APPUNTI DEL CORSO DI ANALISI MATEMATICA 1

Gino Tironi

Stesura provvisoria del 24 settembre, 2007.

Indice

Capitolo 1

Insiemi e logica

1.1 Preliminari

In questo primo capitolo ci limiteremo a fornire quegli elementi del linguaggio logico e della teoria degli insiemi che vengono comunemente usati nella matematica attuale. Si tratta di un uso strumentale che ha sostanzialmente lo scopo di abbreviare le notazioni ed esprimere in modo piú chiaro le varie nozioni introdotte. Gli argomenti qui accennati meriterebbero uno studio approfondito, ma in altra sede che non sia quella di un primo corso di Analisi matematica. Qui noi ne metteremo in evidenza solo l'utilità quale "stenografia dei principali aspetti della matematica che tratteremo.

1.2 Cenni di logica: connettivi, quantificatori

1.2.1 Connettivi logici

Un concetto si dice "primitivo, se non è riconducibile ad altri piú elementari. Assumeremo come primitivo in logica il concetto di *proposizione*. Con ciò si intende un'espressione di un linguaggio umano o un'espressione di tipo matematico della quale si possa affermare che è o vera o falsa. Noi prenderemo in considerazione proposizioni di argomento matematico, spesso piú facili da giudicare rispetto a quelle del linguaggio umano corrente. Cosí la proposizione P: "Il numero 2 è dispari è una proposizione che facilmente si giudica come falsa (ha valore di verità F). Dunque oggetti elementari del linguaggio logico saranno le proposizioni $P, Q, R, S, \ldots$ suscettibili di avere solo due valori di verità: o Vero o Falso. Queste proposizioni si potranno combinare fra loro per mezzo di *connettivi logici* al fine di ottenere altre proposizioni. I connettivi logici che sono comunemente considerati sono: la negazione $\neg P$, che ha valore di verità Vero se P è Falso ed è Falso se P è Vero; $\wedge$: $P \wedge Q$ è Vero se e solo se entrambe le proposizioni P e Q lo sono; $\vee$: $P \vee Q$ è Vero se almeno uno dei due P oppure Q lo è; $\Rightarrow$: $P \Rightarrow Q$ ha lo stesso valore di verità di $\neg P \vee Q$. Ossia è

Falsa se e solo se P è Vera e Q è Falsa. In tutti gli altri casi l'implicazione è Vera. In particolare $P \Rightarrow Q$ è Vera se la premessa P è Falsa. Questo uso dell'implicazione si discosta dall'uso del linguaggio comune nel quale quando si afferma che P "implica Q implicitamente si ammette che P sia Vera. Per questa ragione, cioè per distinguerla dal significato del linguaggio comune, si suole chiamare *implicazione materiale* l'implicazione usata comunemente in Matematica. L'uso è utile per semplificare l'enunciato di molti teoremi, evitando di fare di volta in volta varie precisazioni. Infine c'è la doppia implicazione $\Leftrightarrow$: $P \Leftrightarrow Q$ è vera se e solo se P e Q hanno lo stesso valore di verità. I connettivi logici che abbiamo introdotto hanno il seguente significato nel linguaggio comune: $\neg P$ si legge *non* P; $P \wedge Q$ si legge P *e* Q; $P \vee Q$ si legge P *oppure* Q; $P \Rightarrow Q$ si legge P *implica* Q oppure *se* P *allora* Q, con l'osservazione fatta sul significato in Matematica dell'implicazione materiale; $P \Leftrightarrow Q$ si legge P *se e solo se* Q. È facile notare che $P \Leftrightarrow Q$ significa $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. I connettivi sono caratterizzati dalle loro *tabelle di verità*.

Tabella di verità per la **negazione "non**:

P	$\neg P$
V	F
F	V

Tabella di verità per la **congiunzione "e**:

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

Tabella di verità per la **disgiunzione "o**:

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

Tabella di verità per l'**implicazione "se P allora Q**:

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Tabella di verità per la **doppia implicazione "P se e solo se Q**:

P	Q	$P \Leftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

1.2.2 Predicati e quantificatori logici

Accanto alle proposizioni che hanno un ben preciso valore di verità (V oppure F) considereremo come nozione primitiva quella di *predicato* $P(x)$ dipendente da una variabile x, $P(x, y)$ dipendente da due variabili x, y, $P(x, y, z)$ dipendente da tre variabili x, y, z, ..., che diviene una proposizione quando al posto di $x, y, z, \ldots$ si sostituiscono valori da scegliere in un assegnato *universo*. Esempi di predicati con una, due o tre variabili sono i seguenti: $P(x)$ valga "x è un numero naturale pari; $P(x, y)$ sia "$x < y$ con $x, y \in \mathbb{R}$; $P(x, y, z)$ sia "$x^2 + y^2 = z^2$ con $x, y, z \in \mathbb{R}$. Allora è chiaro che $P(3)$ vale F, mentre $P(7424)$ vale V. $P(3, 4)$ vale V, ma $P(15, -\pi)$ vale F. $P(3, 4, 5)$ vale V, ma $P(6, 7, 8 \cdot e)$ vale F. I predicati possono intendersi come "proposizioni aperte, che divengono proposizioni effettive solo quando al posto della o delle variabili si assegnano valori appartenenti all'"universo nel quale ci si muove (i numeri naturali, o i reali, o i numeri complessi, ...). Si noti che l'indeterminazione e vaghezza con la quale sono presentati i concetti logici ora introdotti è dovuta al fatto che abbiamo deciso di darne una trattazione intuitiva e non formalizzata.

In una trattazione formalizzata e assiomatica sia le nozioni di proposizione che di predicato rientrano nella definizione di "formula o di "formula ben formata che viene data in modo ricorsivo; allora ogni sapore d'indeterminazione sparisce, ma la trattazione è piuttosto pesante per un studente che s'affacci per la prima volta all'insegnamento di tipo universitario.

Dato un predicato $P(x)$, dipendente da una sola variabile, si può ottenere una proposizione sia sostituendo un valore particolare alla variabile x, come già abbiamo ricordato, oppure affermando che esista qualche valore nell'universo considerato che rende vera la proposizione $P(x)$ oppure che essa vale per ogni valore di x. Ciò corrisponde a considerare i quantificatori esistenziale o, rispettivamente, universale applicati a $P(x)$. Espresse in simboli, sono proposizioni

$$(\exists x)P(x) \tag{1.1}$$

che, a parole, significa "esiste x per il quale vale $P(x)$ e

$$(\forall x)P(x) \tag{1.2}$$

che, a parole, significa "per ogni x vale $P(x)$.

Si sottointende in generale l'universo al quale ci si riferisce. Se è importante specificare a quale ambiente si riferisca il quantificatore, si dirà "esiste $x \in \mathbb{R}$ (in simboli $(\exists x \in \mathbb{R})$) oppure "per ogni numero intero relativo n (in simboli $(\forall n \in \mathbb{Z})$).

Conviene mettere in evidenza che la negazione della proposizione $(\forall x)P(x)$ è $(\exists x)\neg P(x)$ (in parole, la negazione della proposizione "per ogni x vale $P(x)$ è "esiste un x per il quale non vale $P(x)$), e che la negazione di $(\exists x)P(x)$ è $(\forall x)\neg P(x)$ (in parole, la negazione di " esiste qualche x per il quale vale $P(x)$ è "per ogni x non vale $P(x)$). Cioè

$$\neg\left((\forall x)\, P(x)\right) \equiv \left((\exists x)\, \neg P(x)\right) \tag{1.3}$$

$$\neg\left((\exists x)\, P(x)\right) \equiv \left((\forall x)\, \neg P(x)\right). \tag{1.4}$$

Qui il simbolo $\equiv$ significa che le due proposizioni messe a confronto hanno lo stesso valore di verità. Vedremo meglio nel seguito esempi di uso dei quantificatori e della loro negazione.

1.3 Cenni di teoria degli insiemi

Ulteriori concetti che assumeremo come primitivi sono quelli di insieme, di elemento e di appartenenza di un elemento ad un insieme. Un insieme si può intendere come una collezione di oggetti pensati come un tutt'uno. Gli oggetti che concorrono a formare un insieme sono i suoi elementi; un insieme è ben formato quando c'è una legge che dato un elemento ci permette di decidere se esso appartenga oppure no ad un assegnato insieme. Esistono varie teorie degli insiemi. Quella che la maggior parte dei matematici usa è quella detta "ingenua, che sostanzialmente esporremo brevemente e che è una rassegna delle operazioni che ci permetteremo di eseguire sugli insiemi. Fra le teorie assiomatiche degli insiemi, la piú comunemente usata dai matematici che si occupano di Fondamenti della Matematica è probabilmente la Teoria di Zermelo - Fraenkel con o senza l'assioma di scelta (Teoria ZF o ZFC). Qui C sta per "choice, cioè "scelta, in inglese. In questa teoria ogni elemento è a sua volta un insieme e quindi è definita la relazione di appartenenza fra due insiemi: $x \in y$ significa l'insieme x è un elemento dell'insieme y (x appartiene a y). Ci sono anche teorie che ammettono l'esistenza di elementi che non sono insiemi, detti "atomi. Un'altra teoria assiomatica degli insiemi molto diffusa è quella dovuta a von Neumann, Bernays e Gödel (Teoria NBG); in essa si distinguono due tipi di collezioni: gli insiemi e le classi. Elemento primitivo è la classe; una classe è un insieme se appartiene ad un'altra classe. Questa teoria presenta alcuni vantaggi formali sulla precedente, qualora si vogliano trattare alcune teorie matematiche come quella delle Categorie, ma le due teorie sono sostanzialmente equivalenti.

1.3.1 Insieme vuoto, inclusione e uguaglianza d'insiemi

Esponiamo ora le nozioni essenziali di una teoria ingenua degli insiemi.

Ci sono gli insiemi quali per esempio quelli dei numeri naturali ($\mathbb{N}$), degli interi relativi ($\mathbb{Z}$), dei razionali ($\mathbb{Q}$), dei reali ($\mathbb{R}$), dei complessi ($\mathbb{C}$), ...e i loro elementi. Se a è un elemento di A, scriveremo $a \in A$. In generale supporremo assegnato un ambiente o universo U (per esempio l'insieme dei numeri reali) e ogni insieme considerato sarà costruito a partire da quell'ambiente o universo. Per descrivere un insieme, quando esso sia finito e si conoscano tutti i suoi elementi, si potrà semplicemente procedere all'elencazione degli elementi stessi fra parentesi graffe.

$$A = \{-1, e, 3\pi\} \tag{1.5}$$

è l'insieme chiamato A e avente per elementi i tre numeri reali -1, e (numero di Nepero) e 3π. Se un insieme non è finito, non si può pensare di elencarne tutti gli elementi. Spesso saremo in grado di descriverlo (all'interno di un assegnato universo) esplicitando la o le proprietà alle quali soddisfano i suoi elementi.

$$P = \{n : n = 2 \cdot k, k \in \mathbb{Z}\} \tag{1.6}$$

descrive l'insieme dei numeri interi relativi pari.

È conveniente considerare anche un insieme come il seguente all'interno di un certo universo U

$$\emptyset = \{x \in U : x \neq x\}. \tag{1.7}$$

Ovviamente ogni elemento è uguale a sé stesso e dunque l'insieme considerato non ha alcun elemento; esso si dice l'*insieme vuoto* e viene indicato con il simbolo $\emptyset$. È da notare che l'insieme vuoto è unico; non cambia al cambiare dell'universo al quale si riferisce. Ciò è una conseguenza della definizione di uguaglianza fra insiemi. Due insiemi sono uguali quando hanno gli stessi elementi. Dunque tutti gli insiemi senza elementi sono fra loro uguali. Dati due insiemi A e B diremo che A è un sottoinsieme di B o che A è contenuto in B (o che B contiene A) se ogni elemento di A è anche elemento di B. Scriveremo $A \subseteq B$ per dire che A è contenuto in B. In formula

$$A \subseteq B \text{ significa } (\forall x)(x \in A \Rightarrow x \in B) \quad . \tag{1.8}$$

Dunque l'uguaglianza di insiemi è formalmente descritta da

$$A = B \text{ significa } (\forall x)(x \in A \Leftrightarrow x \in B) \text{ ossia } A \subseteq B \wedge B \subseteq A \quad . \tag{1.9}$$

Si noti che, anche praticamente, per dimostrare l'uguaglianza di due insiemi A e B conviene dimostrare che valgono sia $A \subseteq B$ che $B \subseteq A$. Si noti che due insiemi sono uguali se contengono gli stessi elementi indipendentemente dall'ordine nel quale gli elementi sono elencati e dall'eventuale ripetizione di uno stesso elemento. Se $A = \{a, b, c\}$ e $B = \{c, c, a, b, b, a, a, a\}$, vale $A = B$. In base alle definizioni date, evidentemente avremo $\emptyset \subseteq A$, quale che sia l'insieme A. Si noti che in $(\forall x)(x \in \emptyset \Rightarrow x \in A)$ la premessa, $x \in \emptyset$, dell'implicazione è falsa e dunque, in base alla definizione di implicazione materiale, l'implicazione è vera, quale che sia A.

