mapsto C$  come segue:

$$\forall a \in A : h(a) = g(f(a)), \quad (6)$$

ovvero la funzione ottenuta applicando ad un elemento di  $A$  prima la funzione  $f$  (ottenendo quindi un elemento di  $B$ ) e poi la funzione  $g$  (ottenendo quindi un elemento di  $C$ ). Si può anche scrivere nel modo seguente:

$$\begin{array}{ccc} & & h \\ & \curvearrowright & \\ A & \xrightarrow{f} & B \xrightarrow{g} C \end{array} \quad (7)$$

oppure:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow h & \downarrow g \\ & & C \end{array} \quad (8)$$

Il significato di questa scrittura è molto semplice: dice che andare da  $A$  a  $C$  mediante la funzione  $h$  è la stessa cosa che andare da  $A$  a  $B$  mediante la funzione  $f$  e poi da  $B$  a  $C$  mediante la funzione  $g$ . Per indicare che  $h$  è composta da  $f$  e  $g$  nel modo indicato (prima applico  $f$ , poi applico  $g$ ) si scrive  $h = g \circ f$ . Si noti che in generale (cioè se gli insiemi  $A, B, C$  sono diversi) non ha senso nemmeno chiedersi se  $f \circ g$  e  $g \circ f$  siano uguali, poiché se è possibile definire l'una non è possibile definire

l'altra. Se gli insiemi  $A$ ,  $B$  e  $C$  sono lo stesso insieme, allora è abbastanza evidente che *non* sono la stessa cosa, e cioè in tal caso la composizione di funzioni non è commutativa.

Dato un insieme qualsiasi  $A$ , è sempre definita una funzione (trivialmente iniettiva e suriettiva!)  $\text{Id}_A : A \mapsto A$  definita da  $\text{Id}_A(a) = a$ , cioè che associa ad ogni elemento di  $A$  se stesso.  $\text{Id}_A$  viene detta FUNZIONE IDENTITÀ dell'insieme  $A$ . Poiché è evidente che ogni insieme ha la sua funzione identità, aggiungiamo al simbolo  $\text{Id}$  un indice che indica l'insieme di riferimento. Nel caso di insiemi numerici ovviamente non ci sarà bisogno di indicare l'insieme di riferimento e scriveremo spesso semplicemente  $\text{Id}$ , qualora non vi sia rischio di ambiguità.

Sia ora  $f : A \mapsto B$  iniettiva. Allora  $\exists g : \text{ran}(f) \subseteq B \mapsto A$  tale che:

$$\forall a \in A : g(f(a)) = a, \quad \forall b \in \text{ran}(f) : f(g(b)) = b, \quad (9)$$

cioè tale che  $g \circ f = \text{Id}_A$ ,  $f \circ g = \text{Id}_{\text{ran}(f)}$ . Infatti, essendo  $f$  iniettiva,  $b$  deriva dall'applicazione della funzione  $f$  ad un unico elemento  $a$  di  $A$ , che viene preso come valore della  $g$  su  $b$ .  $g$  viene detta FUNZIONE INVERSA della  $f$  e si indica con il simbolo  $f^{-1}$ . Se  $f$  è anche suriettiva, allora ancora meglio:  $f$  in tal caso è una corrispondenza biunivoca, che fa corrispondere ad ogni elemento di  $A$  un unico elemento di  $B$  *viceversa*, per cui la funzione inversa è definita su tutto  $B$  e non c'è bisogno di fare riferimento al rango di  $f$ .

Siano ora  $A$  e  $B$  due insiemi totalmente ordinati, ed  $f : A \mapsto B$  una funzione di  $A$  in  $B$ . Diamo le seguenti definizioni:

$x \leq y \Rightarrow f(x) \leq f(y)$	$f$ è CRESCENTE
$x \leq y \Rightarrow f(x) \geq f(y)$	$f$ è DECRESCENTE
$x < y \Rightarrow f(x) < f(y)$	$f$ è STRETTAMENTE CRESCENTE
$x < y \Rightarrow f(x) > f(y)$	$f$ è STRETTAMENTE DECRESCENTE

Nei primi due casi si dice anche che la  $f$  è MONOTÒNA, mentre negli altri due casi si dice che è STRETTAMENTE MONOTÒNA. Ovviamente se una funzione è *strettamente* crescente o *strettamente* decrescente è *a fortiori* crescente o decrescente!

È ovvio (nel senso che il lettore si può convincere della cosa dopo qualche istante di riflessione) che se  $A$ ,  $B$ ,  $C$  sono insiemi totalmente ordinati, allora la composta di due funzioni crescenti è crescente, la composta due funzioni decrescenti è *crescente*, e la composta di una funzione crescente e di una decrescente è decrescente. Se entrambe le funzioni che compongo sono *strettamente* crescenti o decrescenti allora la funzione composta sarà anche lei *strettamente* crescente o decrescente.

Sia infine  $f : A \mapsto B$ ,  $A' \subset A$  un sottoinsieme proprio di  $A$ . Allora possiamo considerare una nuova funzione  $g : A' \mapsto B$  tale che  $\forall a \in A' : g(a) = f(a)$ .  $g$  è detta RESTRIZIONE di  $f$  ad  $A'$  e viene di solito indicata con il simbolo  $f|_{A'}$ . È chiaro che non si tratta di una funzione sostanzialmente "nuova"

rispetto alla  $f$ , ma siccome non manchiamo occasione di ribadire che una funzione è definita anche dal suo dominio, si tratta di una funzione diversa dalla  $f$  e quindi è necessaria una notazione.

In un contesto numerico, ripeteremo tutti i concetti qui introdotti avendo modo di fare moltissimi esempi: l'intero secondo capitolo sarà dedicato sostanzialmente alla discussione delle funzioni di variabili reali.

### 1.3.3. Relazioni di equivalenza

Sia  $A$  un insieme, e  $r(a, b)$  una relazione tra elementi di  $A$ . Si dice che  $r$  è una RELAZIONE DI EQUIVALENZA, che indichiamo con il simbolo  $a \approx b$ , se soddisfa le seguenti proprietà:

$$\forall a \in A : a \approx a \quad (\text{proprietà riflessiva}), \quad (10a)$$

$$\forall a, b \in A : a \approx b \Rightarrow b \approx a \quad (\text{proprietà simmetrica}), \quad (10b)$$

$$\forall a, b, c \in A : a \approx b \wedge b \approx c \Rightarrow a \approx c \quad (\text{proprietà transitiva}). \quad (10c)$$

L'insieme degli elementi  $b$  di  $A$  EQUIVALENTI ad un elemento fissato  $a$  (cioè tali che  $b \approx a$ ) viene detto CLASSE DI EQUIVALENZA di  $a$  ed indicato con il simbolo  $[a]_{\approx}$ . L'indice  $\approx$  apposto sta a ricordarci a quale relazione di equivalenza ci stiamo riferendo: se ciò fosse naturale dal contesto, come in genere avviene, indichiamo la classe di equivalenza di  $a$  semplicemente con  $[a]$ . Se  $a \approx b$  allora  $[a] = [b]$  e viceversa (per la proprietà transitiva!); è altrettanto ovvio che ciascun elemento di  $A$  appartiene a *qualche* classe di equivalenza (la sua!); quindi ciascun elemento di  $A$  appartiene ad una unica classe di equivalenza. Pertanto è ben definito l'insieme delle classi di equivalenza di  $A$  rispetto alla relazione di equivalenza  $\approx$ , detto INSIEME QUOZIENTE di  $A$  rispetto a  $\approx$  ed indicato con il simbolo  $A/\approx$ .

Sia ora  $f : A \mapsto B$  una funzione suriettiva dall'insieme  $A$  all'insieme  $B$ , e  $\sim, \approx$  due relazioni di equivalenza in  $A$  ed in  $B$  rispettivamente. Allora  $f$  è detta COMPATIBILE con le relazioni di equivalenza  $\sim, \approx$  se:

$$\forall a_1, a_2 \in A : a_1 \sim a_2 \Rightarrow f(a_1) \approx f(a_2), \quad (11)$$

cioè se  $f$  manda elementi equivalenti di  $A$  in elementi equivalenti di  $B$ . In tal caso, possiamo definire una nuova funzione  $g : A/\sim \mapsto B/\approx$  ponendo:

$$g([a]) = [f(a)], \quad (12)$$

ovvero  $g$  calcolata sulla classe di equivalenza di  $a$  è pari alla classe di equivalenza di  $f(a)$ . È un semplice esercizio che permette di verificare la comprensione di quanto finora letto verificare che la definizione (12) è ben posta se  $f$  soddisfa (11). Infatti se rappresento la classe  $[a]$  mediante un altro elemento  $a' \in A$  tale che  $a' \sim a$ ,  $f(a') \equiv f(a)$  per cui  $[f(a')] = [f(a)]$  e la proprietà (4b) della definizione di funzione è soddisfatta dalla  $g$ .

Più avanti vedremo parecchi esempi di relazioni di equivalenza utilizzate per definire nuovi oggetti matematici.

## 2. I numeri reali

Gli oggetti fondamentali dell'analisi matematica sono i numeri reali e le loro funzioni. Una introduzione relativamente rigorosa alla costruzione dei numeri reali è essenziale per una comprensione approfondita dell'analisi.

### 2.1. Numeri naturali, interi e razionali

Iniziamo introducendo i numeri piú semplici da “costruire” e da capire, perché “vivono ancora nel mondo del discreto”: i numeri naturali, i numeri interi (relativi) ed i numeri razionali.

#### 2.1.1. Numeri naturali

Gli oggetti fondamentali della matematica sono i numeri naturali, cioè, grossolanamente, i numeri che “si contano con le dita” (ammettendo di avere dita a sufficienza), e che esprimono, per dirla in modo molto approssimato, la molteplicità degli insiemi (“quest’insieme ha tot elementi”) o la posizione all’interno di una relazione d’ordine totale (“il primo, secondo, etc. di una fila”).

I numeri naturali possono essere “costruiti” a partire dagli assiomi della teoria degli insiemi, oppure possono essere presi come oggetti primitivi, definiti da un loro sistema di assiomi (sostanzialmente dovuto al matematico italiano Giuseppe Peano, 1858-1932). Di nuovo, non ci addentriamo nei meandri dei fondamenti della matematica e consideriamo il concetto di numero naturale  $(0, 1, 2, \dots)$  come elementare e ben noto.

L’insieme di tutti i numeri naturali viene indicato con il simbolo  $\mathbb{N}$ . L’insieme dei numeri naturali è totalmente ordinato dalla relazione d’ordine  $\leq$ . Le operazioni elementari (somma, moltiplicazione e loro operazioni inverse – sottrazione e divisione –, così come le potenze di esponente intero) sono ben note.

Un insieme infinito che può essere messo in corrispondenza biunivoca con l’insieme dei numeri interi viene detto NUMERABILE. Lavorare con insiemi infiniti è sempre una cosa delicata, e quindi l’idea intuitiva che due insiemi in corrispondenza biunivoca hanno lo stesso numero di elementi viene messa in questione nel caso di insiemi infiniti. Ad es. l’insieme dei numeri pari è un sottoinsieme *proprio* dei numeri naturali, per cui intuitivamente “piú piccolo”, ma può cionondimeno essere messo in corrispondenza biunivoca con l’insieme dei naturali in modo estremamente semplice: ad es. ad  $n$  pari facciamo corrispondere l’intero  $n/2$  (che esiste perché  $n$  è pari!), e all’intero  $m$  facciamo corrispondere il pari  $2m$ ; che si tratti di una corrispondenza biunivoca è immediato. Esistono insiemi infiniti che non possono essere messi in corrispondenza biunivoca con i naturali, e quindi che non sono numerabili? La risposta a questa domanda è affermativa: vedremo piú avanti che l’insieme dei *numeri reali* non è infatti numerabile, ma ha una cardinalità maggiore (contiene cioè “molti piú elementi” di  $\mathbb{N}$ ).

L'unico punto importante da sottolineare parlando dei numeri interi è il seguente principio logico, in cui la successione degli interi ha un ruolo essenziale e che è molto usato in matematica: il PRINCIPIO DI INDUZIONE MATEMATICA.

**Proposizione 4.** *Sia  $A$  un insieme. Se:*

$$0 \in A \tag{13a}$$

$$\forall n \in \mathbb{N} : n \in A \Rightarrow n + 1 \in A \tag{13b}$$

allora  $A \supseteq \mathbb{N}$ .

*Dimostrazione.* Supponiamo che  $m \in \mathbb{N}$ ,  $m \notin A$ . Allora deve essere anche  $m - 1 \notin A$ , e quindi anche  $m - 2 \notin A$ , e così via; dopo  $m$  passi, arriviamo a  $0 \notin A$ , contraddicendo (13a). Quindi deve essere  $m \in A$ .  $\square$

Il principio di induzione matematica è tipicamente utilizzato come tecnica di dimostrazione, quando bisogna dimostrare che una certa proposizione  $P_n$ , che dipende da  $n \in \mathbb{N}$ , è vera  $\forall \mathbb{N}$ . In tal caso si può dimostrare che  $P_n$  vale per ogni  $n \in \mathbb{N}$  semplicemente dimostrando che vale  $P_0$  e poi che  $\forall n \in \mathbb{N} P_n \Rightarrow P_{n+1}$ . Infatti, basta definire  $A$  come l'insieme degli  $\mathbb{N}$  per cui  $P_n$  è vera ed applicare il principio di induzione per ottenere che  $A = \mathbb{N}$ , cioè  $P_n$  è sempre vera.

La tecnica di dimostrazione per induzione è molto importante e nel seguito la utilizzeremo molto spesso. Una delle prime applicazioni sarà la dimostrazione della formula del binomio di Newton, nel prossimo capitolo.

### 2.1.2. Numeri interi

Per “numeri interi” si intendono i numeri interi dotati di segno. Di nuovo, le loro proprietà sono ben note fin dalle scuole inferiori. L'insieme dei numeri interi viene indicato con il simbolo  $\mathbb{Z}$  (dal tedesco *Zahl*, numero).