1.3.2 Unione, intersezione, differenza, prodotto

Dati due insiemi A e B esiste un insieme che contiene tutti e soli gli elementi di A e di B. Questo insieme si dice l'insieme *unione di A e B* ed è definito da

$$A \cup B = \{x : (x \in A) \vee (x \in B)\}. \tag{1.10}$$

Se $\{A_k : k = 1, \ldots, n\}$, è un insieme di n insiemi indiciati da $k = 1, \ldots, n$

$$\bigcup_{k=1}^{n} A_k = A_1 \cup A_2 \cup \ldots \cup A_n = \{x : (\exists k)(1 \leq k \leq n)(x \in A_k)\}\,. \tag{1.11}$$

Piú in generale, se I è un insieme d'indici e $\{A_i : i \in I\}$ è un *insieme indiciato d'insiemi* o *famiglia indiciata d'insiemi*, diremo *unione della famiglia* $\{A_i\}$ l'insieme

$$\bigcup_{i \in I} A_i = \{x : (\exists i \in I)(x \in A_i)\}\,. \tag{1.12}$$

Dati i due insiemi A e B si dice *intersezione* di essi l'insieme che contiene tutti e soli gli elementi che stanno sia in A che in B; cioè l'insieme degli elementi di A che sono anche elementi di B o, equivalentemente, l'insieme degli elementi di B che sono anche elementi di A. Si noti che questo insieme, essendo sottoinsieme sia di A che di B, esiste certamente

$$\begin{aligned} A \cap B &= \{x \in A : x \in B\} = \{x \in B : x \in A\} \\ &= \{x : (x \in A) \wedge (x \in B)\} \quad . \end{aligned} \tag{1.13}$$

Se $\{A_k : k = 1, \ldots, n\}$, è un insieme di n insiemi indiciati da $k = 1, \ldots, n$

$$\begin{aligned} \bigcap_{k=1}^{n} A_k &= A_1 \cap A_2 \cap \ldots \cap A_n = \{x : (x \in A_1) \wedge \ldots \wedge (x \in A_n)\} = \\ &= \{x : (\forall k)(1 \leq k \leq n)(x \in A_k)\} \quad . \end{aligned} \tag{1.14}$$

Piú in generale, se I è un insieme d'indici e $\{A_i : i \in I\}$ è una famiglia indiciata d'insiemi, diremo *intersezione della famiglia* $\{A_i\}$ l'insieme

$$\bigcap_{i \in I} A_i = \{x \in U : (\forall i)\ ((i \in I) \Rightarrow (x \in A_i))\}\,. \tag{1.15}$$

Cioè si tratta dell'insieme degli elementi comuni a tutti gli insiemi $\{A_i\}$. Si noti che (1.15) è stata scritta in modo che appaia chiaro che se $I = \emptyset$ allora

$$\bigcap_{i \in \emptyset} A_i = U \quad , \tag{1.16}$$

dove U è l'universo nel quale andiamo a scegliere gli elementi. Infatti la premessa $(i \in \emptyset)$ è falsa. Invece per l'unione si ha, meno sorprendentemente, che

$$\bigcup_{i \in \emptyset} A_i = \emptyset \quad , \tag{1.17}$$

Dati due insiemi A e B si dice *differenza* di A e B l'insieme che contiene tutti e soli gli elementi che stanno in A ma non in B.

$$A \setminus B = \{x \in A : x \notin B\} \quad . \tag{1.18}$$

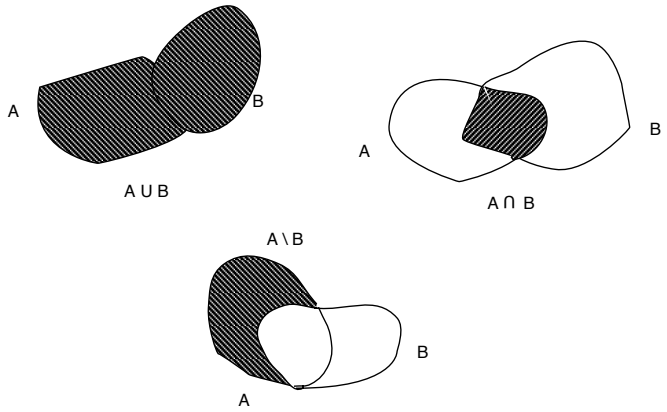

Figura 1.1: Sono tratteggiati gli insiemi $A \cup B$, $A \cap B$ e $A \setminus B$

Nella Figura (**??**) sono rappresentati con il tratteggio gli insiemi $A \cup B$, $A \cap B$ e $A \setminus B$.

In base alle definizioni date, le operazioni introdotte soddisfano le seguenti proprietà

$$A \cup \emptyset = A; \qquad A \cap \emptyset = \emptyset; \quad A \setminus \emptyset = A\,, \tag{1.19}$$

quale che sia l'insieme A. Quali che siano gli insiemi A, B, C valgono le seguenti

Proprietà associativa dell'unione e dell'intersezione

$$A \cup (B \cup C) = (A \cup B) \cup C; \quad A \cap (B \cap C) = (A \cap B) \cap C. \tag{1.20}$$

Proprietà commutativa dell'unione e dell'intersezione

$$A \cup B = B \cup A; \quad A \cap B = B \cap A. \tag{1.21}$$

Proprietà distributiva dell'unione rispetto all'intersezione e dell'intersezione rispetto all'unione

$$\begin{aligned} A \cup (B \cap C) &= (A \cup B) \cap (A \cup C); \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C). \end{aligned} \tag{1.22}$$

Valgono poi le Formule di De Morgan

$$\begin{aligned} A \setminus (\bigcup_{i \in I} B_i) &= \bigcap_{i \in I} (A \setminus B_i) \\ A \setminus (\bigcap_{i \in I} B_i) &= \bigcup_{i \in I} (A \setminus B_i). \end{aligned} \tag{1.23}$$

Si dice *complementare* di un insieme C, sottoinsieme dell'universo U, l'insieme $U \setminus C = \mathcal{C}C = \tilde{C}$. Le formule di De Morgan applicate ai complementari affermano che il complementare dell'unione di una famiglia d'insiemi è l'intersezione dei complementari e che il complementare d'una intersezione d'insiemi è l'unione dei complementari. Il complementare dell'insieme vuoto è l'universo e il complementare dell'universo è l'insieme vuoto.

Un insieme che contenga un solo elemento x (cioè l'insieme $\{x\}$), si dice un *singoletto*. Un insieme contenente due elementi x e y (cioè l'insieme $\{x, y\}$) si dice una *coppia non ordinata*. È chiaro che se $x = y$ la coppia si riduce ad un singoletto. Una *coppia ordinata* è un insieme rappresentato con (x, y) nel quale contano gli elementi presenti, ma anche l'ordine nel quale sono elencati. Cioè si richiede che $(x, y) = (a, b)$ se e solo se $x = a$ e $y = b$. Si noti che la coppia ordinata (x, y) è cosa ben diversa dalla coppia non ordinata $\{x, y\}$. In particolare $(x, x) \neq \{x\}$ e se $x \neq y$ $(x, y) \neq (y, x)$. Il matematico polacco Kazimierz Kuratowski ha escogitato la seguente rappresentazione della coppia ordinata in termini puramente insiemistici $(x, y) := \{\{x\}, \{x, y\}\}$. Chi studia dimostri come utile esercizio che vale la proprietà fondamentale $(x, y) = (a, b)$ se e solo se $x = a$ e $y = b$.

Dati due insiemi A e B, diremo *prodotto cartesiano* di A e B, denotato da $A \times B$ l'insieme formato da tutte le coppie ordinate (a, b) con il primo elemento in A ed il secondo in B

$$A \times B = \{(a, b) : a \in A, b \in B\} \quad . \tag{1.24}$$

Esercizio 1.3.1 *Si dimostrino le uguaglianze*

$$\begin{aligned} (A \cup B) \times (C \cup D) &= (A \times C) \cup (A \times D) \cup (B \times C) \cup (B \times D) \\ (A \times C) \cap (B \times D) &= (A \cap B) \times (C \cap D) \end{aligned}$$

1.3.3 Applicazioni o funzioni

Dati due insiemi non vuoti A e B, un'*applicazione o funzione* f definita su A e a valori in B, è una legge che, ad ogni $x \in A$ associa un **unico** elemento $y \in B$. Essa viene indicata con

$$f : A \to B \tag{1.25}$$

e il valore $y \in B$ si denota con $y = f(x)$. L'insieme A si dice il *dominio* della funzione o applicazione f; $A = \operatorname{dom} f$. B si dice il *codominio* della funzione; $B = \operatorname{codom} f$. L'insieme dei punti di B che sono immagine dei punti di A, si dice l'*immagine* di f.

$$\operatorname{im} f = \{y \in B : (\exists x \in A)\ (y = f(x))\}\,. \tag{1.26}$$

Un'applicazione o funzione $f : A \to B$ si dice *suriettiva* se $\operatorname{im} f = B$, ossia se per ogni $y \in B$ esiste qualche $x \in A$ tale che $y = f(x)$. L'applicazione $f : A \to B$ si dice *iniettiva* se porta punti distinti di A in punti distinti di B; cioè se, essendo $x_1, x_2 \in A$, $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$. Un'applicazione che sia iniettiva e suriettiva si dice *biiettiva*. Se $f : A \to B$ è biiettiva, allora ad ogni $y \in B$ si può associare un $x \in A$ (per la suriettività) ed uno solo (per l'iniettività). Dunque ad ogni $y \in B$ resta associato un solo $x \in A$ tale che $f(x) = y$. Ma questa è una legge che ad ogni elemento di B associa uno ed un solo elemento di A; cioè abbiamo un'applicazione $\varphi : B \to A$. Quest'applicazione si dice l'*inversa* dell'applicazione $f : A \to B$ e si denota con $f^{-1} : B \to A$. Precisamente $f^{-1}(y) = x$ se x è l'unico elemento di A tale che $f(x) = y$. Se $f : A \to B$ e $g : D \to C$, con $B \subseteq D$, si può considerare la *funzione composta* $g \circ f : A \to C$ definita come segue: per ogni $x \in A$, $(g \circ f)(x) := g(f(x))$. Cioè a $x \in A$ si associa il valore $g(f(x)) \in C$. Si noti che se f e g sono componibili, nel senso che si può valutare $g \circ f$, non è detto che si possano comporre g ed f nel senso che si possa considerare $f \circ g$; lo si può facilmente comprendere perché, in generale, il codominio di g, cioè C, non è un sottoinsieme del dominio di f, cioè A. Si consideri il seguente semplice esempio. Sia $f(x) = \sqrt{x}$, $f : A \to \mathbb{R}$, con $A = \{x \in \mathbb{R} : x \geq 0\}$. Sia poi $g(y) = \operatorname{sen} y$ definita per ogni $y \in \mathbb{R}$ a valori in $\mathbb{R}$, anzi nell'intervallo $I = [-1, 1] = \{z \in \mathbb{R} : -1 \leq z \leq 1\}$; dunque $g : \mathbb{R} \to I$. Allora è definita $(g \circ f) : A \to I$, ma non è definita su tutto $\mathbb{R}$ la funzione $(f \circ g)$. Infatti se $y = \frac{3\pi}{2}$, $g(y) = -1$ e $f(-1) = \sqrt{-1}$ non è definita in $\mathbb{R}$. Inoltre, anche nel caso in cui sia $g \circ f$ che $f \circ g$ siano entrambe definite, cosa che certamente accade se $f, g : A \to A$, cioè se dominio e codominio di f e g coincidono, avremo $f \circ g \neq g \circ f$. Si pensi, per esempio, a $f : \mathbb{R} \to \mathbb{R}$ data da $f(x) = x + 1$ e $g : \mathbb{R} \to \mathbb{R}$ data da $g(x) = 2x$. Allora $g(f(x)) = 2x + 2$, mentre $f(g(x)) = 2x + 1$. Dunque $f \circ g \neq g \circ f$.

Fra tutte le applicazioni da un insieme E in sé la piú semplice è l'applicazione identità su E che lascia ogni elemento di E invariato: $i_E : E \to E$, tale che $\forall x \in E$, $i_E(x) = x$. Se $f : A \to B$ è biiettiva essa è legata a f^{-1} dalle relazioni

$$\begin{aligned} f \circ f^{-1} : B \to B \quad &\text{e} \quad f \circ f^{-1} = i_B; \\ f^{-1} \circ f : A \to A \quad &\text{e} \quad f^{-1} \circ f = i_A\,. \end{aligned} \tag{1.27}$$

Infatti se $y \in B$, $f^{-1}(y)$ è l'unico $x \in A$ tale che $f(x) = y$. Dunque $(f \circ f^{-1})(y) = y$, $\forall y \in B$. Analogamente, dato $x \in A$, $f(x) \in B$ e, per definizione, $(f^{-1} \circ f)(x) = x$, $\forall x \in A$.

Se $f : A \to B$ ed $E \subseteq A$, diremo *immagine di E per mezzo di f*, il sottinsieme di B dato da

$$f(E) = \{y \in B : (\exists x \in E)(y = f(x))\} \quad . \tag{1.28}$$

Se $E' \subseteq B$, diremo *controimmagine o immagine inversa di E' per mezzo di f*, l'insieme

$$f^{-1}(E') = \{x \in A : f(x) \in E'\} \quad . \tag{1.29}$$

È evidente dalla definizione che

$$f(f^{-1}(E')) \subseteq E' \quad \text{e} \quad f^{-1}(f(E)) \supseteq E \quad . \tag{1.30}$$

Chi studia lo provi come esercizio. Si noti che le inclusioni possono valere in senso proprio. Se, per esempio, $f(x) = x^2$ come funzione da $\mathbb{R}$ a $\mathbb{R}$, allora se $E' = \{x \in \mathbb{R} : -1 \leq x \leq 0\}$, $f^{-1}(E') = \{0\}$ e $f(f^{-1}(E')) = \{0\} \subsetneq E'$; se $E = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$, $f(E) = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ e $f^{-1}(f(E)) = \{x \in \mathbb{R} : -1 \leq x \leq 1\} \supsetneq E$.

Data $f : A \to B$, se $E \subseteq A$ possiamo considerare la funzione $f|_E$ (denotata anche con $f \restriction E$) avente dominio E e codominio B e definita dalla relazione $f|_E(x) = f(x)$, $\forall x \in E$, mentre non è definita sugli eventuali $x \in A \setminus E$. Essa si dice la *restrizione* di f ad E. È spesso un problema interessante in matematica quello, per cosí dire inverso: data $f : E \to B$ e dato $A \supseteq E$ si cerca una funzione $F : A \to B$, tale che $F|_E = f$. La funzione F si dice allora il *prolungamento* o *estensione* di f ad A. Mentre il problema fra le applicazioni intese in senso puramente insiemistico è banale, esso diviene interessante quando si chiede che F conservi certe proprietà importanti di f, quali, per esempio, la continuità. In questo caso il problema diviene importante e non sempre ha soluzione.

Dati due insiemi A e B non vuoti, penseremo come operazione lecita su di essi, quella consistente nel considerare tutte le applicazioni $f : A \to B$. Questa totalità, forma un insieme che denoteremo con

$${}^AB = B^A := \{f : (f : A \to B)\} \quad . \tag{1.31}$$

Torniamo brevemente sul concetto di insieme prodotto. Se sono dati tre insiemi A, B, C, possiamo considerare i seguenti insiemi prodotti cartesiani: $(A \times B) \times C$, cioè l'insieme delle coppie $\{((a, b), c) : a \in A, b \in B, c \in C\}$ e $A \times (B \times C) = \{(a, (b, c)) : a \in A, b \in B, c \in C\}$. Chiaramente i due insiemi sono diversi, ma sono in corrispondenza biunivoca tra di loro. Infatti $\kappa : (A \times B) \times C \to A \times (B \times C)$ definita da $\kappa((a, b), c) = (a, (b, c))$ è un'applicazione biettiva fra i due insiemi. Dunque potremo pensare di confonderli fra loro in molte situazioni pratiche. Inoltre, disponendo della nozione di applicazione, potremo pensare ad un insieme $A \times B \times C$ (senza alcuna parentesi frapposta), come l'insieme di tutte le possibili applicazioni f dall'insieme $\{1, 2, 3\}$ nell'insieme $A \cup B \cup C$, tali che $f(1) \in A, f(2) \in B, f(3) \in C$. Anche quest'ultimo insieme è in corrispondenza biunivoca con i primi due, e, se non ci sono esigenze particolari per tenerle distinte, potremo confondere fra loro le tre nozioni. Si pensi anche che $A \times B$ è in corrispondenza biunivoca con l'insieme delle applicazioni $f : \{1, 2\} \to A \cup B$, tali che $f(1) \in A, f(2) \in B$. In generale, data una famiglia d'insiemi $\{A_i : i \in I\}$

il prodotto cartesiano della famiglia sarà l'insieme di tutte le applicazioni dall'insieme d'indici I in $\cup_{i\in I}A_i$ tali che, per ogni $i \in I$, $f(i) \in A_i$

$$\prod_{i\in I} A_i = \{f : (f : I \to \bigcup_{i\in I} A_i), (\forall i \in I)\,(f(i) \in A_i)\}\,. \tag{1.32}$$

Un caso particolare interessante è quello della famiglia costante d'insiemi. In questo caso, se $A = B$, l'insieme $A \times A$ si denota anche con A^2; se $A = B = C$, allora $A \times A \times A$ è denotato anche A^3. Piú in generale, se $A_i = A, (\forall i \in I)$,

$$\prod_{i\in I} A_i = A^I \quad , \tag{1.33}$$

ciò coincide con la notazione già introdotta per l'insieme delle applicazioni da I ad A.