Ricordiamo la definizione di VALORE ASSOLUTO O MODULO di  $n$ , indicato con il simbolo  $|n|$ , come il più grande fra  $n$  e  $-n$ :

$$|n| = \max\{n, -n\}. \tag{14}$$

Diamo per scontate le proprietà del valore assoluto, tra cui importantissime la DISUGUAGLIANZA TRIANGOLARE:

$$|n + m| \leq |n| + |m|, \tag{15}$$

e l'altra:

$$|n| = 0 \Rightarrow n = 0. \tag{16}$$

Diamo anche per scontate le nozioni di DIVISORE, di MASSIMO COMUN DIVISORE (indicato con  $\text{gcd}$ ), di MINIMO COMUNE MULTIPLO, di NUMERO PRIMO e di SCOMPOSIZIONE DI UN INTERO IN FATTORI PRIMI.

È abbastanza facile, anche se molto noioso, costruire i numeri interi a partire dai numeri naturali come classi di equivalenza di coppie di numeri naturali.

Consideriamo l'insieme  $\mathbb{N}^2$  delle coppie ordinate  $(n, m)$  di numeri naturali. In tale insieme introduciamo una relazione di equivalenza  $\sim$  nel modo seguente:

$$(n, m) \sim (p, q) \quad \text{se} \quad n + q = m + p. \quad (17)$$

Tale relazione di equivalenza non è scelta a caso; infatti due coppie sono equivalenti se la differenza tra  $n$  e  $m$  è uguale: il problema è che se  $n < m$  la differenza negli interi non ha senso. Quindi sostanzialmente identifichiamo i numeri negativi con l'insieme di tutte le possibili sottrazioni che generano il numero negativo considerato.

È un esercizio banale e noioso verificare che effettivamente le proprietà riflessiva, simmetrica e transitiva sono soddisfatte. Quindi definiamo  $\mathbb{Z}$  come il quoziente  $\mathbb{N}/\sim$ . Definiamo poi somma e moltiplicazione come:

$$\begin{aligned} (n, m) + (p, q) &= (n + p, m + q), \\ (n, m) \cdot (p, q) &= (np + mq, mp + nq). \end{aligned}$$

Definiamo inoltre l'operazione "cambio di segno" ponendo  $-(n, m) = (m, n)$ . Tali operazioni sono compatibili con la relazione di equivalenza  $\sim$  e quindi definiscono operazioni sulle classi di equivalenza (cioè su  $\mathbb{Z}$ ). A questo punto *identifichiamo  $\mathbb{N}$  con le classi della forma  $[(n, 0)]$  (INTERI POSITIVI)*, ed indichiamo le classi della forma  $[(0, n)]$  con  $-n$  (INTERI NEGATIVI). La relazione d'ordine totale  $\leq$  viene definita in  $\mathbb{Z}$  distinguendo i segni: se  $n, m$  sono positivi, li interpretiamo come numeri naturali e definiamo la relazione d'ordine nel modo usuale; se uno è negativo e l'altro positivo, allora il positivo è sempre maggiore del negativo, e se entrambe sono negativi, poniamo  $n \leq m$  se  $-m \leq -n$  ( $-m, -n$  sono positivi!). Infine, definiamo  $|n|$  (MODULO O VALORE ASSOLUTO di  $n$ ) come il più grande tra  $n$  e  $-n$ . È noioso ma elementare verificare che queste definizioni sono scelte esattamente in modo tale da generare le note proprietà di quelli che sono noti alle scuole inferiori come *numeri relativi*.

L'insieme dei numeri interi è numerabile. Ecco una corrispondenza biunivoca fra interi e naturali:

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

Anche se non abbiamo scritto esplicitamente la formula l'idea dovrebbe essere chiara.

### 2.1.3. Numeri razionali

La definizione elementare di numero razionale è quella di frazione i cui numeratori e denominatori sono numeri interi (il denominatore diverso da 0!), ed avendo identificato le frazioni simili. L'insieme dei numeri razionali viene indicato con il simbolo  $\mathbb{Q}$  (da "quoziente").

Le operazioni, la relazione d'ordine  $\leq$  ed il valore assoluto sono definiti nel modo naturale e noto fin dalle scuole inferiori. È importante sottolineare che le proprietà del valore assoluto, che verranno utilizzate pesantemente in tutto il corso, continuano naturalmente a valere per i numeri razionali.

I numeri razionali possono essere costruiti molto facilmente a partire dagli interi usando il linguaggio delle classi di equivalenza, semplicemente formulando in tale linguaggio la teoria delle frazioni. Infatti, è immediato verificare che l'insieme delle frazioni è l'insieme  $\mathbb{Z} \times \mathbb{Z}^*$ , dove con  $\mathbb{Z}^*$  indichiamo l'insieme degli interi diversi da 0 (il denominatore non può essere 0!), e che la relazione di similitudine fra frazioni è una relazione di equivalenza.

I numeri razionali godono di due importanti proprietà.

**Proposizione 5** (Densità dei numeri razionali). *Dati due razionali distinti esiste sempre un razionale compreso fra i due:*

$$\forall x, y \in \mathbb{Q}, x < y, \exists z \in \mathbb{Q} : x < z < y. \quad (18)$$

*Dimostrazione.* Basta prendere:

$$z = \frac{x+y}{2};$$

ovviamente  $z$  è compreso fra  $x$  e  $y$  (ne è la media!) ed è razionale.  $\square$

Conseguentemente ne esistono infiniti: infatti avremo  $z_1$  fra  $x$  e  $y$ ,  $z_2$  tra  $x$  e  $z_1$ ,  $z_3$  tra  $x$  e  $z_2$ , e così via.

**Proposizione 6** (Proprietà archimedeica dei numeri razionali).

$$\forall x, y > 0, x, y \in \mathbb{Q}, \exists n \in \mathbb{N} \text{ tale che } nx > y. \quad (19)$$

*Dimostrazione.* Sia  $x = p/q, y = r/s, p, q, r, s > 0$  interi. Allora basta prendere  $n > rq$ :

$$nx > rq \frac{p}{q} = rp > \frac{r}{s}.$$

$\square$

In particolare, preso qualsiasi razionale, *arbitrariamente piccolo*, possiamo sempre moltiplicarlo per un intero in modo tale che il risultato sia ad es. maggiore di 1, di 0.1, di 0.0000001 o di 100000000.

L'insieme dei numeri razionali è numerabile. Un modo per NUMERARE (cioè mettere corrispondenza biunivoca con i naturali)  $\mathbb{Q}$  è il seguente. Per ogni razionale  $r$ , scritto come frazione ridotta ai minimi termini con denominatore positivo nella forma  $p/q$ , chiamiamo "altezza" di  $r$  l'intero  $|p| + q$ . Ad es. non esistono numeri di altezza 0, l'unico numero di altezza 1 è  $0 = 0/1$ , i numeri di altezza 2 sono  $-1 = -1/1$  e  $1 = 1/1$ , e così via; per ogni valore dell'altezza c'è un numero *finito* di razionali. Possiamo quindi numerare i razionali disponendoli prima in ordine di altezza, e all'interno di quelli della medesima altezza li ordiniamo in modo crescente. Ad es.:

$ p  + q$	1	2	3		4				...			
$p/q \in \mathbb{Q}$	0/1	-1/1	1/1	-2/1	-1/2	1/2	2/1	-3/1	-1/3	1/3	3/1	...
$m \in \mathbb{N}$	0	1	2	3	4	5	6	7	8	9	10	...