È ovvio che se per qualche $k \in I$, $A_k = \emptyset$, allora il prodotto cartesiano $\prod_{i\in I} A_i = \emptyset$. Infatti non è possibile trovare un'applicazione $f : I \to \bigcup_{i\in I} A_i)$, tale che $f(k) \in A_k$, dal momento che A_k non ha elementi. Uno dei modi per enunciare il tanto discusso *Assioma di scelta* è di assumere che il prodotto cartesiano sia vuoto solamente quando qualche insieme A_k è vuoto. L'assioma di scelta è stato discusso e controverso nei primi anni del 1900, poiché alcune delle conseguenze che se ne traggono appaiono paradossali.

1.3.4 Insieme potenza

Dato un insieme A si dice *insieme potenza di A* o *insieme delle parti di A*, l'insieme di tutti i sottinsiemi di A. La definizione significa che noi decidiamo di pensare lecita l'operazione che consiste nel prendere in considerazione tutti i sottoinsiemi di un insieme dato, e produrre cosí un nuovo insieme, denotato da

$$\mathcal{P}(A) := \{E : E \subseteq A\} \quad . \tag{1.34}$$

Si noti che $\mathcal{P}(A) \neq \emptyset$, anche se $A = \emptyset$. Infatti $\mathcal{P}(\emptyset) = \{\emptyset\}$, insieme che contiene un elemento e dunque non è vuoto.

Se, per ogni $E \subseteq A$, definiamo come segue un'applicazione, detta *funzione caratteristica di E*

$$\chi_E(x) = \begin{cases} 0 & : \quad x \notin E \\ 1 & : \quad x \in E \end{cases} \tag{1.35}$$

allora vi è una corrispondenza biunivoca tra i sottoinsiemi di A e le applicazioni da A in $\{0, 1\}$. Cioè una corrispondenza biunivoca tra gli insiemi $\mathcal{P}(A)$ e $\{0, 1\}^A$, che si indica anche con 2^A, avendo definito $2 = \{0, 1\}$. Spesso 2^A viene usato nei due sensi. In generale, questo doppio uso della notazione non genera confusione. In particolare $2^\emptyset = \mathcal{P}(\emptyset) = \{\emptyset\}$. Infatti esiste sempre l'applicazione vuota dall'insieme vuoto in un insieme non vuoto.

1.4 Relazioni binarie

Dato un insieme non vuoto A diremo che è data una relazione binaria $\mathcal{R}$ su A, se è dato un sottoinsieme $R \subseteq A \times A$. Diremo che due elementi $a, b \in A$ sono in relazione $\mathcal{R}$ fra loro e scriveremo $a\mathcal{R}b$ se la coppia ordinata $(a, b) \in R$; se $(a, b) \notin R$ a e b non stanno in relazione $\mathcal{R}$ fra loro e si scrive $a \not\mathcal{R} b$. Equivalentemente, diremo che è data una relazione $\mathcal{R}$ su A se è assegnata un'applicazione

$$\rho : A \times A \to \{0, 1\} \quad . \tag{1.36}$$

Gli elementi $a, b \in A$ (nell'ordine), sono in relazione $\mathcal{R}$ fra loro se $\rho(a, b) = 1$. Se $\rho(a, b) = 0$, i due elementi **non** stanno in relazione fra loro. È chiaro che il sottoinsieme R di $A \times A$ è la controimmagine di $\{1\}$ per l'applicazione ρ: $R = \rho^{-1}(\{1\})$. Interessano alcune proprietà formali delle relazioni binarie. Diremo che la relazione binaria $\mathcal{R}$ ha la proprietà

1. Riflessiva, se $\forall a \in A$ si ha $a\mathcal{R}a$, ossia se ogni $a \in A$ è in relazione $\mathcal{R}$ con sé stesso.
2. Simmetrica, se $\forall a, b \in A$ si ha $(a\mathcal{R}b) \Rightarrow (b\mathcal{R}a)$, ossia se per ogni coppia di elementi $a, b \in A$, se a è in relazione $\mathcal{R}$ con b allora b è in relazione $\mathcal{R}$ con a.
3. Antisimmetrica, se $\forall a, b \in A$ $(a\mathcal{R}b) \wedge (b\mathcal{R}a) \Rightarrow (a = b)$, ossia se per ogni coppia di elementi $a, b \in A$, se a è in relazione $\mathcal{R}$ con b e b è in relazione $\mathcal{R}$ con a, allora $a = b$.
4. Transitiva, se $\forall a, b, c \in A$ $(a\mathcal{R}b) \wedge (b\mathcal{R}c) \Rightarrow (a\mathcal{R}c)$, ossia se per ogni terna a, b, c di elementi di A, se a è in relazione $\mathcal{R}$ con b e b è in relazione $\mathcal{R}$ con c, allora a è in relazione $\mathcal{R}$ con c.

1.4.1 Relazioni d'equivalenza

Una relazione che soddisfi le proprietà riflessiva, simmetrica e transitiva si dice una *relazione d'equivalenza*. Solitamente si usa denotare una relazione d'equivalenza, usando il simbolo $\sim$. Naturalmente ci possono essere piú relazioni d'equivalenza e, volendo essere piú precisi, si scriverà $a \sim_{\mathcal{R}} b$ per dire che a e b sono equivalenti secondo la relazione $\mathcal{R}$. Data una relazione d'equivalenza $\mathcal{R}$, possiamo considerarne le *classi d'equivalenza*:

$$[a]_{\mathcal{R}} = \{b \in A : b \sim_{\mathcal{R}} a\} \quad . \tag{1.37}$$

L'insieme delle classi d'equivalenza $\mathcal{R}$ su A, è un insieme (sottoinsieme di $\mathcal{P}(A)$), che denoteremo con $A/\mathcal{R}$, che si dice *l'insieme quoziente di A, rispetto all'equivalenza* $\mathcal{R}$, (o *A su* $\mathcal{R}$). Se scegliamo un particolare elemento $\bar{a}$ da ogni classe d'equivalenza $[a]_{\mathcal{R}}$, abbiamo un *rappresentante* per ogni classe d'equivalenza. L'insieme di tutti i rappresentanti è detto un *sistema completo di rappresentanti* ed è in corrispondenza biunivoca con l'insieme quoziente $A/\mathcal{R}$.

Dato un insieme non vuoto A, diremo *partizione* (o *ripartizione*) di A una famiglia di sottoinsiemi $E_i \subseteq A$, con $i \in I$, tale che $E_i \neq \emptyset$ per ogni $i \in I$, $E_i \cap E_j = \emptyset$, per $i \neq j$ e $A = \cup_{i \in I} E_i$. Data che sia una relazione d'equivalenza, le classi $[a]_{\mathcal{R}}$, con $a \in A$, costituiscono una ripartizione di A. Le classi della ripartizione sono indiciate dagli elementi di A e $[a] \cap [b] = \emptyset$ se e solo se $a \not\sim b$. Se abbiamo

un sistema completo di rappresentanti, la descrizione è piú chiara: da $\bar{a} \neq \bar{b}$ segue $[\bar{a}] \cap [\bar{b}] = \emptyset$. Viceversa, data una ripartizione $\mathcal{E} = \{E_i : i \in I\}$ di A, si può definire un'equivalenza dicendo che $a \sim_{\mathcal{E}} b$ se esiste un elemento $E_i \in \mathcal{E}$, tale che $a, b \in E_i$. Considerando le classi dell'equivalenza cosí ottenuta si ritrova la ripartizione $\mathcal{E}$. Dunque ad ogni ripartizione $\mathcal{E}$ su A si può associare l'insieme che ha come elementi le classi della ripartizione e quest'insieme si dirà ancora insieme quoziente $A/\mathcal{E}$.

Vedremo nel seguito quale ruolo importante abbiano le relazione d'equivalenza nelle estensioni dei campi numerici da $\mathbb{N}$ a $\mathbb{Z}$ e da $\mathbb{Z}$ a $\mathbb{Q}$.

1.4.2 Relazioni d'ordine

Una relazione binaria che soddisfi le proprietà riflessiva, antisimmetrica e transitiva si dice una *relazione d'ordine* (*in senso debole*, se si vuole essere precisi). In generale, per indicare che i due elementi a e b di A (nell'ordine dato) stanno in una relazione d'ordine fra loro, si scrive $a \preceq b$ che si legge "a precede b oppure $b \succeq a$ che si legge "b segue a. Data una relazione d'ordine "debole $\preceq$ si può ottenere una relazione d'ordine "forte o "stretta che si denota con $\prec$ e si legge "precede strettamente, definendo $a \prec b$ se e solo se $a \preceq b$ e $a \neq b$. Una relazione d'ordine in senso stretto soddisfa le proprietà IRRIFLESSIVA, cioè $a \not\prec a$ per ogni $a \in A$, CONTROSIMMETRICA, cioè $a \prec b$ non è compatibile con $b \prec a$, e transitiva.

Una relazione d'ordine si dice *totale* se $\forall a, b \in A$ è verificato che $a \preceq b$ o che $b \preceq a$; ossia che vale $a \prec b$ oppure $a = b$ oppure $b \prec a$.

Dato un insieme A, con piú di un elemento, la relazione d'inclusione $E \subseteq F$ fra sottoinsiemi di A è un tipico esempio di relazione d'ordine in senso debole parziale (cioè non totale). Se, per esempio, $A = \{1, 2, 3, 4\}$ i due sottoinsiemi $E = \{1, 2, 3\}$ e $F = \{2, 4\}$ sono tali che né $E \subseteq F$, né $F \subseteq E$. Dunque essi sono *inconfrontabili*. Due sottoinsiemi E ed F *disgiunti*, cioè tali che $E \cap F = \emptyset$ non solo sono inconfrontabili, ma essi si diranno *incompatibili*, poiché non esiste alcun insieme non vuoto che sia sottoinsieme di entrambi.

Dato un insieme ordinato che indicheremo con la notazione $(A, \preceq)$, diremo che un suo elemento ν è il *minimo* di A se $\forall a \in A$ vale $\nu \preceq a$. Diremo che μ è il *massimo* di A, se $\forall a \in A$ vale $a \preceq \mu$ o $\mu \succeq a$. Piú in generale, dato $E \subseteq A$, ν è il minimo di E, se $\nu \in E$ e per ogni $x \in E$ vale $\nu \preceq x$; μ è il massimo di E se $\mu \in E$ e per ogni $x \in E$ vale $x \preceq \mu$. Un elemento $\delta \in E$ si dice un elemento *massimale* di E se $\delta \in E$, ma non esiste $x \in E$ tale che $\delta \prec x$; ossia se $x \in E$ e $\delta \preceq x$ implica $x = \delta$. Analogamente si definiscono gli elementi *minimali*. Se un insieme ha massimo tale massimo è unico. Infatti da $\mu_1, \mu_2 \in E$, entrambi soddisfacenti le condizioni di massimo, segue $\mu_1 \preceq \mu_2$ e $\mu_2 \preceq \mu_1$. Ma ciò implica $\mu_1 = \mu_2$. Analogamente per il minimo di un insieme ordinato: se esiste è unico. Ci possono essere però piú elementi massimali (o minimali). Se $A = \{a, b, c, d, e\}$ con $a \prec b$, $a \prec c$, $b \prec d$, $c \prec e$, $d \prec e$ e non vale alcun'altra relazione d'ordine stretto, allora $E = \{b, c, d\}$ ha b e c come elementi minimali, c e d come elementi massimali, ma non c'è né massimo né minimo. Nella figura le relazioni d'ordine sono rappresentate da una linea continua; b e c, d e c non sono confrontabili fra loro.

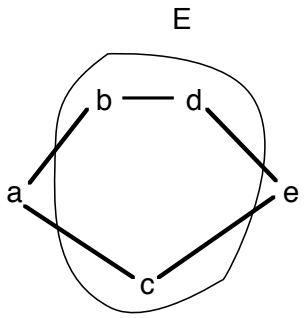

Figura 1.2: E ha elementi massimali e minimali, ma né max né min.

Diremo che $E \subset A$ è *superiormente limitato* o *maggiorato*, se esiste un elemento $k \in A$ tale che $\forall x \in E$ si ha $x \preceq k$. Analogamente, $E \subseteq A$ si dice *inferiormente limitato* o *minorato* se esiste $h \in A$ tale che $\forall x \in E$ si ha $x \succeq h$. Il numero $k \in A$ per il quale $x \preceq k$, per ogni $x \in E$, si dice una *limitazione superiore* o un *maggiorante* di E. Analogamente h si dice una *limitazione inferiore*

o un *minorante* di E. Se fra tutti i maggioranti ce n'è uno minimo, esso si dice *l'estremo superiore di* E. Analogamente il massimo minorante, quando esiste, si dice *l'estremo inferiore di* E. Questi elementi, quando esistono, si denotano con $\sup(E)$ e $\inf(E)$ rispettivamente e sono necessariamente unici. Dunque, per definizione, si ha

$$\sup(E) = \min\{k : (\forall x \in E)\ (x \preceq k)\} \quad , \tag{1.38}$$

$$\inf(E) = \max\{h : (\forall x \in E)\ (x \succeq h)\} \quad , \tag{1.39}$$

quando tali massimo e minimo esistano. Vedremo che nell'insieme ordinato dei numeri razionali $\mathbb{Q}$, non sempre un insieme superiormente (inferiormente) limitato ha estremo superiore (inferiore). Ciò invece è verificato nell'insieme ordinato dei numeri reali.

Capitolo 2

Numeri

2.1 I numeri naturali

Secondo l'opinione di molti matematici della fine dell'ottocento e degli inizi del novecento, la Matematica può pensarsi fondata sui numeri naturali. Attualmente è noto che un modello dei numeri naturali si può costruire all'interno della teoria degli insiemi, spostando così ulteriormente verso concetti più elementari i fondamenti della Matematica. Tuttavia, per i limitati scopi di questo corso, faremo l'ipotesi che i nostri fondamenti siano dati dai numeri naturali stessi, ricordando l'affermazione di Leopold Kronecker (1823 - 1891) secondo la quale "Dio creò gli interi, tutto il resto è opera dell'uomo. Julius Wilhelm Richard Dedekind (1831 - 1916) e Giuseppe Peano (1858 - 1932) riconobbero la validità di certe proposizioni fondamentali soddisfatte dai numeri naturali e, in particolare, nel 1889, Peano mostrò come tutta l'aritmetica si potesse fondare a partire da quei principi, noti ora come "Assiomi di Peano. Esporremo qui, utilizzando un sistema assiomatico sostanzialmente equivalente a quello trovato da Dedekind e Peano, alcune delle proprietà dell'insieme dei numeri naturali. Lo scopo principale è quello di abituare gli studiosi all'arte del ragionamento e della deduzione. L'insieme dei numeri naturali è l'insieme

$$\mathbb{N} = \{0, 1, 2, \ldots\} \quad ,$$

indicheremo con $\mathbb{N}^+$ l'insieme dei naturali senza lo zero: $\mathbb{N}^+ = \{1, 2, \ldots\}$. $\mathbb{N}$ è totalmente ordinato da una relazione d'ordine $\leq$ (detto ordine per grandezza dei naturali) che ha inoltre le seguenti proprietà:

(N1) Esiste in $\mathbb{N}$ un primo elemento (il suo minimo), detto *zero*; cioè $\exists 0 \in \mathbb{N}$ tale che $\forall n \in \mathbb{N}\ 0 \leq n$.

(N2) Ogni elemento di $\mathbb{N}$ ha un *immediato seguente* o *successivo*. Cioè $\forall n \in \mathbb{N}\ \exists n' \in \mathbb{N}$ tale che $n \leq n'$ e se $n \leq x < n'$, $x \in \mathbb{N}$, allora $x = n$. (Cioè, detto altrimenti, non esiste alcun elemento $x \in \mathbb{N}$ strettamente compreso tra n e n').

(N3) (**Principio d'induzione**). Sia $S \subset \mathbb{N}$. Se (a) $0 \in S$ e (b) $(\forall n \in \mathbb{N})\ ((n \in S) \Rightarrow (n' \in S))$, allora $S = \mathbb{N}$.

Al posto di (N3) si può considerare equivalentemente la proposizione

(N3') (**Principio d'induzione**). Sia $P(n)$ una proposizione dipendente da n (un predicato). Se (a) $P(0)$ è vera e se (b) $(\forall n \in \mathbb{N})$ dall'essere vera $P(n)$ segue che è vera $P(n')$, allora $P(n)$ è vera per ogni $n \in \mathbb{N}$.

Esempio 2.1.1 *Dimostrare per induzione che*

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6} \quad .$$

SVOLGIMENTO: In questo caso ha senso partire non da $n = 0$ ma da $n = 1$. Il predicato $P(n)$ è "$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$. Si verifica che $P(1)$ è vera: $1 = 1^2 = \frac{1\cdot(1+1)\cdot(2\cdot1+1)}{6} = 1$. Diamo per scontato che sia $n' = n + 1$, cosa che verificheremo successivamente. Supponiamo che valga $1^2+2^2+\ldots+n^2 = \frac{n(n+1)(2n+1)}{6}$ e computiamo $1^2+2^2+\ldots+n^2+(n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{n+1}{6} \cdot [n(2n+1) + 6(n+1)] = \frac{n+1}{6}(2n^2 + 7n + 6) = \frac{(n+1)(n+2)(2n+3)}{6}$. Dunque anche $P(n+1)$ è vera. Per il principio d'induzione $P(n)$ è vera per ogni $n \in \mathbb{N}^+$. $\square$

Come si è visto nell'esempio precedente, la "base alla quale si applica il principio d'induzione, non sempre è $n = 0$. Talvolta si prende come base un valore $n_0 > 0$. Allora il Principio d'induzione viene enunciato come segue: se $P(n_0)$ è vero e se $P(n)$ vero implica $P(n')$ vero per ogni $n \geq n_0$, allora $P(n)$ è vero per ogni $n \geq n_0$.

Mostriamo ora come l'uso degli assiomi alla Peano permetta di dimostrare alcune delle più importanti proprietà aritmetiche di $\mathbb{N}$. Un notevolissimo risultato è dato dal seguente

Teorema 2.1.1 *Ogni sottoinsieme non vuoto di* $\mathbb{N}$ *ha un minimo.*

DIMOSTRAZIONE: Sia $M \subset \mathbb{N}$, $M \neq \emptyset$. Consideriamo la proposizione dipendente da $n \in \mathbb{N}$, $P(n)$: "$(\forall x \in M)\ (x \geq n)$". Ovviamente $P(0)$ è vera (ogni numero naturale è ≥ 0, e quindi anche quelli di M). Tuttavia è facile verificare che la proposizione non può essere vera per ogni $n \in \mathbb{N}$. Infatti se $m \in M$ (poiché $M \neq \emptyset$ qualche elemento c'è) non può valere $P(m')$. Non può essere $(\forall x \in M)\ (x \geq m')$: infatti $m \in M$ e vale $m < m'$. Dunque non può essere che per ogni $n \in \mathbb{N}$ $P(n)$ vera implichi $P(n')$ vera. Esiste perciò un $k \in \mathbb{N}$ tale che $P(k)$ è vera, ma $P(k')$ è falsa. Leggiamo cosa ciò significhi.

$P(k)$ vera significa che $\forall x \in M$ è $k \leq x$. $P(k')$ falsa significa che la negazione della proposizione $P(k')$ è vera, cioè che esiste qualche $x^\star \in M$ tale che $x^\star < k'$. Dunque esiste $x^\star \in M$ tale che

$$k \leq x^\star < k' \quad .$$

Ma da (N2) segue che $x^\star = k$, con $x^\star \in M$. Dunque $k \in M$ e $\forall x \in M$ si ha $k \leq x$. Cioè k è il minimo di M. □

Un insieme ordinato nel quale ogni sottinsieme non vuoto abbia minimo, si dice un insieme *bene ordinato* e l'ordine si dice un *buon ordine*. Abbiamo verificato che $\mathbb{N}$ è bene ordinato dall'ordine per grandezza. Gli insiemi bene ordinati sono in corrispondenza biunivoca con quelli che nella teoria degli insiemi si dicono i *numeri ordinali*. Poiché $\mathbb{N}$ è bene ordinato esso è un numero ordinale, il minimo degli ordinali infiniti; $\mathbb{N}$ pensato come ordinale si suole indicare con il simbolo ω_0. Anche gli elementi di $\mathbb{N}$ sono numeri ordinali, i numeri ordinali finiti. Più avanti faremo qualche accenno alla *cardinalità* e ai *numeri cardinali*. Nel caso finito i numeri ordinali e cardinali coincidono. In generale invece, i numeri ordinali infiniti sono cosa diversa dai numeri cardinali infiniti.

In modo analogo si dimostra il seguente

Teorema 2.1.2 *Se $M \subset \mathbb{N}$ è non vuoto e superiormente limitato, allora ha massimo.*

SUGGERIMENTO: Conviene ricordare che un insieme M si dice superiormente limitato in $\mathbb{N}$ se esiste $k \in \mathbb{N}$ tale che $\forall x \in M$ è $x \leq k$. Si consideri inoltre la proposizione

$$P(n): \text{ “esiste un } x \in M \text{ tale che } x \geq n'' \quad . \square$$

Il principio d'induzione, con gli altri assiomi opportunamente utilizzati, permette di definire le operazioni in $\mathbb{N}$ e di dimostrare le loro ben note proprietà aritmetiche.

ADDIZIONE

Siano a, b numeri naturali; definiamo

$$\begin{cases} a+0 &= a \\ a+b' &= (a+b)' \quad . \end{cases} \tag{2.1}$$

MOLTIPLICAZIONE

Siano a, b numeri naturali; definiamo

$$\begin{cases} a \cdot 0 &= 0 \\ a \cdot b' &= a \cdot b + a \quad . \end{cases} \tag{2.2}$$

In particolare, se indichiamo $0' = 1$, abbiamo dalla definizione di addizione $a + 1 = a + 0' = (a + 0)' = a'$. Cioè, come avevamo già annunciato (e come è intuitivamente noto) $\forall a \in \mathbb{N}$ si ha $a' = a + 1$.

Si può dimostrare, usando opportunamente il principio d'induzione, che valgono le seguenti proprietà dell'addizione:

ASSOCIATIVA:

$$(\forall a, b, c \in \mathbb{N}) \;\; a + (b + c) = (a + b) + c \quad ,$$

COMMUTATIVA:

$$(\forall a, b \in \mathbb{N}) \;\; a + b = b + a \quad .$$

Per la moltiplicazione valgono le seguenti proprietà:

ASSOCIATIVA:

$$(\forall a, b, c \in \mathbb{N}) \;\; a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad ,$$

DISTRIBUTIVA DELLA MOLTIPLICAZIONE RISPETTO ALL'ADDIZIONE

$$(\forall a, b, c \in \mathbb{N}) \;\; a \cdot (b + c) = a \cdot b + a \cdot c \quad ,$$

COMMUTATIVA:

$$(\forall a, b \in \mathbb{N}) \;\; a \cdot b = b \cdot a \quad .$$

Si noti che le proprietà sono elencate nell'ordine nel quale conviene siano dimostrate, nel senso che, per dimostrare la commutatività dell'addizione, si fa uso dell'associatività, e così via.

Si possono pure dimostrare le seguenti proposizioni

"Se $a + c = b + c$, allora $a = b$.

Cioè vale la legge di cancellazione a destra (e quindi anche a sinistra).

"Se $a \leq b$, $\exists! c \in \mathbb{N}$ tale che $a + c = b$.

c si dice la differenza di b e a. La *sottrazione* non la riterremo un'operazione in $\mathbb{N}$ poiché non è definita per ogni coppia di numeri naturali, ma solo per quelli per i quali è $a \leq b$. In questo caso il risultato si denota con $c = b - a$.

2.1.1 Divisione in $\mathbb{N}$

Si dimostra il seguente

Teorema 2.1.3 *Per ogni coppia di numeri naturali a, b, con $b \neq 0$, esiste una sola coppia di naturali (q, r) tali che*

$$\begin{cases} a &= q \cdot b + r \\ r &< b. \end{cases} \tag{2.3}$$

Il numero q si dice il quoziente *e r si dice il* resto *della divisione euclidea.*

DIMOSTRAZIONE: Sia $b \neq 0$, allora l'insieme dei multipli di b

$$0 < b < 2 \cdot b < \ldots < n \cdot b < \ldots$$

non ha massimo e quindi non può essere superiormente limitato. Esiste perciò $q \in \mathbb{N}$ tale che

$$q \cdot b \leq a < (q+1) \cdot b = q \cdot b + b \quad .$$

Tra $q \cdot b$ e $q \cdot b + b$ sono compresi i numeri: $q \cdot b < q \cdot b + 1 < \ldots < q \cdot b + (b-1)$. a è uno di questi numeri e quindi

$$a = q \cdot b + r$$

con $r \in \{0, 1, \ldots, b-1\}$.

Dimostriamo ora l'unicità della coppia. Siano (q, r) e (q', r') tali che

$$a = q \cdot b + r = q' \cdot b + r' \quad ,$$

con $r < b$, $r' < b$. Supponiamo, per esempio, $q \leq q'$, $q' = q + h$. Allora abbiamo

$$q' \cdot b + r' = q \cdot b + r \,. \text{ Cioè}$$

$$q \cdot b + h \cdot b + r' = q \cdot b + r \,.$$

Ma allora, cancellando a sinistra $q \cdot b$, si trova

$$h \cdot b + r' = r \quad .$$

Se fosse $h \neq 0$, non potrebbe accadere che $r < b$. Deve perciò essere $h = 0$ e quindi $q = q'$ e inoltre $r = r'$. □

Se $r = 0$, il numero b si dice un *divisore* di a e a si dice un *multiplo* di b. Ogni numero naturale è divisibile per 1 e per sé stesso. Un numero $p > 1$ divisibile **solo** per 1 e per sé stesso, si dice un *numero primo.*

Teorema 2.1.4 *Esistono infiniti numeri primi.*

DIMOSTRAZIONE: Siano dati i numeri primi $2, 3, 5, \ldots, p$. Consideriamo il numero

$$n = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p + 1 \quad .$$

Questo numero non è divisibile per $2, 3, 5, \ldots, p$ (infatti il resto della divisione è 1). Dunque ci sono due possibilità: o n è primo o ha un fattore primo q diverso da $2, 3, 5, \ldots, p$. □

Teorema 2.1.5 [Unicità della scomposizione in fattori]. *Ogni numero naturale > 1 è rappresentabile in modo essenzialmente unico (cioè a meno di una permutazione dei fattori) come prodotto di numeri primi:*

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s} \quad .$$

DIMOSTRAZIONE: Dato $n > 1$, esso è primo oppure è composto: $n = m_1 \cdot m_2$, con $m_1, m_2 > 1$. Se, per ipotesi induttiva, supponiamo che ogni numero naturale $< n$ sia rappresentabile in modo unico come prodotto di fattori primi, allora certamente n è rappresentabile come prodotto di fattori primi. Mostriamo ora che c'è un'essenziale unicità.

Tra i fattori primi di n, sia p il minimo (ricordiamo che ogni insieme non vuoto di naturali ha un minimo). Allora è $n = p \cdot n_1$. Per $n_1 < n$ vale l'unicità della scomposizione e quindi, fra le decomposizioni in fattori primi aventi il fattore primo p, ce n'è sostanzialmente una sola.

Supponiamo che possa esserci una scomposizione che non contiene il fattore primo p. Sia allora $n = p^\star \cdot n_2$, essendo necessariamente $p^\star > p$ (ma $p^\star$ minimo nell'altra fattorizzazione). Perciò $n_2 < n_1$. Sia $h = n - p \cdot n_2 < n$. È $h = p \cdot n_1 - p \cdot n_2 = p \cdot (n_1 - n_2)$, ma anche $h = p^\star \cdot n_2 - p \cdot n_2 = (p^\star - p) \cdot n_2$. Allora il numero $h < n$ avrebbe due fattorizzazioni diverse: $h = p \cdot (n_1 - n_2) = (p^\star - p) \cdot n_2$; la prima contiene il fattore primo p, mentre la seconda non lo contiene (infatti $p^\star - p$ non può essere divisibile per p). Ma ciò va contro l'ipotesi induttiva. □

2.1.2 Rappresentazione dei numeri naturali in una base $B > 1$

Teorema 2.1.6 *Sia B un numero naturale > 1. Per ogni numero naturale $A > 0$ esiste un naturale n tale che A si scrive in modo unico come*

$$A = a_n \cdot B^n + a_{n-1} \cdot B^{n-1} + \ldots + a_1 \cdot B + a_0 \quad .$$

con $0 \leq a_k \leq B - 1, k = 0, 1, \ldots, n$ e $a_n > 0$.

DIMOSTRAZIONE: Se $A = 1, 2, \ldots, B - 1$, ovviamente ciò vale. Facciamo l'ipotesi induttiva che la proposizione sia vera per ogni numero naturale $< A$.