**Esercizio 1.** Rappresentare le frazioni  $\frac{p}{q}$  geometricamente come punti di  $\mathbb{Z}^2$ , utilizzando  $p$  e  $q$  come coordinate (ovviamente rimuovendo il semipiano  $q \leq 0$ !), ed evidenziare le frazioni che hanno la medesima “altezza”.

È evidente che esistono molti altri modi, alcuni geometricamente intuitivi, per realizzare la corrispondenza biunivoca fra naturali ed interi.

## 2.2. Numeri reali

Si potrebbe pensare che i numeri razionali siano sufficienti per gli usi che se ne devono fare in geometria ed in fisica. In realtà non è così, come è noto sostanzialmente da Pitagora (569 a. C.-475 a. C.). Infatti, consideriamo un quadrato di lato 1, e calcoliamone la diagonale. Utilizzando, appunto, il teorema di Pitagora, otteniamo che la diagonale  $d$  del quadrato soddisfa  $d^2 = 1^2 + 1^2 = 2$ . Il problema è che non esiste alcun numero razionale il cui quadrato è 2.

Infatti, sia  $p/q \in \mathbb{Q}$  tale che  $p^2/q^2 = 2$ . Allora deve essere  $p^2 = 2q^2$ . In realtà ciò è impossibile; se infatti scomponiamo sia  $p$  che  $q$  in fattori primi, ciascuno di essi avrà un certo numero di fattori 2 nella scomposizione in fattori primi; pertanto  $p^2$ , essendo un quadrato, avrà un numero pari di fattori 2, ed analogamente  $q^2$ . Ma allora  $2q^2$  ha un numero dispari di fattori due (quelli di  $q^2$  più uno!) e quindi non può essere uguale a  $p^2$ .

La costruzione dei numeri reali è piuttosto complessa, ed esistono diverse varianti. La costruzione più famosa, storicamente la prima e concettualmente la più chiara, è quella dovuta al matematico tedesco Richard Dedekind (1831-1916). Nel seguito introdurremo i numeri reali nel modo in cui sono definiti alle scuole inferiori, e cioè come sviluppi decimali non periodici, e descriveremo la costruzione di Dedekind in dettaglio come complemento: tale costruzione ci permetterà di dimostrare che una proprietà dei numeri reali, essenziale per l'analisi matematica, effettivamente vale.

Assumendo nota la notazione posizionale per i numeri razionali (nel seguito useremo quasi esclusivamente quella in base 10, o notazione decimale) assumiamo come note ed elementari le seguenti proprietà:

1. Se  $r = p/q \in \mathbb{Q}$ , allora  $r$  è rappresentato in forma decimale come segue:

$$\pm a_m a_{m-1} \dots a_1 a_0 . b_1 \dots b_k (c_1 \dots c_n), \quad (20)$$

dove  $a_i, b_i$  e  $c_i$  sono cifre decimali (cioè interi compresi fra 0 e 9), e le parentesi intorno agli  $c_i$  indicano che la quella successione di cifre si ripete infinitamente. Se gli  $a_i$  non ci sono vuol dire

che LA PARTE INTERA del numero decimale è nulla; gli  $b_i$  formano il cosiddetto ANTIPERODO, che può non esserci (poniamo in tal caso  $k = 0$ ), e la sequenza periodica degli  $c_i$ , che può anche lei non esserci ( $n = 0$ ), è il PERIODO.

2. Viceversa, uno sviluppo decimale della forma (20) definisce un unico numero razionale  $r$  (che più avanti impareremo a calcolare).

È importante osservare che ogni numero decimale non periodico può essere sempre scritto come periodico, con un periodo che consiste nella singola cifra 9: ad es.  $1 = 0.(9)$ , o  $0.37 = 0.36(9)$ . Per eliminare tale ambiguità, imponremo che i numeri con periodo costituito dalla singola cifra 9 siano immediatamente riscritti come numeri decimali non periodici.

I numeri decimali che non rientrano nella categoria precedente, e cioè i numeri decimali che non terminano e la cui infinita sequenza di cifre *non è periodica* vengono detti NUMERI IRRAZIONALI. I NUMERI REALI, il cui insieme viene denotato con il simbolo  $\mathbb{R}$ , sono i numeri razionali e i numeri irrazionali. Le operazioni sono definite su di essi nel modo noto fin dalle scuole inferiori, così come la relazione d'ordine totale  $\leq$ . Definiamo quindi il modulo di un numero reale nel modo solito:

$$|x| = \max\{x, -x\};$$

continuano a valere le proprietà  $|x + y| \leq |x| + |y|$ , detta DISUGUAGLIANZA TRIANGOLARE, e  $|x| = 0 \Rightarrow x = 0$ .

I numeri reali godono della importante PROPRIETÀ DI COMPLETEZZA O PROPRIETÀ DI DEDEKIND, che i numeri razionali *non possiedono*:

**Teorema 1.** *Sia  $A \subset \mathbb{R}$ , limitato superiormente. Allora esiste  $a = \sup A$ .*

Questa proprietà è palesemente falsa per i numeri razionali. Ad es. l'insieme:

$$A = \{x \in \mathbb{Q} : x^2 \leq 2\}$$

non possiede, in  $\mathbb{Q}$ , alcun estremo superiore (altrimenti la radice quadrata di 2 sarebbe razionale, il che non è!).

### 2.2.1. La costruzione di Dedekind

Sia  $(L, R)$  una partizione di  $\mathbb{Q}$  in due insiemi tali che:

$$L \cup R = \mathbb{Q}, \tag{21a}$$

$$\forall x \in L, y \in R : x < y. \tag{21b}$$

La coppia  $(L, R)$  viene detta COPPIA DI CLASSI CONTIGUE di numeri razionali o TAGLIO di  $\mathbb{Q}$ .

Per chiarire il concetto di taglio, facciamo qualche esempio notevole.

**Esempio 5.**  $L = \{x \in \mathbb{Q} : x < 0\}$  e  $R = \{x \in \mathbb{Q} : x > 0\}$  non è un taglio, perché la condizione (21a) non è soddisfatta (0 non è incluso né in  $L$  né in  $R$ ).

**Esempio 6.**  $L = \{x \in \mathbb{Q} : x \geq 0\}$  e  $R = \{x \in \mathbb{Q} : x < 0\}$  non è un taglio, perché la condizione (21b) non è soddisfatta (i numeri in  $L$  sono maggiori dei numeri in  $R$ ).

**Esempio 7.**  $L = \{x \in \mathbb{Q} : x \leq 0\}$  e  $R = \{x \in \mathbb{Q} : x \geq 0\}$  non è un taglio, perché la condizione (21b) non è soddisfatta (0 appartiene ad entrambe gli insiemi!).

**Esempio 8.**  $L = \{x \in \mathbb{Q} : x < 0\}$  e  $R = \{x \in \mathbb{Q} : x \geq 0\}$  è un taglio.

**Esempio 9.**  $L = \{x \in \mathbb{Q} : x \leq 1\}$  e  $R = \{x \in \mathbb{Q} : x > 1\}$  è un taglio.

**Esempio 10.**  $L = \{x \in \mathbb{Q} : x \leq 0 \text{ oppure } x^2 < 2\}$  e  $R = \{x \in \mathbb{Q} : x^2 \geq 2 \text{ e } x > 0\}$  è un taglio.