Sia dunque $A \geq B$. Dividiamo A per B. Esiste una sola coppia (q, r), con $r < B$ tale che

$$A = q \cdot B + r \quad .$$

Poiché $B > 1$ è $q < A$. Allora per l'ipotesi induttiva fatta esiste $m \in \mathbb{N}$ tale che $q = a'_m \cdot B^m + a'_{m-1} \cdot B^{m-1} + \ldots + a'_0$, essendo i coefficienti $a'_m, a'_{m-1}, \ldots, a'_0$ univocamente determinati e $a'_m > 0$. Sostituendo

$$A = (a'_m \cdot B^m + a'_{m-1} \cdot B^{m-1} + \ldots + a'_0) \cdot B + r =$$

$$= a'_m \cdot B^{m+1} + a'_{m-1} \cdot B^m + \ldots + a'_0 \cdot B + r = a_n \cdot B^n + a_{n-1} \cdot B^{n-1} + \ldots + a_1 \cdot B + a_0 \,,$$

dove si sono fatte le posizioni $a_0 = r, a_1 = a'_0, \ldots a_{n-1} = a'_{m-1}, a_n = a'_m$, $n = m + 1$ e $a_n > 0$. Per l'ipotesi induttiva e per l'algoritmo di divisione $r = a_0$ e $a_1, \ldots, a_n$ sono univocamente determinati e $a_n > 0$. □

Esempio 2.1.2 *Si scriva il numero 4581 dato in base dieci, nelle basi sette e due.*

SVOLGIMENTO: Si consideri la seguente tabella

4581	7	3
654	7	3
94	7	2
13	7	6
1	7	1
0	-	-

La tabella si ottiene come segue: il numero sulla sinistra viene diviso per 7 (numero della colonna centrale). Nella colonna di destra si riporta il resto, mentre il quoziente viene scritto nella riga sottostante della colonna di sinistra. Il procedimento viene ripetuto finché è possibile (cioè finché non si ottiene quoziente 0). Scrivendo poi i resti nell'ordine inverso a quello in cui sono stati calcolati, si trova la rappresentazione del numero nella base voluta (sette nel nostro caso). Dunque

$$(4581)_{\text{dieci}} = (16233)_{\text{sette}} \quad .$$

Per la base due si trova

4581	2	1
2290	2	0
1145	2	1
572	2	0
286	2	0
143	2	1
71	2	1
35	2	1
17	2	1
8	2	0
4	2	0
2	2	0
1	2	1
0	-	-

e dunque

$$(4581)_{\text{dieci}} = (1000111100101)_{\text{due}} \quad .$$

La ragione per la quale il metodo sopra esposto fornisce il passaggio di base, sta nel fatto che si può scrivere in modo opportuno la rappresentazione in base B, mettendo in evidenza le successive divisioni per B con resto:

$$A = (a_n \cdot B^{n-1} + a_{n-1} \cdot B^{n-2} + \ldots + a_1)B + a_0 =$$

$$= (\ldots(((a_n \cdot B + a_{n-1}) \cdot B + a_{n-2}) \cdot B \ldots) \cdot B + a_1) \cdot B + a_0 \quad .$$

Una verifica dell'algoritmo assegnato si ottiene, tenendo conto della scrittura posizionale

$$4581 = 1 \cdot 7^4 + 6 \cdot 7^3 + 2 \cdot 7^2 + 3 \cdot 7 + 3 = 2401 + 6 \cdot 343 + 2 \cdot 49 + 3 \cdot 7 + 1 \quad .$$

Analogamente per la base due. Il passaggio dalla base due alle basi quattro, otto, sedici,... si può fare agevolmente, raggruppando le cifre dei numeri scritti in base due, a due a due, a tre a tre, a quattro a quattro, ... a partire da destra (tenendo conto che $2^2 = 4, 2^3 = 8, 2^4 = 16 \ldots$). Così si trova

$$(1000111100101)_{\text{due}} = (1|00|01|11|10|01|01)_{\text{due}} = (1013211)_{quattro} \quad ,$$

(infatti $(00)_{\text{due}} = (0)_{\text{quattro}}$, $(01)_{\text{due}} = (1)_{\text{quattro}}$, $(10)_{\text{due}} = (2)_{\text{quattro}}$, $(11)_{\text{due}} = (3)_{\text{quattro}}$); analogamente, prendendo le cire a tre a tre:

$$(1000111100101)_{\text{due}} = (1|000|111|100|101)_{\text{due}} = (10745)_{otto} \quad .$$

Per scrivere un numero in base sedici servono ulteriori simboli per rappresentare le cifre da dieci a quindici. Solitamente, per questo scopo, si usano i simboli A (dieci), B (undici), C (dodici), D (tredici), E (quattordici), F (quindici).

$$(1000111100101)_{\text{due}} = (1|0001|1110|0101)_{\text{due}} = (11E5)_{sedici} \quad .$$

In generale per passare da un numero scritto in base B a uno scritto in base D, se non si conosce l'algoritmo di divisione in base B (sostanzialmente le "tabelline del B), converrà passare dalla base B alla base dieci, calcolando, in base dieci $a_n \cdot B^n + \ldots + a_1 \cdot B + a_0$ e quindi passare dalla base dieci alla base D con l'algoritmo di divisioni successive che si è applicato sopra.

2.2 Gli interi relativi

Come già abbiamo osservato, la sottrazione non è sempre possibile in $\mathbb{N}$. Infatti l'equazione

$$a + x = b \tag{2.4}$$

non ha soluzione in $\mathbb{N}$ se $a > b$.

Perciò è necessario ampliare l'insieme $\mathbb{N}$ dei naturali in modo da conservare, per quanto è possibile, le proprietà formali delle operazioni, fornendo nel contempo soluzione all'equazione (1.4) in tutti i casi che interessano. Tradizionalmente ciò si fa utilizzando la " teoria delle coppie . Il procedimento è probabilmente più noto nell'estensione da $\mathbb{Z}$ a $\mathbb{Q}$; perciò lo esporremo con un dettaglio maggiore nel caso in considerazione.

Prendiamo dunque l'insieme $\mathbb{N}\times\mathbb{N}$ e introduciamo in esso una relazione binaria fra coppie di numeri naturali, che si verifica subito essere una relazione d'equivalenza (soddisfa le proprietà riflessiva, simmetrica e transitiva).

$$(h,k)\sim(p,q) \text{ se } h+q=k+p, \quad h,k,p,q\in\mathbb{N} \quad .$$

Per esempio $(3,5)\sim(4,6)\sim(9,11)\ldots$. (Queste coppie rappresentano tutte il nuovo ente -2). In $\mathbb{N}\times\mathbb{N}$ si possono definire due operazioni di addizione $(h,k)+(p,q):=(h+p,k+q)$ e di moltiplicazione $(h,k)\times(p,q):=(h\cdot p+k\cdot q, h\cdot q+k\cdot p)$. L'equivalenza è **compatibile** con le operazioni sopra definite. Precisamente se $(h,k)\sim(h',k')$ e $(p,q)\sim(p',q')$ allora $(h,k)+(p,q)\sim(h',k')+(p',q')$ e $(h,k)\times(p,q)\sim(h',k')\times(p',q')$. Ciò permette di definire le operazioni fra le classi d'equivalenza in $\mathbb{N}\times\mathbb{N}$. Dunque, posto

$$[h,k]=\{(h',k'){:}\,(h',k')\sim(h,k)\} \quad ,$$

potremo definire

$$[h,k]+[p,q]:=[h+p,k+q] \text{ e } [h,k]\times[p,q]:=[h\cdot p+k\cdot q, h\cdot q+k\cdot p] \ .$$

Infatti, grazie alla compatibilità fra equivalenza e operazioni, la classe d'equivalenza della somma o del prodotto non dipende dalla scelta del rappresentante all'interno di ogni classe d'equivalenza.

Si verifica facilmente che $(h,k)\sim(h+c,k+c)$. Perciò le coppie (h,k) si possono ridurre a tre forme tipiche a seconda che sia $h>k$ oppure $h=k$ oppure $h<k$. Precisamente, se $h>k$, cioè se $\exists c\in\mathbb{N}^+=\mathbb{N}\setminus\{0\}$ tale che $h=k+c$, si ottiene $(h,k)=(k+c,k)\sim(c,0)$; se $h=k$ allora $(h,k)=(h,h)\sim(0,0)$; infine, se $h<k$, ossia se $\exists c\in\mathbb{N}^+$ tale che $k=h+c$, allora $(h,k)=(h,h+c)\sim(0,c)$. Le coppie dei primi due tipi (e le rispettive classi d'equivalenza) sono in corrispondenza biunivoca con i numeri di $\mathbb{N}$ e si comportano rispetto alle operazione come i numeri naturali. Potremo perciò confondere le rispettive classi d'equivalenza con i naturali e denotarle con i simboli dei numeri stessi: $[c,0]\equiv c, c\in\mathbb{N}$. Gli unici enti "nuovi sono le classi d'equivalenza del tipo $[0,c], c\in\mathbb{N}, c>0$, che denoteremo con $-c$ e che diremo "numeri negativi. È facile verificare che la classe $[0,0]=[c,c]$ fa da elemento neutro per l'addizione, nel senso che $[h,k]+[0,0]=[h,k]$, mentre la classe $[1,0]$ è l'elemento neutro della moltiplicazione: $[h,k]\times[1,0]=[h\cdot1+k\cdot0, h\cdot0+k\cdot1]=[h,k]$. Si verifica inoltre che l'addizione e la moltiplicazione che abbiamo definito sono entrambe associative e commutative; la moltiplicazione è distributiva rispetto all'addizione. Ogni elemento di $\mathbb{Z}$ ha un simmetrico rispetto all'addizione, detto l'*opposto* dell'elemento stesso. L'opposto di $[h,k]$ è $[k,h]$. Infatti $[h,k]+[k,h]=[h+k,k+h]=[0,0]=0$. L'opposto di $a\in\mathbb{Z}$ verrà indicato con $-a$.

Ora l'equazione (1.4) ha sempre una e una sola soluzione in $\mathbb{Z}$. Infatti da $a+x=b$ segue (sommando $-a$ ai due membri e tenendo conto delle proprietà commutativa e associativa) $x=b-a$ (abbiamo indicato, come è d'uso, con $b-a$ il risultato dell'addizione $b+(-a)$). Dunque se l'equazione (1.4) ha una soluzione, essa è della forma $x=b-a$ (unicità). D'altra parte, sostituendo $b-a$ al posto di x in (1.4), si trova $a+(b-a)=a+(-a+b)=(a-a)+b=0+b=b$ (avendo applicato le proprietà commutativa e associativa). Cioè $b-a$ è la soluzione cercata (esistenza).

In $\mathbb{Z}$ si può definire una relazione d'ordine, dapprima sulle coppie e poi sulle classi (infatti è compatibile con l'equivalenza di coppie): $[h,k] < [p,q]$ se $h+q < k+p$. Ciò coincide con il dichiarare che tutti i numeri negativi vengono prima dello 0 e dei numeri positivi; per i numeri che si possono confondere con quelli di $\mathbb{N}$, l'ordine è lo stesso che c'era in $\mathbb{N}$; per i numeri negativi $-c_1 < -c_2$ se $c_2 < c_1$ $(c_1, c_2 \in \mathbb{N})$.

La relazione d'ordine è compatibile con le operazioni nel senso seguente

$$\forall a,b,c \in \mathbb{Z} \text{ se } a < b \text{ allora } a + c < b + c \ , \tag{2.5}$$

$$\forall a,b,c \in \mathbb{Z} \text{ se } a < b \text{ e } c > 0 \text{ allora } a \cdot c < b \cdot c \ . \tag{2.6}$$

Si noti che la (1.6) implica che da $a < b$ e $c < 0$ segue $a \cdot c > b \cdot c$; cioè la moltiplicazione per un numero negativo inverte l'ordine di una disuguaglianza.

Ricorderemo infine la validità del seguente

Teorema 2.2.1 [Divisione euclidea in $\mathbb{Z}$.] *Siano $a, b \in \mathbb{Z}$, con $b > 0$. Allora esiste una e una sola coppia (q, r) tale che*

$$\begin{cases} a &= q \cdot b + r \\ 0 &\leq r < b. \end{cases} \tag{2.7}$$

Dimostrazione: Omessa. □

Si verifica infine (con calcolo diretto sulle classi d'equivalenza) che $\forall a, b \in \mathbb{Z}$ se $a \cdot b = 0$ e $a \neq 0$ allora necessariamente $b = 0$. (Legge d'annullamento del prodotto).

In conclusione, i numeri interi sono un insieme $\mathbb{Z}$ dotato di due operazioni $+$ e $\times$ (indicata anche con $\cdot$) tali che valgono le seguenti proprietà

Associativa per l'addizione

$$(\forall\ a,b,c \in \mathbb{Z})\ a + (b + c) = (a + b) + c \tag{2.8}$$

Esistenza dello zero

$$(\exists\ 0 \in \mathbb{Z})\,(\forall a \in \mathbb{Z})\ a + 0 = 0 + a = a \tag{2.9}$$

Esistenza dell'opposto

$$(\forall\ a \in \mathbb{Z})\,(\exists (-a) \in \mathbb{Z})\ a + (-a) = (-a) + a = 0 \tag{2.10}$$

Commutativa per l'addizione

$$(\forall\ a, b \in \mathbb{Z})\ a + b = b + a \tag{2.11}$$

Associativa per la moltiplicazione

$$(\forall\ a, b, c \in \mathbb{Z})\ a \cdot (b \cdot c) = (a \cdot b) \cdot c \tag{2.12}$$

Distributiva

$$(\forall\ a, b, c \in \mathbb{Z})\ a \cdot (b + c) = a \cdot b + a \cdot c \tag{2.13}$$

Commutativa per la moltiplicazione

$$(\forall a, b \in \mathbb{Z})\ a \cdot b = b \cdot a \tag{2.14}$$

Esistenza dell'Unità

$$(\exists\ 1 \in \mathbb{Z})\,(\forall a \in \mathbb{Z})\ 1 \cdot a = a \cdot 1 = a \tag{2.15}$$

Ricordiamo la terminologia corrente. Un insieme dotato di un'operazione (qui indicata con $+$ e più in generale indicata con $*$) che soddisfi le condizioni da (2.8) a (2.10) si dice un **gruppo**. Se è soddisfatta anche la (2.11) il gruppo si dice **commutativo o abeliano** e l'operazione si indica solitamente con il simbolo d'addizione come qui è stato fatto. Se l'insieme è dotato di due operazioni $+$ e $\cdot$ che soddisfano le condizioni da (2.8) a (2.15) e inoltre vale la distributività anche a destra :

$$(\forall\ a, b, c)\ (b + c) \cdot a = b \cdot a + c \cdot a \quad ,$$

esso si dice un **anello**. Se la moltiplicazione è commutativa, l'anello si dice commutativo. Se esiste l'unità, l'anello si dice con unità. Se infine vale la legge d'annullamento del prodotto l'anello si dice **privo di nullifici** o **dominio d'integrità**.

Vale infine la pena di notare che in ogni anello il prodotto di un qualsiasi elemento per lo zero dà zero: $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ (grazie alla distributività); sommando ai due membri dell'uguaglianza $-(a \cdot 0)$ (questo elemento esiste in ogni anello) si trova $0 = a \cdot 0$.

In conclusione $(\mathbb{Z}, +, \cdot)$ è un anello commutativo con unità, privo di nullifici. L'insieme dei numeri pari relativi con le stesse operazioni, fornisce un esempio di anello commutativo senza unità. Le matrici quadrate con coefficienti interi, per esempio di tipo 2×2, con la somma definita elemento per elemento e il prodotto riga per colonna, forniscono un esempio di anello con unità, non commutativo nel quale **non** vale la legge d'annullamento del prodotto. Si verifica infatti che:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \ .$$

Ovviamente in questo caso la matrice zero è la matrice che ha tutti gli elementi nulli: $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

2.3 I numeri razionali

L'equazione $a \cdot x = b$, con $a \neq 0$, in generale, non ha soluzione in un anello commutativo con unità. In $\mathbb{Z}$, $a \cdot x = b$, $a \neq 0$, $a, b \in \mathbb{Z}$, ha soluzione se e solo se a divide b. Se si vuole ottenere una soluzione in ogni caso, si passa ai numeri razionali, estendendo opportunamente l'insieme numerico degli interi.