$L$  viene detta CLASSE SINISTRA e  $R$  viene detta CLASSE DESTRA (infatti, se rappresentiamo i razionali come punti su una retta orientata verso destra come d'abitudine, i numeri in  $L$  stanno a sinistra di quelli in  $R$ ). La coppia o taglio  $(L, R)$  viene detta coppia di classi *contigue* per la seguente ragione.

**Proposizione 7.**  $\forall \varepsilon > 0 \exists x \in L, y \in R : y - x < \varepsilon$  (in altri termini, esistono in  $L$  e  $R$  razionali arbitrariamente vicini fra loro).

*Dimostrazione.* Supponiamo che la proposizione sia falsa. Allora:

$$\exists \varepsilon > 0 \forall x \in L, y \in R : y - x \geq \varepsilon. \quad (22)$$

Siano allora  $\bar{x} \in L, \bar{y} \in R$  qualsiasi. Per la proprietà di densità dei razionali  $\exists N \in \mathbb{N}$  tale che:

$$\delta = \frac{\bar{y} - \bar{x}}{N} < \varepsilon.$$

Consideriamo gli  $N + 1$  razionali:

$$x_0 = \bar{x}, x_1 = \bar{x} + \delta, x_2 = \bar{x} + 2\delta, \dots, x_N = \bar{x} + N\delta = \bar{y}.$$

Per definizione di classi contigue, essi devono tutti appartenere a  $L$  o a  $R$ , anzi, per l'esattezza, i primi – diciamo fino a che l'indice è minore o uguale a  $k$  – devono appartenere a  $L$ , e gli altri – quindi quelli con indice che è maggiore di  $k$  – devono appartenere ad  $R$ . Ora,  $x_k \in L$ , e  $x_{k+1} \in R$ , ma la loro differenza è  $\delta < \varepsilon$ , che contraddice la (22). La (22) non può quindi essere vera (perché implica una contraddizione!) per cui deve essere vera la tesi.  $\square$

Si osservi che  $L$  è limitato superiormente (da qualsiasi numero in  $R$ ) e che  $R$  è limitato inferiormente (da qualsiasi numero in  $L$ ). Potrebbero avere massimo o minimo. Sono infatti possibili tre tipi di tagli: (1)  $L$  ha massimo e  $R$  non ha minimo (ad es. l'esempio 9), (2)  $L$  non ha massimo e  $R$  ha minimo (ad es. l'esempio 8), (3)  $L$  non ha massimo e  $R$  non ha minimo (ad es. l'esempio 10). Il quarto caso che potrebbe teoricamente essere dato ( $L$  ha massimo e  $R$  ha minimo) non è in realtà possibile. Sia infatti  $l = \max L$  e  $r = \min R$ ;  $l$  e  $r$  sono razionali (essendo massimi e minimi fanno parte dei rispettivi insiemi: ed in ogni caso null'altro che i razionali v'è al momento!). Ma allora  $(l + r)/2$  sarebbe razionale, maggiore di  $l$  e minore di  $r$  (essendone la media!), quindi non sarebbe contenuto né in  $L$  né in  $R$ , contraddicendo la definizione di taglio.

Ovviamente, tutte le classi del tipo (1) sono della forma:

$$L' = \{x \leq r\}, R' = \{x > r\} \quad \text{per qualche } r \in \mathbb{Q},$$

mentre tutte quelle del tipo (2) sono della forma:

$$L'' = \{x < r\}, R'' = \{x \geq r\} \quad \text{per qualche } r \in \mathbb{Q}.$$

Quindi se consideriamo equivalenti le coppie  $(L', R')$ ,  $(L'', R'')$  definite come sopra, l'insieme dei tagli di tipo (1), (2) è in corrispondenza biunivoca con  $\mathbb{Q}$ , perché ad ogni razionale  $r$  corrispondono esattamente due tagli, uno di tipo (1) ed uno di tipo (2). Noi pertanto identifichiamo con  $\mathbb{Q}$  l'insieme dei tagli di tipo (1), (2), avendo avuto cura di identificare le coppie equivalenti. A questo punto estendiamo  $\mathbb{Q}$  aggiungendo le coppie di classi del tipo (3), che palesemente non corrispondono a nessun numero razionale. Una classe di tipo (3) definirà un NUMERO IRRAZIONALE  $\alpha$ .

L'insieme di tutti i numeri razionali ed irrazionali (cioè di tutti i tagli, avendo avuto cura di identificare i tagli corrispondenti di tipo (1) e (2)) è l'insieme dei NUMERI REALI, denotato con il simbolo  $\mathbb{R}$ .

Nonostante le apparenze, si tratta di una definizione intuitiva: infatti un numero irrazionale non può mai essere enunciato nella sua interezza, con precisione assoluta, perché occorrerebbe dare un numero infinito di cifre (mentre un numero razionale ha uno sviluppo decimale periodico o addirittura finito). Quindi dobbiamo immaginare che, "in pratica", una quantità reale (CONTINUA) sia determinata da un susseguirsi di approssimazioni per difetto e per eccesso, viepiù precise, che la determinano approssimandola dall'alto e dal basso.

È facile mostrare come  $\mathbb{R}$  sia un insieme totalmente ordinato. Infatti, diremo che due numeri reali  $\alpha, \beta$  diversi tra loro sono in relazione  $\alpha < \beta$  se le classi corrispondenti  $(L_\alpha, R_\alpha), (L_\beta, R_\beta)$  soddisfano:

$$L_\alpha \subset L_\beta, \quad R_\alpha \supset R_\beta.$$

È necessario escludere  $\alpha = \beta$  perché allora, nel caso in cui entrambe siano razionali, sorgerebbe qualche problema se rappresentiamo  $\alpha$  con una classe del tipo (2) e  $\beta$  con una classe di tipo (1). Ovviamente  $\alpha \leq \beta$  se  $\alpha < \beta$  o  $\alpha = \beta$ .

Definiamo ora le operazioni elementari sui numeri reali. Abbiamo innanzitutto:

$$\alpha + \beta = \gamma = (L_\gamma, R_\gamma),$$

dove:

$$L_\gamma = \{x + y, x \in L_\alpha, y \in L_\beta\}, \quad R_\gamma = \{x + y, x \in R_\alpha, y \in R_\beta\}.$$

È banale verificare che  $(L_\gamma, R_\gamma)$  è un taglio, e che nel caso in cui  $\alpha$  e  $\beta$  siano razionali il risultato corrisponde al razionale somma di  $\alpha$  e  $\beta$ , e cioè che tale definizione estende senza contraddire la definizione di somma tra razionali ai reali. L'OPPOSTO  $-\alpha$  è definito dalle classi:

$$L_{-\alpha} = \{-x, x \in R_\alpha\}, \quad R_{-\alpha} = \{-x, x \in L_\alpha\},$$

e  $\alpha - \beta = \alpha + (-\beta)$ . E poi, naturalmente, definiamo  $|\alpha| = \max(\alpha, -\alpha)$ .

La definizione di moltiplicazione è più macchinosa a causa dei segni. Definiamola prima per i numeri positivi (per cui, dunque, la classe inferiore  $L_\alpha$  contiene tutti i numeri negativi). Se  $\alpha \geq 0, \beta \geq 0$  (cosicché

$L_\alpha \supseteq \{x \in \mathbb{Q}, x \leq 0\}$ ,  $R_\alpha \subseteq \{x \in \mathbb{Q}, x \geq 0\}$  ed analogamente per  $\beta$ ), definiamo il prodotto  $\alpha \cdot \beta$  o brevemente  $\alpha\beta$  mediante le due classi:

$$R_{\alpha\beta} = \{x \cdot y, x \in R_\alpha, y \in R_\beta\}, L_{\alpha\beta} = \{x \cdot y, x \in L_\alpha, y \in L_\alpha, e x, y > 0\} \cup \{x \in \mathbb{Q}, x \leq 0\}.$$

È opportuno fermarsi un attimo a riflettere per convincersi che le due classi formano effettivamente un taglio, e che tale definizione estende senza contraddire la nozione di prodotto fra razionali ai reali; è necessario costruire la classe sinistra in quel modo apparentemente macchinoso perché, se fosse definita semplicemente in analogia con la definizione della classe destra, non otterremo un taglio: infatti il prodotto di due grandi numeri *negativi* nelle classi sinistre di  $\alpha$  e  $\beta$  darebbe un grande numero *positivo* e quindi “fuori posto” nella classe sinistra del prodotto.

Se  $\alpha, \beta$  sono positivi definiamo poi:

$$(-\alpha)\beta = -\alpha\beta, \alpha(-\beta) = -\alpha\beta, (-\alpha)(-\beta) = \alpha\beta.$$

Se  $\alpha > 0$ , definiamo  $\frac{1}{\alpha}$  tramite le classi:

$$R_{1/\alpha} = \left\{x \in \mathbb{Q}, \frac{1}{x} \in L_\alpha, e x > 0\right\}, L_{1/\alpha} = \left\{x \in \mathbb{Q}, \frac{1}{\alpha} \in R_\alpha\right\} \cup \{x \in \mathbb{Q}, x \leq 0\},$$

e poniamo  $1/(-\alpha) = -(1/\alpha)$ . Definiamo quindi  $\alpha/\beta$ , con  $\beta \neq 0$ , come  $\alpha \cdot (1/\beta)$ .

È facile, anche se *piuttosto laborioso*, dimostrare che le operazioni così definite sui reali estendano senza contraddire le nozioni delle analoghe operazioni sui razionali, e che le note proprietà delle operazioni elementari effettivamente valgono sui reali.

Accingiamoci ora a dimostrare il teorema di completezza 1. Per farlo, consideriamo *coppie di classi contigue di numeri reali* o *tagli* dell'insieme  $\mathbb{R}$  dei numeri reali, invece che razionali. La definizione è identica al caso dei razionali, e cioè diremo che  $(L, R)$  è un TAGLIO DEI REALI se  $L \cup R = \mathbb{R}$  e se  $\forall x \in L, \forall y \in R$  vale  $y > x$ . In modo del tutto analogo al caso razionale, si dimostra che  $\forall \varepsilon > 0 \exists x \in L, \exists y \in R$  tali che  $y - x < \varepsilon$ . Vale allora il seguente teorema.

**Teorema 2** (Dedekind). *Se  $(L, R)$  è un taglio dei reali, allora  $\exists \alpha \in \mathbb{R}$  tale che  $L$  contiene tutti i reali minori di  $\alpha$ ,  $R$  contiene tutti i reali maggiori di  $\alpha$  e  $\alpha$  appartiene o a  $L$  o a  $R$ .*

*Dimostrazione.* Come nel caso dei numeri razionali, sono possibili in linea di principio 4 casi: (1)  $L$  ha massimo  $l$  e  $R$  ha minimo  $r$ , (2)  $L$  ha massimo  $l$  e  $R$  non ha minimo, (3)  $L$  non ha massimo e  $R$  ha minimo  $r$ , (4)  $L$  non ha massimo e  $R$  non ha minimo. Ora, il caso (1) non è possibile: se fosse vero allora  $l < (l+r)/2 < r$  ed  $(l+r)/2$  non apparterebbe allora né a  $L$  né a  $R$ , come nel caso dei tagli dei razionali. Ma, a differenza del caso dei tagli dei razionali, *ora nemmeno il caso (4) è possibile!*. Infatti, se tale caso è possibile, poniamo  $L' = L \cap \mathbb{Q}$ ,  $R' = R \cap \mathbb{Q}$ . Ovviamente  $(L', R')$  è *taglio dei razionali* e quindi definisce un numero reale  $\beta$ .  $\beta$  deve appartenere a  $L$  o a  $R$ ; se appartiene a  $L$ , allora deve essere il massimo di  $L$  (altrimenti detto  $\beta'$  un elemento di  $L$  maggiore di  $\beta$ , fra  $\beta$  e  $\beta'$  c'è almeno un razionale  $\beta'' \in L'$  maggiore di  $\beta$  e quindi in  $R$  ed essendo razionale anche in  $R'$ , il che contraddice il fatto che  $(L', R')$  è un taglio dei razionali); se appartiene a  $R$  allora deve necessariamente esserne il minimo (per un ragionamento analogo al precedente). Quindi il caso (4) non può essere dato.

A questo punto il teorema di Dedekind è dimostrato perché nel caso (2)  $\alpha = l$  mentre nel caso (3)  $\alpha = r$ , e non sono possibili altri casi. □

*Dimostrazione del teorema di completezza.* Sia  $A \subset \mathbb{R}$  limitato superiormente. Consideriamo i due insiemi:

$$R = \{\text{insieme dei maggioranti di } A\}, \quad L = \mathbb{R} \setminus R.$$

È evidente che  $(L, R)$  è un taglio dei reali. Essa definisce pertanto un numero reale  $\alpha$  per il teorema di Dedekind. Dimostriamo ora che  $\alpha = \sup A$ .

Se  $\alpha > \sup A$ , esisterebbe un maggiorante di  $A$  in  $L$  il che è assurdo. Se  $\alpha < \sup A$ , esisterebbe in  $R$  un reale che non è maggiorante di  $A$ , il che contraddice la definizione di  $R$ . Quindi non può che essere  $\alpha = \sup A$ .  $\square$

Osserviamo a questo punto che le operazioni sui numeri reali possono essere interpretate come operazioni sui tagli dei reali allo stesso modo in cui sono state definite sui tagli dei razionali.

L'insieme dei reali viene anche detto CONTINUO. Il concetto di numero reale è centrale nell'analisi, e con esso quello di continuità.

### 2.2.2. Ulteriori proprietà dei numeri reali

Anche se che  $\mathbb{R}$  è formato da infiniti elementi come  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ , si tratta di un infinito di "ordine" più elevato: si dice che  $\mathbb{R}$  non è numerabile. Per l'esattezza, dimostriamo che non è possibile mettere in corrispondenza biunivoca l'insieme dei reali compresi tra 0 e 1 ed i numeri naturali.