Precisamente, si considerano le coppie di elementi di $\mathbb{Z}$, con secondo elemento non nullo, che chiameremo (come comunemente si fa) "frazioni, cioè

$$F = \mathbb{Z} \times \mathbb{Z}' = \{(a, b) \colon a \in \mathbb{Z}, b \in \mathbb{Z}'\} \ ,$$

dove $\mathbb{Z}' = \mathbb{Z} \setminus \{0\}$. È più usuale indicare le coppie (a, b) con la scrittura $\frac{a}{b}$. Nell'insieme F delle frazioni si definisce una relazione binaria che è un'equivalenza:

$$\frac{a}{b} \sim \frac{p}{q} \text{ se } a \cdot q = b \cdot p \ ,$$

e si defiscono due operazioni

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{d \cdot c} \quad \text{e} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d} \ .$$

Si verifica che l'equivalenza è compatibile con le operazioni e dunque che le operazioni sono estendibili alle classi d'equivalenza, cioè all'insieme $F/\sim$, che è l'insieme cercato $\mathbb{Q}$.

Dunque, se $[\frac{a}{b}] = \{\frac{a'}{b'} \colon \frac{a'}{b'} \sim \frac{a}{b}\}$,

$$\mathbb{Q} = \{[\frac{a}{b}] \colon a \in \mathbb{Z}, b \in \mathbb{Z} \text{ e } b \neq 0\} \quad ,$$

dotato delle due operazioni

$$[\frac{a}{b}] + [\frac{c}{d}] = [\frac{a \cdot d + b \cdot c}{d \cdot c}] \quad \text{e} \quad [\frac{a}{b}] \cdot [\frac{c}{d}] = [\frac{a \cdot c}{b \cdot d}] \ .$$

Si può osservare che vale $\frac{a \cdot k}{b \cdot k} \sim \frac{a}{b}$ per ogni $k \in \mathbb{Z}$, $k \neq 0$. Tutti gli elementi del tipo $[\frac{a}{1}]$ si possono confondere con gli elementi $a \in \mathbb{Z}$. Infatti essi si comportano come gli elementi di $\mathbb{Z}$ nelle operazioni. Fondamentale è la proprietà seguente:

$$[\frac{a}{b}] \neq [\frac{0}{1}] \text{ (cioè } a \neq 0) \ \Rightarrow \quad \text{esiste l'inverso di } [\frac{a}{b}] \text{ che è } [\frac{b}{a}] \, . \tag{2.16}$$

Infatti $[\frac{a}{b}] \cdot [\frac{b}{a}] = [\frac{a \cdot b}{b \cdot a}] = [\frac{1}{1}]$. D'ora in poi gli elementi del tipo $[\frac{a}{1}]$ si denoteranno semplicemente con a; un insieme nel quale valgono le proprietà dell'anello e inoltre la (2.16) si dice un *corpo*. Se la moltiplicazione è commutativa, il corpo si dice commutativo o *campo*. È facile riconoscere che in ogni corpo vale la legge d'annullamento del prodotto: se $q \neq 0, \exists q^{-1} : q^{-1} \cdot q = 1$. Perciò, se $a \cdot b = 0$ e $a \neq 0$, moltiplicando per a^{-1} i due membri, si trova: $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$. Ma

$a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = b$ e quindi $b = 0$. Poiché $[\frac{a \cdot k}{b \cdot k}] = [\frac{a}{b}]$, osserviamo che ci si può sempre ridurre a frazioni con numeratori e denominatori primi fra loro e con denominatore > 0. Se siamo in questa condizione, diremo che $\frac{p}{q} < \frac{m}{n} (q > 0, n > 0)$ se $p \cdot n < m \cdot q$. L'ordine in $\mathbb{Q}$ è totale ed è compatibile con le operazioni, cioè

$$\forall a, b, c \in \mathbb{Q}, \quad a < b \quad \Rightarrow \quad a + c < b + c \ , \tag{2.17}$$

$$\forall a, b \in \mathbb{Q}, \quad a < b, c > 0 \quad \Rightarrow \quad a \cdot c < b \cdot c \ . \tag{2.18}$$

Cioè valgono le stesse condizioni (2.5) e (2.6) che valevano in $\mathbb{Z}$.

L'ordine in $\mathbb{Q}$ soddisfa inoltre la proprietà di essere denso in sé. Cioè, se $a < b$, $a, b \in \mathbb{Q}$, esiste $c \in \mathbb{Q}$ tale che $a < c < b$; è sufficiente prendere $c = \frac{a+b}{2}$.

2.4 I numeri reali

Fin dai tempi dei pitagorici, ci si rese conto dell'insufficienza dei numeri razionali nell'ambito dell'operazione di misurazione di un segmento di retta rispetto a un segmento assegnato come unità. L'esempio tipico è la verifica che la diagonale di un quadrato è incommensurabile rispetto al lato del quadrato stesso. In termini algebrici ciò si esprime dimostrando che l'equazione

$$x^2 = 2$$

non ha soluzioni razionali. Infatti, se per assurdo ci fosse una soluzione razionale $p = \frac{m}{n}$, con m e n primi fra loro, allora $\dfrac{m^2}{n^2} = 2$ e quindi

$$m^2 = 2 \cdot n^2 \quad .$$

In tale caso m^2 e perciò m dovrebbero essere pari: $m = 2 \cdot k$, $k \in \mathbb{N}$. Ma allora $4 \cdot k^2 = 2 \cdot n^2$ e quindi n^2 (e perciò n) dovrebbe essere pari. Dunque m ed n, supposti primi fra loro, dovrebbero essere entrambi pari e quindi avere un fattore comune 2. È una contraddizione.

Per descrivere la situazione d'insufficienza dei numeri razionali in modo più chiaro e costruttivo, presentiamo la situazione che si verifica in $\mathbb{Q}$. Diciamo che due classi di numeri (per esempio razionali) sono *separate* se $A, B \neq \emptyset$ e $\forall a \in A, \forall b \in B$ risulta $a \leq b$. Un elemento c del campo numerico in considerazione si dice *elemento di separazione* delle classi A e B se

$$\forall a \in A, \forall b \in B \qquad a \leq c \leq b \quad .$$

In $\mathbb{Q}$ esistono due classi $A = \{r \in \mathbb{Q} \colon r \geq 0, r^2 < 2\}$ e $B = \{s \in \mathbb{Q} \colon s \geq 0, s^2 > 2\}$, che sono separate, ma che non hanno alcun elemento di separazione in $\mathbb{Q}$. Infatti da $r^2 < s^2$, essendo tutti e due numeri positivi, segue $r < s$. Dunque le classi sono separate. Non vi può essere in $\mathbb{Q}$ elemento di separazione, come verificheremo meglio nel seguito. Infatti dimostreremo, in un caso più generale, che in questa situazione la classe A non ha massimo e la classe B non ha minimo. L'elemento di separazione allora non potrebbe stare né in A né in B e quindi dovrebbe essere $c^2 = 2$, cosa che non è possibile per un elemento di $\mathbb{Q}$.

Ipotizzeremo allora l'esistenza di un corpo numerico commutativo ordinato $\mathbb{R}$ soddisfacente le proprietà da (2.8) a (2.15), l'esistenza del reciproco per ogni $a \in \mathbb{R}, a \neq 0$, la compatibilità tra operazioni e ordine analoghe a (2.5) e (2.6) e soddisfacente inoltre il seguente Postulato o Principio di Dedekind

(D) Se A, B sono separate, allora $\exists c \in \mathbb{R}$ che è elemento di separazione delle classi.

Un corpo commutativo ordinato che soddisfa la condizione (D) si dice un corpo ordinato *completo*. Da quanto sopra si è detto, $\mathbb{Q}$ è un corpo commutativo ordinato **non** completo. Si può dimostrare che esiste un unico corpo commutativo ordinato completo che contenga come sottocorpo quello dei

razionali: è il corpo dei numeri reali. Un modello dei numeri reali è fornito dalle scritture decimali limitate e illimitate, periodiche e non periodiche.

Passiamo ora in rassegna le più importanti proprietà del corpo (o campo) reale $\mathbb{R}$.

2.4.1 L'estremo superiore

Diremo che un sottoinsieme non vuoto $A \subset \mathbb{R}$ è *superiormente limitato* o *maggiorato* se esiste un numero reale $k \in \mathbb{R}$ tale che

$$(\forall a \in A)\ (a \leq k) \quad .$$

Un valore $k \in \mathbb{R}$ siffatto si dice un *maggiorante* o una *limitazione superiore* di A. La minima limitazione superiore di A, se esiste, si dice l'*estremo superiore* di A e si indica con $\sup A$.

Ebbene è fondamentale il seguente

Teorema 2.4.1 [Esistenza dell'estremo superiore]. *Se A è un sottoinsieme non vuoto e superiormente limitato di $\mathbb{R}$ allora esiste in $\mathbb{R}$ la minima limitazione superiore di A. Cioè esiste* $\sup A \in \mathbb{R}$.

DIMOSTRAZIONE: Indichiamo con $K = \{k \in \mathbb{R}: k \text{ è una limitazione superiore di } A\}$. Per ipotesi $K \neq \emptyset$ e $A \neq \emptyset$. Dunque per ogni $k \in K$ e per ogni $a \in A$ abbiamo $a \leq k$. Allora A e K sono due classi separate. Esiste, poiché vale (D), un elemento c che separa le due classi. Cioè vale

$$\forall a \in A, \forall k \in K, \quad a \leq c \leq k \quad .$$

La prima disuguaglianza dice che c è una limitazione superiore di A, cioè $c \in K$; la seconda dice che c è la minima limitazione superiore di A. In un insieme totalmente ordinato come $\mathbb{R}$ (o $\mathbb{Q}$), il minimo o il massimo di un insieme, se esistono, sono unici. (Infatti se m_1 e m_2 sono minimi di un insieme M, vale, in particolare, $m_1 \leq m_2$, ma anche $m_2 \leq m_1$. Per l'antisimmetria della relazione d'ordine, segue che $m_1 = m_2$).

Dunque esiste uno e un solo minimo di K nell'insieme $\mathbb{R}$ dei numeri reali. Cioè esiste ed è unico l'estremo superiore di A: $\sup A$. $\square$

Per la comodità d'uso è utile tenere presente la seguente caratterizzazione dell'estremo superiore di un insieme non vuoto A.

Teorema 2.4.2 [Proprietà caratteristiche del sup]. *Sia A un insieme non vuoto e superiormente limitato di $\mathbb{R}$. Un numero $\lambda \in \mathbb{R}$ è l'estremo superiore di A se e solo se soddisfa le seguenti proprietà*

1. $(\forall a \in A) \quad (a \leq \lambda)$;

2. $(\forall \varepsilon > 0) \quad (\exists \overline{a} \in A)\ \overline{a} > \lambda - \varepsilon.$

DIMOSTRAZIONE: Sia $\emptyset \neq A \subset \mathbb{R}$ e sia A superiormente limitato. Allora, per il teorema precedente, esiste $\sup A$. Il numero $\sup A \in \mathbb{R}$ è una limitazione superiore di A, dunque soddisfa la condizione 1. Ma è anche la minima limitazione superiore e, quindi nessun numero $< \sup A$ può essere una limitazione superiore di A: ogni numero $< \sup A$ deve essere superato da qualche elemento di A; ma questo è quanto afferma la condizione 2.

Viceversa, supponiamo che un numero $\lambda \in \mathbb{R}$ soddisfi le condizioni 1. e 2. Allora la 1. ci dice che questo numero è una limitazione superiore di A, mentre la 2. ci dice che è la minima fra le limitazioni superiori. Dunque $\lambda = \sup A$. $\square$

Osservazione 2.4.1 *Analogamente a quanto si è fatto per l'estremo superiore, si dimostra che se* $\emptyset \neq A \subset \mathbb{R}$ *è* inferiormente limitato*, o* minorato*, cioè se esiste* $h \in \mathbb{R}$ *tale che* $\forall a \in A$ *vale* $h \leq a$*, allora esiste la* massima limitazione inferiore *che si dice l'*estremo inferiore *di* A*, indicato da* $\inf A$*. Le proprietà caratteristiche dell'*inf *sono le seguenti: un numero reale* μ *è estremo inferiore di* A *non vuoto e inferiormente limitato se e solo se valgono*

1. $(\forall a \in A) \quad (a \geq \mu)$*;*

2. $(\forall \varepsilon > 0) \quad (\exists \overline{a} \in A)\ \overline{a} < \mu + \varepsilon.$

Osservazione 2.4.2 *Se* $\emptyset \neq A \subset \mathbb{R}$ **non** *è superiormente limitato, cioè, se* $\forall k \in \mathbb{R}$*,* $\exists a \in A$ *tale che* $a > k$*, allora si dice in modo convenzionale, che* $\sup A = +\infty$*. Analogamente, se* A *non è inferiormente limitato, allora, convenzionalmente,* $\inf A = -\infty$*. Scrivere* $\sup A < +\infty$ *significa dire che* A *è superiormente limitato;* $\inf A > -\infty$ *significa che* A *è inferiormente limitato.*

Osservazione 2.4.3 *Si noti che* $+\infty$ *e* $-\infty$ **non** *sono numeri reali !*

Osservazione 2.4.4 *Noi abbiamo fatto discendere l'esistenza di* $\sup A$ *dal postulato di Dedekind. Se ammettiamo che ogni insieme non vuoto e superiormente limitato di* $\mathbb{R}$ *abbia un estremo superiore, allora si può dedurre che vale la proprietà* (D)*. Dunque il postulato di Dedekind e l'esistenza dell'estremo superiore sono proprietà equivalenti in* $\mathbb{R}$*. Analogamente sono equivalenti l'esistenza dell'estremo superiore e dell'estremo inferiore. Dimostriamo, per esempio, che se ogni insieme inferiormente limitato non vuoto ha estremo inferiore, allora ogni coppia di classi separate* A *e* B *ha un elemento di separazione. Infatti* B *è inferiormente limitata (per esempio da tutti gli elementi di* A*) e non vuota. Perciò esiste* $\nu = \inf B$*. Per definizione* $\nu \leq b$*, per ogni* $b \in B$*. Inoltre* ν *è la massima delle limitazioni inferiori e gli elementi* $a \in A$ *sono limitazioni inferiori. Perciò vale* $a \leq \nu$*, per ogni* $a \in A$*. In conclusione* ν *è compreso tra le due classi.*

Le affermazioni che non sono già state dimostrate nell'osservazione precedente possono costituire un ottimo esercizio per verificare la comprensione dell'argomento [1].

2.4.2 La proprietà di Archimede

Si dimostra quanto segue

Teorema 2.4.3 *Siano a e b due numeri reali > 0. Allora esiste un numero naturale $n > 0$ tale che $n \cdot a > b$.*

DIMOSTRAZIONE: Se $0 < b < a$, basta prendere $n = 1$. Supponiamo dunque $0 < a < b$. Consideriamo l'insieme dei multipli di a:

$$A = \{n \cdot a : n \in \mathbb{N}^+\} \quad .$$

Osserviamo che non può essere $n \cdot a \leq b \ , \forall n \in \mathbb{N}^+$. Se così fosse, esisterebbe $c = \sup A$ e quindi varrebbe

1. $n \cdot a \leq c \ , \forall n \in \mathbb{N}^+$
2. $\forall \varepsilon > 0, \ \exists \overline{n} \in \mathbb{N}^+$ tale che $\overline{n} \cdot a > c - \varepsilon$.