Ammettiamo infatti che sia possibile. Potremmo allora numerare i reali fra 0 e 1 nel modo seguente:

1	$0.a_1^{(1)}a_2^{(1)}a_3^{(1)}a_4^{(1)}\dots$
2	$0.a_1^{(2)}a_2^{(2)}a_3^{(2)}a_4^{(2)}\dots$
3	$0.a_1^{(3)}a_2^{(3)}a_3^{(3)}a_4^{(3)}\dots$
4	$0.a_1^{(4)}a_2^{(4)}a_3^{(4)}a_4^{(4)}\dots$
...	...

dove le  $a_j^{(i)}$  è la  $j$ -esima cifra decimale del  $i$ -esimo numero reale nella lista. Un numero reale non compreso nella lista è allora quello il cui sviluppo decimale è:

$$\beta = 0.b_1b_2b_3b_4\dots,$$

dove le cifre decimali  $b_i$  soddisfano  $b_i \neq a_i^{(i)}$  (scelta che è sempre possibile fare, avendo cura di scegliere  $b_i \neq 9$  e i numeri nella lista scritti in modo "normale", senza cifre 9 periodiche). Ci si soffermi un attimo a riflettere che effettivamente  $\beta$  non appare nella lista; se apparisse, sarebbe il primo, o il secondo, o il terzo, etc.: ma le cifre di  $\beta$  sono scelte appunto in modo da evitare che possa essere il primo (perché la prima cifra differisce), il secondo (perché la seconda cifra differisce), il terzo (perché la terza cifra differisce), e così via. L'idea della dimostrazione, dovuta al matematico tedesco Georg Cantor (1845-1918), è detta *metodo diagonale*.

Un numero reale che è radice di una equazione algebrica a coefficienti razionali viene detto **ALGEBRICO**: ad es. tutti i razionali sono algebrici,  $\sqrt{2}$  è algebrico,  $(\sqrt{5} - 1)/2$  è algebrico così come qualsiasi espressione costruita mediante operazioni elementari a partire da radici quadrate o in generale  $n$ -esime, e la radice di  $x^5 + x - 1 = 0$  è un numero algebrico anche se non è possibile scriverla in termini di radici ed operazioni elementari.

Un numero reale che non è algebrico viene detto **TRASCENDENTE**. Ad es. è noto che il numero  $\pi$ , pari al rapporto tra l'area del cerchio ed il quadrato del suo raggio, è trascendente. In generale, le dimostrazioni della trascendenza di un numero irrazionale sono difficili.

### 2.2.3. Intervalli di numeri reali

Poiché  $\mathbb{R}$  è totalmente ordinato, possiamo definire gli **INTERVALLI** come segue:

$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$	intervallo CHIUSO
$(a, b) = \{x \in \mathbb{R} : a < x < b\}$	intervallo APERTO
$[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$	intervallo CHIUSO A SINISTRA E APERTO A DESTRA
$(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$	intervallo CHIUSO A DESTRA E APERTO A SINISTRA
$[a, +\infty) = \{x \in \mathbb{R} : x \geq a\}$	intervallo CHIUSO A SINISTRA E INFINITO A DESTRA
$(-\infty, a] = \{x \in \mathbb{R} : x \leq a\}$	intervallo CHIUSO A INFINITO A SINISTRA
$(a, +\infty) = \{x \in \mathbb{R} : x > a\}$	intervallo APERTO A SINISTRA E INFINITO A DESTRA
$(-\infty, a) = \{x \in \mathbb{R} : x < a\}$	intervallo APERTO A DESTRA E INFINITO A SINISTRA

Si osservi che  $+\infty$  e  $-\infty$  non sono numeri ma sono solo dei simboli che caratterizzano l'illimitatezza dell'intervallo in questione. In pratica, la parentesi quadra indica l'inclusione dell'estremo nell'intervallo e la parentesi tonda la sua esclusione; non essendo numeri,  $\pm\infty$  sono sempre esclusi.

## 2.3. Potenze, radici, e logaritmi

Definiamo ora per i numeri reali alcune operazioni particolarmente importanti, e cioè le potenze e i loro inversi: le radici ed i logaritmi. Si tratta di nozioni ben note dalle scuole inferiori ma è il caso di rivisitarle dal punto di vista rigoroso che abbiamo cercato, fin dove possibile, di adottare.

### 2.3.1. Potenze e radici

Definiamo ora le potenze dei numeri reali.

Sia  $a \in \mathbb{R}$ ,  $n \in \mathbb{N}$ ; allora:

$$a^n = \underbrace{a \cdot \dots \cdot a}_{n \text{ volte}}. \quad (23)$$

Si definisce inoltre  $a^0 = 1$ . Se  $m \in \mathbb{Z}$  ed  $m < 0$ , allora si definisce:

$$a^m = \frac{1}{a^{-m}} \quad (24)$$

(si osservi che se  $m < 0$  allora  $-m > 0$  quindi  $-m \in \mathbb{N}$ !).

La RADICE  $q$ -ESIMA  $\sqrt[q]{a}$ ,  $q \in \mathbb{Z}$ , è definita come l'operazione inversa dell'elevamento a potenza  $q$ -esima, per  $a \geq 0$ .

Per definire effettivamente la radice  $q$ -esima ( $q \in \mathbb{N}$ ) è necessario utilizzare la costruzione di Dedekind. La RADICE  $q$ -ESIMA di un numero reale  $a \geq 0$  è definita dal seguente taglio dei numeri reali:

$$R = \{x \in \mathbb{R} : x > 0 \text{ e } x^n \geq a\}, \quad L = \mathbb{R} \setminus R = \{x \in \mathbb{R} : x < 0 \text{ o } x^n < a\}.$$

$(L, R)$  è effettivamente un taglio dei reali perché per costruzione ogni reale appartiene a  $R$  o a  $L$ , e perché essendo  $x^n$  una funzione *crescente* di  $x$ , tutti i reali di  $L$  sono minori di quelli in  $R$ . Quindi  $(L, R)$  identifica un unico numero reale che indichiamo con  $\sqrt[q]{a}$ , per ogni  $a > 0$ . Bisogna inoltre dimostrare, affinché la definizione sia di qualche ausilio, che  $(\sqrt[q]{a})^q = a$ . Ma ciò è ovvio interpretando la potenza  $q$ -esima in termini di tagli dei reali:

$$(\sqrt[q]{a})^q = (L', R'),$$

dove:

$$R' = \{y > 0 \text{ e } y \geq a\}, \quad L' = \{y < 0 \text{ o } y < a\},$$

per cui  $(L', R')$  è esattamente il taglio dei reali che corrisponde ad  $a$ .

Le radici di argomento negativo ovviamente pongono dei problemi, perché le potenze pari di numeri negativi sono sempre positive. Quindi, se  $q$  è *dispari*, definiamo per  $a < 0$ :

$$\sqrt[q]{a} = -\sqrt[q]{-a}, \quad (25)$$

mentre per  $q$  pari  $\sqrt[q]{a}$  non è definita se  $a < 0$ . Si osservi inoltre che con la nostra definizione, nel caso  $q$  pari la radice  $q$ -esima di un numero positivo è la sua radice *positiva*. Qualora sia necessario indicare la radice pari di segno negativo di un numero positivo, si indica esplicitamente il segno così:  $-\sqrt[q]{a}$ .

Definiamo quindi  $a^r$  per  $r \in \mathbb{Q}$ ,  $r = p/q$  e  $a \geq 0$  come segue:

$$a^{\frac{p}{q}} = \sqrt[q]{a^p}. \quad (26)$$

Le proprietà delle potenze dei numeri reali sono quelle ben note fin dalle scuole inferiori e non verranno ripetute qui.

Infine, definiamo  $a^x$  nel caso in cui  $a \in \mathbb{R}$ ,  $a \geq 0$  e  $x \in \mathbb{R}$  qualsiasi, quindi anche irrazionale.

Definiamo quindi per  $a > 1$ :

$$a^x = \sup\{a^r, r \in \mathbb{Q}, r \leq x\}. \quad (27)$$

La definizione è corretta, perché l'insieme considerato palesemente non è vuoto ed è limitato (basta prendere qualsiasi razionale  $\bar{r}$  maggiore di  $x$  per ottenerne il maggiorante  $a^{\bar{r}}$ !). Inoltre, tale definizione estende senza contraddire le definizioni precedenti, perché se  $x \in \mathbb{Q}$  allora l'estremo superiore è proprio il massimo dell'insieme.

Inoltre la proprietà fondamentale delle potenze  $a^{\alpha+\beta} = a^\alpha \cdot a^\beta$  continua ad essere soddisfatta:

$$\begin{aligned} a^{\alpha+\beta} &= \sup\{a^r, r \in \mathbb{Q}, r \leq \alpha + \beta\} = \sup\{a^{r_1+r_2}, r_1, r_2 \in \mathbb{Q}, r_1 \leq \alpha, r_2 \leq \beta\} = \\ &= \sup\{a^{r_1}, r_1 \in \mathbb{Q}, r_1 \leq \alpha\} \cdot \sup\{a^{r_2}, r_2 \in \mathbb{Q}, r_2 \leq \beta\} = a^\alpha \cdot a^\beta. \end{aligned} \quad (28)$$

Per  $0 \leq a < 1$ , definiamo:

$$a^x = \left(\frac{1}{a}\right)^x, \quad (29)$$

essendo  $1/a > 1$ , e per  $a = 1$  definiamo  $1^x = 1$ .

### 2.3.2. Logaritmi

Se  $a^x = y$ , allora scriviamo:

$$x = \log_a y \quad (\text{LOGARITMO IN BASE } a \text{ di } y). \quad (30)$$

I logaritmi sono stati introdotti dal matematico scozzese John Napier (1550-1617) nella sua opera *Mirifici logarithmorum canonis descriptio* del 1614, quindi in una epoca piuttosto antica. Furono definiti in modo un po' diverso dal modo odierno, ed il loro principale scopo era quello dell'aiuto al calcolo numerico. Una loro importante applicazione pratica da questo punto di vista, in uso fino a circa gli anni '70, cioè all'epoca in cui le calcolatrici elettroniche sono diventate sufficientemente economiche, era il *regolo calcolatore*, un semplicissimo dispositivo meccanico che permetteva di calcolare moltiplicazioni, divisioni e potenze molto facilmente anche con 3-4 cifre decimali di precisione.

Chiaramente:

$$\log_{\frac{1}{a}} y = -\log_a y, \quad (31)$$

per cui possiamo considerare solo il caso  $a > 1$  (il caso  $a = 1$  non si pone, perché  $1^x = 1$  sempre!).

Poiché  $a^x > 0$ ,  $\log_a y$  esiste solo se  $y > 0$ . Inoltre, poiché  $a^0 = 1$ ,  $\log_a 1 = 0$ , Poiché  $a^x$  è funzione crescente di  $x$ , anche  $\log_a y$  è funzione crescente di  $y$ .

Il logaritmo soddisfa alcune proprietà, che *dovrebbero* essere ben note fin dalle scuole superiori; le riassumiamo nella seguente tabella, in cui assumiamo che la base del logaritmo sia sempre un reale positivo e diverso da 1.

$\forall x > 0 :$	$a^{\log_a x} = x$
$\forall x, y > 0 :$	$\log_a xy = \log_a x + \log_a y$
$\forall x > 0 :$	$\log_a \frac{1}{x} = -\log_a x$
$\forall x, y > 0 :$	$\log_a \frac{x}{y} = \log_a x - \log_a y$
$\forall x > 0, b \in \mathbb{R} :$	$\log_a x^b = b \log_a x$
$\forall x > 0, x \neq 1 :$	$\log_a x = \frac{1}{\log_x a}$
$\forall x > 0 :$	$\log_b x = \frac{\log_a x}{\log_a b}$

Le regole in tabella vanno applicate *cum grano salis*. Infatti se  $x < 0$  abbiamo:

$$\log_a x^2 = 2 \log_a |x|, \quad (32)$$

e se  $x \cdot y > 0$  (pur avendo, eventualmente,  $x$  e  $y$  negativi!) abbiamo:

$$\log_a xy = \log_a |x| + \log_a |y|. \quad (33)$$

Occorre riflettere su queste due ultime identità e capire bene perché esse valgono, onde non cadere in molteplici errori facendo calcoli utilizzando i logaritmi.

Ulteriori proprietà del logaritmo verranno studiate nei capitoli successivi.

### 3. Esempi ed esercizi

**Esempio 11.** Esistono infiniti numeri primi. Infatti, ammettiamo che esistano un numero finito di numeri primi (chiamiamoli  $p_1, p_2, \dots, p_N$ ) e che quindi l'ultimo numero primo sia  $p_N$ . Poniamo allora:

$$M = p_1 \cdot p_2 \cdot \dots \cdot p_N + 1.$$

Chiaramente  $M - 1$  è divisibile per ogni numero primo (minore o uguale ad  $p_N$ , cioè per ipotesi tutti), per cui  $M$  darebbe resto 1 alla divisione per qualsiasi numero primo, quindi sarebbe primo, ed è palesemente maggiore di  $p_N$ : abbiamo ottenuto una contraddizione, per cui l'ipotesi di partenza (e cioè che i numeri primi siano finiti) deve essere falsa.

La dimostrazione, *mutatis mutandis*, è dovuta ad Euclide di Alessandria (325 a. C.-265 a. C.).

Da oltre duemila anni si cerca, invano, di scorgere delle regolarità nella successione dei numeri primi, che, come dice il matematico D. Zagier, “crescono come gramigna nella successione dei numeri interi”. Il più grande numero primo noto oggi (agosto 2011) è  $2^{43112609} - 1$  ed ha 12978189 cifre decimali, e mantiene tale record da

tre anni. La pagina web <http://primes.utm.edu/largest.html> contiene informazioni aggiornate sui piú grandi numeri primi noti.

**Esempio 12.** Una qualsiasi equazione algebrica della forma:

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n = 0,$$

in cui tutti i coefficienti  $a_i$  siano interi, non può avere radici razionali che non siano anche intere. In altri termini, tutte le sue radici sono o intere o irrazionali.

Infatti, se scriviamo  $x$  come frazione *ridotta ai minimi termini*  $x = p/q$ , otteniamo:

$$\left(\frac{p}{q}\right)^n + a_1\left(\frac{p}{q}\right)^{n-1} + a_2\left(\frac{p}{q}\right)^{n-2} + \cdots + a_n = 0,$$

e moltiplicando per  $q^{n-1}$  otteniamo:

$$-\frac{p^n}{q} = a_1p^{n-1} + a_2p^{n-2}q + \cdots + a_nq^{n-1},$$

che, uguagliando una frazione propria con un numero intero, è impossibile.

Questa dimostrazione, dovuta al matematico tedesco Carl Gauss (1777-1855), è presa da G. H. Hardy, *A Course of Pure Mathematics*, Cambridge 1955.