Preso, in particolare, $\varepsilon = a > 0$, avremmo $\overline{n} \cdot a > c - a$, cioè $(\overline{n} + 1) \cdot a > c$, contro la validità della condizione 1. Dunque esiste qualche valore $n > 1$ tale che $n \cdot a > b$. $\square$

2.4.3 Il valore assoluto

Si definisce il *valore assoluto* di un numero reale x come segue

$$|x| = \begin{cases} x, & \text{se } x \geq 0, \\ -x, & \text{se } x < 0. \end{cases} \tag{2.19}$$

Per il valore assoluto valgono le seguenti proprietà.

$$| - a| = |a|; ||a|| = |a|; |a \cdot b| = |a| \cdot |b| \quad .$$

Inoltre vale la disuguaglianza triangolare

$$|a + b| \leq |a| + |b| \quad , \tag{2.20}$$

[1] Infine si può osservare che se $A = \emptyset$ si può coerentemente affermare che $\sup A = -\infty$ e che $\inf A = +\infty$ (ma si tratta di ... stranezze da matematici, che si possono anche trascurare per il momento)!

e anche

$$||a| - |b|| \leq |a - b| \quad . \tag{2.21}$$

Per dimostrare la (2.20) non c'è altro da fare che verificare i vari casi possibili: $a \geq 0$ e $b \geq 0$; $a > 0$, $b < 0$ ma $a + b \geq 0$; $a > 0$, $b < 0$ ma $a + b < 0$; $a < 0$ e $b < 0$. Infine ci sono i casi nei quali a e b si scambiano i segni. Se $a \geq 0$ e $b \geq 0$, allora $a + b \geq 0$ e quindi $|a + b| = a + b = |a| + |b|$. Analogamente se $a < 0$ e $b < 0$ allora $a+b < 0$ e quindi $|a+b| = -(a+b) = (-a)+(-b) = |a|+|b|$. La disuguaglianza vale come uguaglianza. Se $a > 0$, $b < 0$ ma $a + b \geq 0$, si ha $|a + b| = a + b < a + (-b) = |a| + |b|$ (b è negativo, e quindi $-b$ è positivo). Infine, se $a > 0$, $b < 0$ ma $a+b < 0$, si ha $|a + b| = -(a + b) = -a + (-b) < |a| + |b|$. Infatti, essendo $a > 0$ è $-a < |a| = a$, mentre $-b = |b|$, essendo $b < 0$. Scambiando a e b, si tiene conto degli altri due casi. Dimostrata che sia la (1.20), si trova:

$$|a| = |a - b + b| \leq |a - b| + |b| \quad \text{cioè} \quad |a| - |b| \leq |a - b| \, .$$

Analogamente

$$|b| = |b - a + a| \leq |b - a| + |a| \quad \text{cioè} \quad |b| - |a| \leq |b - a| \, .$$

Ossia

$$|a| - |b| \geq -|b - a| = -|a - b| \quad .$$

In definitiva

$$-|a - b| \leq |a| - |b| \leq |a - b| \quad \text{ossia} \quad ||a| - |b|| \leq |a - b| \, .$$

2.4.4 Densità di $\mathbb{Q}$ in $\mathbb{R}$

Vale il seguente

Teorema 2.4.4 *$\mathbb{Q}$ è denso in $\mathbb{R}$. Ossia, dato $a \in \mathbb{R}$ e $\varepsilon > 0$, $\varepsilon \in \mathbb{R}$, esiste $q \in \mathbb{Q}$ tale che*

$$a - \varepsilon < q < a + \varepsilon \quad \text{cioè} \quad |a - q| < \varepsilon \quad .$$

Dimostrazione: Cominciamo a supporre $a \geq 0$. Allora esiste certamente un numero naturale m tale che $m \leq a < m + 1$. (Per verificare ciò si può ricorrere ancora alla proprietà di Archimede: presi i numeri reali $a \geq 0$ e 1 esiste certamente un numero naturale $n \geq 1$ tale che $n \cdot 1 > a$. Preso il minimo di tali numeri (si sa che il minimo esiste) e scritto tale minimo nella forma $m+1$, si ottiene $m \leq a < m + 1$). Sia poi dato $\varepsilon > 0$. Se $\varepsilon \geq 1$, vale $a - \varepsilon < m \leq a < m + 1 \leq a + \varepsilon$ e dunque $q = m$ è il numero cercato tale che $a - \varepsilon < q < a + \varepsilon$. Sia poi $0 < \varepsilon < 1$. Esiste, per Archimede, $k \in \mathbb{N}^+$ tale che $k \cdot \varepsilon > 1$ e quindi $\dfrac{1}{k} < \varepsilon$. Consideriamo i numeri del tipo $n_h = m + h \cdot \dfrac{1}{k}$. Per $h = 0$ si ha $n_0 = m \leq a$; per $h = k$ vale $n_k = m + 1 > a$. Dunque esiste qualche $h^\star$ tale che $n_{h^\star} \leq a < n_{h^\star+1} = n_{h^\star} + \dfrac{1}{k} < a + \varepsilon$. Preso $p = n_{h^\star+1}$, esso è un numero razionale tale che $a < p < a + \varepsilon$ e, a maggior ragione, $a - \varepsilon < p < a + \varepsilon$. Quindi

$$|a - p| < \varepsilon \quad .$$

Se $a < 0$, $-a > 0$; dunque esiste un numero razionale q tale che $|-a-q| < \varepsilon$. Allora, se $p = -q$ si trova $|-a+p| = |a-p| < \varepsilon$. $\square$

Osserviamo che, se $c < d$ con $c, d \in \mathbb{R}$, posto $a = \dfrac{c+d}{2}$ e $\varepsilon = \dfrac{d-c}{2}$, si può affermare che vale il teorema di densità di $\mathbb{Q}$ in $\mathbb{R}$ nella forma seguente

Teorema. *Se c, d sono numeri reali e $c < d$, allora esiste un numero razionale r tale che $c < r < d$.*
$\square$

Possiamo infine osservare che fra due numeri reali qualsiasi c'è sempre un numero irrazionale. Infatti, siano $a < b$ due numeri reali. Per la densità di $\mathbb{Q}$ in $\mathbb{R}$, esiste un numero razionale r tale che $a < r < b$ e, per la stessa ragione, ne esiste un altro $s \in \mathbb{Q}$ tale che $a < r < s < b$. Allora il numero $c = r + \dfrac{s-r}{\sqrt{2}}$ è certamente irrazionale e vale $a < r < c < s < b$, e quindi, a maggior ragione, $a < c < b$.

2.4.5 Radice n-esima di un numero reale

Abbiamo il seguente

Teorema 2.4.5 *Sia $a \geq 0$ un numero reale. Sia n un numero naturale ≥ 1. L'equazione*

$$x^n = a$$

ha una e una sola soluzione reale ≥ 0.

Dimostrazione: Osserviamo che la funzione $f(x) = x^n$ è crescente su $\mathbb{R}^+$. Cioè, se $0 < x_1 < x_2$ e $n \geq 1$, allora vale $0 < x_1^n < x_2^n$.

(Se qualcuno ne dubitasse, ciò si può dimostrare per induzione. Per n=1, ovviamente, la proposizione vale: $0 < x_1 < x_2 \Rightarrow 0 < (x_1)^1 < (x_2)^1$. Supponiamo che la proposizione valga per n e dimostriamo che vale anche per $n+1$. Dunque valga $0 < x_1 < x_2 \Rightarrow 0 < (x_1)^n < (x_2)^n$. Moltiplicando i due membri della disuguaglianza $0 < (x_1)^n < (x_2)^n$ per $x_1 > 0$, si trova (*) $0 < (x_1)^{n+1} < (x_2)^n \cdot x_1$, mentre moltiplicando i due membri della disuguaglianza $0 < x_1 < x_2$ per $(x_2)^n > 0$, si trova (**) $0 < x_1 \cdot (x_2)^n < (x_2)^{n+1}$. Confrontando le due disuguaglianze (*) e (**), per transitività, si ottiene finalmente $0 < (x_1)^{n+1} < (x_2)^{n+1}$. Per induzione vale dunque $0 < x_1 < x_2 \Rightarrow 0 < (x_1)^n < (x_2)^n \ \forall\, n \in \mathbb{N}^+$).

Consideriamo ora le due classi

$$C = \{c \in \mathbb{R} \colon c \geq 0, c^n < a\} \quad \text{e} \quad D = \{d \in \mathbb{R} \colon d \geq 0, d^n > a\} \ .$$

Le due classi C e D sono non vuote e separate. Infatti, $0 \in C$ e $(a+1) \in D$; inoltre per ogni $c \in C$ e per ogni $d \in D$ si ha $c^n < a < d^n$ e quindi $c < d$. Per Dedekind esiste un elemento di

separazione $\alpha \in \mathbb{R}$ tale che $\forall c \in C\,, \forall d \in D\; c \leq \alpha \leq d$. Possiamo chiederci se è $\alpha \in C$ oppure $\alpha \in D$. Mostreremo che nessuna di queste ipotesi vale e che quindi non vale né $\alpha^n < a$, né $\alpha^n > a$, restando quindi la sola alternativa che sia $\alpha^n = a$. Per verificare questo fatto dimostreremo che la classe C non ha massimo e che la classe D non ha minimo.

Sia $c \in C$, dimostriamo che esiste $c_1 > c$, tale che $c_1 \in C$. Cercheremo c_1 nella forma $c + \varepsilon$, con $\varepsilon > 0$.

$$c_1^n = (c+\varepsilon)^n = c^n + \binom{n}{1}\varepsilon \cdot c^{n-1} + \binom{n}{2}\varepsilon^2 \cdot c^{n-2} + \ldots + \binom{n}{n}\varepsilon^n \quad .$$

Possiamo supporre che sia $\varepsilon < 1$; in questo caso vale $\varepsilon > \varepsilon^k$, se $k > 1$. Perciò avremo

$$c_1^n = (c+\varepsilon)^n < c^n + n \cdot \varepsilon \cdot c^{n-1} + \binom{n}{2}\varepsilon \cdot c^{n-2} + \ldots + \binom{n}{n}\varepsilon = c^n + \varepsilon \cdot K \;,$$

dove $K = n \cdot c^{n-1} + \binom{n}{2} \cdot c^{n-2} + \ldots + \binom{n}{n} > 0$. Osservando che $c^n < a$, se scegliamo $0 < \varepsilon < \dfrac{a - c^n}{K}$, si ha $c^n + \varepsilon \cdot K < a$ e, a maggior ragione, $c_1^n = (c+\varepsilon)^n < a$, dunque $c_1 \in C$. Questo fatto ci dice che $\alpha \notin C$. Infatti, se fosse $\alpha \in C$, esisterebbe $c_1 > \alpha$, $c_1 \in C$, contro il fatto che $\forall c \in C\, c \leq \alpha$. Dunque $\alpha \notin C$ e quindi $\alpha^n \geq a$. Ma la classe D non ha minimo. Cioè dimostriamo che se $d \in D$, ossia, se $d^n > a$, esiste $d_1 < d$, tale che $d_1 \in D$.

Prendiamo d_1 della forma $d_1 = d - \varepsilon$ e cerchiamo di scegliere $\varepsilon > 0$ in modo che $d_1^n = (d-\varepsilon)^n > a$.

$$d_1^n = (d-\varepsilon)^n = d^n - \binom{n}{1}\varepsilon \cdot d^{n-1} + \binom{n}{2}\varepsilon^2 \cdot d^{n-2} + \ldots + (-1)^n \cdot \binom{n}{n}\varepsilon^n$$

Tenendo presente che si può prendere $0 < \varepsilon < 1$, con ragionamento analogo a quello sopra fatto, si trova

$$d_1^n = (d-\varepsilon)^n > c^n - n \cdot \varepsilon \cdot d^{n-1} - \binom{n}{2}\varepsilon \cdot d^{n-2} - \ldots - \binom{n}{n}\varepsilon = d^n - \varepsilon \cdot H \;,$$

dove $H = n \cdot d^{n-1} + \binom{n}{2} \cdot d^{n-2} + \ldots + \binom{n}{n} > 0$. Se chiediamo che $d^n - \varepsilon \cdot H > a$, e quindi se $0 < \varepsilon < \dfrac{d^n - a}{H}$, allora, a maggior ragione, $d_1^n > a$, cioè $d_1 \in D$, con $d_1 < d$. Ora si può concludere che $\alpha \notin D$. Se fosse $\alpha \in D$, allora esisterebbe $d_1 \in D$, $d_1 < \alpha$, contro la proprietà di α di essere elemento di separazione fra le classi C e D. Non potendo essere neppure $\alpha^n > a$, resta $\alpha^n = a$.

Abbiamo così dimostrato che una soluzione dell'equazione $x^n = a$ esiste; d'altra parte essa è unica, essendo x^n funzione crescente. Se $0 \leq \alpha_1 < \alpha_2$ allora $\alpha_1^n < \alpha_2^n$. Dunque solo uno dei due numeri può uguagliare a. $\square$

L'unico numero $\alpha \geq 0$ tale che $\alpha^n = a$, con $a \geq 0$ si dice la *radice n-esima di a* e si denota con $\sqrt[n]{a}$ o con $(a)^{\frac{1}{n}}$.

Se n è pari, null'altro è da aggiungere; $\sqrt[n]{a}$ è definita solo per gli $a \geq 0$.

Se n è dispari e $a < 0$, allora $-a > 0$. Esiste un solo numero positivo α $(= \sqrt[n]{-a})$, tale che $\alpha^n = -a$. Allora $(-\alpha)^n = (-1)^n \cdot \alpha^n = -\alpha^n = -(-a) = a$. Dunque, se n è dispari, esiste una soluzione (necessariamente unica) dell'equazione $x^n = a$ quale che sia $a \in \mathbb{R}$. Questa soluzione si indica ancora con il simbolo $\sqrt[n]{a}$. Invece conveniamo che la scrittura $(a)^{\frac{1}{n}}$ sia definita solamente se $a \geq 0$.

In definitiva: se $a \geq 0$, $\sqrt[n]{a} = (a)^{\frac{1}{n}}$; se $a < 0$ e n è dispari, $\sqrt[n]{a} = -(-a)^{\frac{1}{n}}$. Se $a < 0$ e n è pari, $\sqrt[n]{a}$ **non** è definito.

2.4.6 Scrittura decimale dei numeri razionali e reali

È noto che i numeri razionali ammettono una scrittura decimale che è limitata (cioè da un certo punto in poi tutte le cifre sono 0) o periodica (cioè esiste un gruppo di cifre $c_{k+1} \dots c_{k+p}$ che si ripetono indefinitamente). Ossia ogni numero razionale ammette una scrittura del tipo

$$\frac{m}{n} = q, c_1 c_2 \dots c_r \quad \text{oppure} \quad \frac{m}{n} = q, c_1 c_2 \dots c_k c_{k+1} \dots c_{k+p} \dots = q, c_1 c_2 \dots c_k \overline{c_{k+1} \dots c_{k+p}} \quad .$$

Vediamo di giustificare brevemente questo fatto. Supponiamo, per semplicità, che il numero razionale $\frac{m}{n}$ sia positivo e quindi, supponiamo $m > 0, n > 0$ e primi fra loro. Dividendo m per n, troveremo quoziente q e resto $r < n$: $m = q \cdot n + r$ e quindi

$$\frac{m}{n} = q + \frac{r}{n} \quad ,$$

con $\frac{r}{n} < 1$. Vogliamo trovare quanti decimi ci sono in $\frac{r}{n}$. Perciò scriveremo

$$\frac{m}{n} = q + \frac{1}{10} \cdot \frac{10 \cdot r}{n} \quad ,$$

ed eseguiremo la divisione di $10 \cdot r$ per n: $10 \cdot r = c_1 \cdot n + r_1$, con $r_1 < n$. Ossia $\frac{10 \cdot r}{n} = c_1 + \frac{r_1}{n}$ e quindi

$$\frac{m}{n} = q + \frac{c_1}{10} + \frac{1}{10} \cdot \frac{r_1}{n} = q + \frac{c_1}{10} + \frac{1}{10^2} \cdot \frac{10 \cdot r_1}{n} \quad .$$

Ora si dovrà determinare il numero di decimi in $\frac{r_1}{n} < 1$ (e quindi il numero di centesimi in $\frac{1}{10} \cdot \frac{r_1}{n}$). Si procederà come in precedenza: $10 \cdot r_1 = c_2 \cdot n + r_2$, $r_2 < n$, e quindi $\frac{10 \cdot r_1}{n} = c_2 + \frac{r_2}{n}$, ossia

$$\frac{m}{n} = q + \frac{c_1}{10} + \frac{c_2}{10^2} + \frac{1}{10^2} \cdot \frac{r_2}{n} = q + \frac{c_1}{10} + \frac{c_2}{10^2} + \frac{1}{10^3} \cdot \frac{10 \cdot r_2}{n} \quad .$$

Si ottengono così le successive cifre decimali dell'espansione della frazione $\frac{m}{n}$. In generale, la cifra k-esima si ottiene dall'uguaglianza $10 \cdot r_{k-1} = c_k \cdot n + r_k$, $r_k < n$. Poiché i possibili resti

della divisione per n sono n, cioè $0, 1, 2, \ldots, (n-1)$, ci dovranno essere numeri naturali k e p tali che $r_{k-1} = r_{k+p-1}$, e quindi $c_k = c_{k+p}$; le cifre $c_{k+1} \ldots c_{k+p}$ si ripeteranno indefinitamente e costituiranno il periodo della scrittura decimale considerata. Osserviamo infine che la scrittura decimale di un numero razionale non può avere periodo 9. Se così fosse, per qualche $k \in \mathbb{N}^+$, dovrebbe aversi $10 \cdot r_k = 9 \cdot n + r_k$, cioè $9 \cdot r_k = 9 \cdot n$, e quindi $r_k = n$, contro il fatto che è invece $0 \leq r_k < n$.

Le cifre comprese tra la virgola e il periodo si sogliono chiamare *antiperiodo*.

Naturalmente può accadere che sia $r_{k-1} = 0$ per qualche valore di $k \geq 1$. In questo caso si otterrà $0 = c_k \cdot n + r_k$, che è possibile solo se $c_k = 0, r_k = 0$, e quindi $c_h = 0, r_h = 0$ per ogni $h \geq k$. Allora accade che $\dfrac{m}{n} = \dfrac{d}{10^k}$ e quindi che $10^k \cdot m = d \cdot n$, con $d \in \mathbb{N}^+$. Se n contenesse qualche fattore primo diverso da 2 e da 5, esso dovrebbe dividere m, contro l'ipotesi che m e n siano primi fra loro. Dunque, se il numero ha scrittura decimale limitata, il denominatore n può contenere solo potenze di 2 e di 5. Viceversa, se $n = 2^r \cdot 5^s$, moltiplicando entrambi i termini della frazione $\dfrac{m}{n}$ per 5^{r-s} se $r > s$ o per 2^{s-r} se $s > r$, ci si può ridurre a una frazione del tipo $\dfrac{5^{r-s} \cdot m}{10^r}$ oppure $\dfrac{2^{s-r} \cdot m}{10^s}$. Se $r = s$ il numero è già nella forma voluta. Se un numero si scrive in forma $\dfrac{M}{10^k}$, allora certamente è $r_h = 0$, per qualche valore di h; infatti basta pensare a M scritto in base dieci. La scrittura decimale di $\dfrac{m}{n}$ si denoterà dunque come è usuale: $\dfrac{m}{n} = q, c_1 c_2 c_3 \ldots$, e sarà o limitata o periodica. Se la scrittura è limitata, cioè $q, c_1 c_2 c_3 \ldots c_k = q + \dfrac{c_1}{10} + \ldots \dfrac{c_k}{10^k}$, è immediato costruire una frazione dalla quale essa proviene. Se invece la scrittura è di tipo periodico, $q, c_1 c_2 c_3 \ldots c_k \overline{c_{k+1} \ldots c_{k+p}}$, supposto che essa rappresenti un numero razionale, detto $x = q, c_1 c_2 c_3 \ldots c_k \overline{c_{k+1} \ldots c_{k+p}}$ tale numero, si vede facilmente che $10^{k+p} \cdot x - 10^k \cdot x = qc_1 \ldots c_k c_{k+1} \ldots c_{k+p}, \overline{c_{k+1} \ldots c_{k+p}} - qc_1 \ldots c_k, \overline{c_{k+1} \ldots c_{k+p}}$, cioè $10^k \cdot (10^p - 1) \cdot x = qc_1 \ldots c_k c_{k+1} \ldots c_{k+p} - qc_1 \ldots c_k$. Di qui si ottiene la ben nota regola per la *frazione generatrice*

$$x = \frac{qc_1 \ldots c_k c_{k+1} \ldots c_{k+p} - qc_1 \ldots c_k}{\underbrace{999 \ldots 9}_{\text{p volte}} \underbrace{000 \ldots 0}_{\text{k volte}}} \quad .$$

Evidentemente $qc_1 \ldots c_k c_{k+1} \ldots c_{k+p}$ e $qc_1 \ldots c_k$ sono due numeri naturali dati in base dieci, dove $c_1 \ldots$ sono cifre mentre q non è una cifra ma un numero di $\mathbb{N}$, che si dovrà pensare rappresentato dalle sue cifre. È poi chiaro che lo sviluppo della frazione x ha la scrittura decimale dalla quale siamo partiti.

Supponiamo ora che sia data una scrittura decimale qualsiasi: $q, c_1 \ldots c_k \ldots$. Se essa è limitata o periodica, rappresenta un numero razionale, come abbiamo visto. Supponiamola illimitata, non periodica. Ad essa si potrà associare una coppia di classi così costruite

$$A = \{q, q + \frac{c_1}{10}, \ldots, q + \frac{c_1}{10} + \ldots \frac{c_k}{10^k}, \ldots\}$$

e

$$B = \{q + 1, q + \frac{c_1}{10} + \frac{1}{10}, \ldots, q + \frac{c_1}{10} + \ldots \frac{c_k}{10^k} + \frac{1}{10^k}, \ldots\} \ .$$

Gli elementi di A e B sono elencati in ordine crescente quelli di A e decrescente quelli di B e ogni elemento di A è minore di ogni elemento di B. Dunque le classi sono classi separate di numeri

razionali (e quindi reali). Debbono avere un elemento di separazione α, che però è unico. Infatti la distanza tra $q + \frac{c_1}{10} + \ldots \frac{c_k}{10^k} + \frac{1}{10^k} \in B$ e $q + \frac{c_1}{10} + \ldots \frac{c_k}{10^k} \in A$ è $\frac{1}{10^k}$ che può essere piccola quanto si vuole. Se due elementi α e β fossero compresi tra le due classi, la distanza tra esse non potrebbe scendere al di sotto di $\beta - \alpha$, contro quanto qui accade. Dunque ogni scrittura decimale individua un numero reale (eventualmente razionale). Date due scritture decimali (che individuano due numeri reali) $\alpha = a_0, a_1 \ldots a_k \ldots$ e $\beta = b_0, b_1 \ldots b_k \ldots$, diremo che $\alpha < \beta$ se α precede β nell'*ordine lessicografico*. Cioè se $a_0 < b_0$ oppure se esiste $k \in \mathbb{N}^+$ tale che $a_0 = b_0, a_1 = b_1, \ldots, a_{k-1} = b_{k-1}$, ma $a_k < b_k$. Si vede che si tratta di una relazione d'ordine tra scritture decimali che è un ordine totale. Faremo ora vedere che l'insieme delle scritture decimali è completo. È più semplice mostrare che ogni insieme inferiormente limitato di scritture decimali ha un estremo inferiore. Sia $B \neq \emptyset$ un insieme non vuoto di scritture decimali, inferiormente limitato. Ciò significa che esiste una scrittura decimale $\kappa = k_0, k_1 k_2 \ldots$ tale che $\kappa \leq \beta$, $\forall \beta \in B$. Sia $\beta \in B$, $\beta = b_0, b_1 \ldots b_h \ldots$. È $k_0 \leq b_0$. Si considerino i numeri $k_0 - 1 < k_0 < \ldots < b_0 - 1 < b_0$. (Cominciamo da $k_0 - 1$ perché κ potrebbe essere negativo). Esiste certamente uno di questi numeri n_0 che è un minorante di B ed è il massimo tra tali minoranti. Ossia n_0 è tale che $n_0 \leq \beta$, per tutti i $\beta \in B$, ma c'è qualche $\beta \in B$ minore di $n_0 + 1$. Si divida poi l'intervallo compreso tra n_0 e $n_0 + 1$ in dieci parti uguali e si prenda n_1 in modo che $n_0 + \frac{n_1}{10}$ sia il massimo minorante di B, fra i numeri di quel tipo. (Cioè $n_0 + \frac{n_1}{10} \leq \beta$, per tutti i $\beta \in B$, ma esiste qualche elemento di B minore di $n_0 + \frac{n_1}{10} + \frac{1}{10}$). Determinato $n_0 + \frac{n_1}{10} + \ldots + \frac{n_h}{10^h}$ in modo che sia il massimo minorante di B, fra i numeri di quel tipo, si divida in dieci parti uguali la distanza tra $n_0 + \frac{n_1}{10} + \ldots + \frac{n_h}{10^h}$ e $n_0 + \frac{n_1}{10} + \ldots + \frac{n_h}{10^h} + \frac{1}{10^h}$. In questo modo si può trovare n_{h+1} in modo tale che $n_0 + \frac{n_1}{10} + \ldots + \frac{n_h}{10^h} + \frac{n_{h+1}}{10^{h+1}}$ sia il massimo minorante di B tra i numeri di quel tipo.

È allora chiaro che il numero

$$\nu = n_0, n_1 n_2 \ldots n_h \ldots$$

è un minorante di B e che fra tutti i minoranti, per costruzione, è il massimo; cioè

$$\nu = \inf B \quad .$$

Sulla base di quanto detto nell'osservazione 2.4.4, l'insieme delle scritture decimali è perciò completo.

Diamo ora un accenno di verifica delle proprietà formali di $\mathbb{R}$. Dati $\alpha = a_0, a_1 \ldots a_k \ldots$ e $\beta = b_0, b_1 \ldots b_k \ldots$ e supposti entrambi i numeri positivi, definiamo $\alpha + \beta$ e $\alpha \cdot \beta$ come segue

$$\alpha + \beta = \sup\{a_0 + b_0, a_0 + \frac{a_1}{10} + b_0 + \frac{b_1}{10}, \ldots,$$
$$a_0 + \frac{a_1}{10} + \ldots \frac{a_k}{10^k} + b_0 + \frac{b_1}{10} + \ldots \frac{b_k}{10^k}, \ldots\}$$

e

$$\alpha \cdot \beta = \sup\{a_0 \cdot b_0, (a_0 + \frac{a_1}{10}) \cdot (b_0 + \frac{b_1}{10}), \ldots,$$
$$(a_0 + \frac{a_1}{10} + \ldots \frac{a_k}{10^k}) \cdot (b_0 + \frac{b_1}{10} + \ldots \frac{b_k}{10^k}), \ldots\}$$

Dei segni si terrà conto in modo ovvio. Si verifica facilmente che le operazioni sono associative, commutative, che la moltiplicazione è distributiva rispetto all'addizione. Lo zero è dato da 0 e l'unità da 1. L'opposto di $\alpha = a_0, a_1 \dots a_k \dots$ è $-a_0, a_1 \dots a_k \dots$, con l'ovvio significato del segno $-$. Il reciproco di $\alpha = a_0, a_1 \dots a_k \dots > 0$ è naturalmente

$$\alpha^{-1} = \inf\{\frac{1}{a_0}, \frac{1}{a_0 + \frac{a_1}{10}}, \dots, \frac{1}{a_0 + \frac{a_1}{10} + \dots \frac{a_k}{10^k}}, \dots\} \quad .$$

2.4.7 Intervalli di $\mathbb{R}$

Si dicono intervalli di $\mathbb{R}$ gli insiemi

$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$ con $a, b \in \mathbb{R}$, $a < b$. **Intervallo chiuso e limitato** di **estremi** a e b.

$(a, b] =]a, b] = \{x \in \mathbb{R} : a < x \leq b\}$. **Intervallo limitato aperto a sinistra e chiuso a destra** di **estremi** a e b.

$[a, b) = [a, b[= \{x \in \mathbb{R} : a \leq x < b\}$. **Intervallo limitato chiuso a sinistra e aperto a destra** di **estremi** a e b.

$(a, b) =]a, b[= \{x \in \mathbb{R} : a < x < b\}$. **Intervallo limitato aperto** di **estremi** a e b.

$[a, +\infty) = [a, +\infty[= \{x \in \mathbb{R} : a \leq x\}$. **Semiretta destra chiusa** di **origine** a.

$(a, +\infty) =]a, +\infty[= \{x \in \mathbb{R} : a < x\}$. **Semiretta destra aperta** di **origine** a.

$(-\infty, b] =]-\infty, b] = \{x \in \mathbb{R} : x \leq b\}$. **Semiretta sinistra chiusa** di **origine** b.

$(-\infty, b) =]-\infty, b[= \{x \in \mathbb{R} : x < b\}$. **Semiretta sinistra aperta** di **origine** b.

$\mathbb{R} = (-\infty, +\infty) =]-\infty, +\infty[$. **Retta reale**.

Gli intervalli sono caratterizzati dalla seguente proprietà

Proposizione 2.4.1 *Un insieme $E \subset \mathbb{R}$ che contenga più di un punto è un intervallo se e solo se ha la seguente proprietà:*

(I) *Se $x_1, x_2 \in E$ e $x_1 < x_2$, $x_1 < x < x_2$ implica $x \in E$.*

DIMOSTRAZIONE: Omessa. □

Abbiamo già introdotto il concetto di classi separate di numeri reali. Ci sarà utile un concetto simile al precedente:

Diremo che due classi separate A e B di numeri reali sono *contigue* se, preso comunque un numero $\varepsilon > 0$, esistono $\overline{a} \in A$ e $\overline{b} \in B$ tali che $\overline{b} - \overline{a} < \varepsilon$.

Osservazione 2.4.5 *Dalla definizione segue facilmente che se due classi separate A e B sono contigue, allora esiste* **un solo** *elemento di separazione tra le due classi. Infatti, se ce ne fossero due, $\delta_1 < \delta_2$, la distanza tra le classi non potrebbe scendere sotto $\delta_2 - \delta_1$ e, in particolare, scegliendo $0 < \varepsilon < \delta_2 - \delta_1$, la definizione di contiguità non potrebbe essere soddisfatta.*

Teorema 2.4.6 [di Cantor, sugli intervalli incapsulati]. *Sia data una successione $\{I_n : n \in \mathbb{N}\}$ di intervalli chiusi e limitati, decrescenti per inclusione. Cioè sia data la successione*

$$I_0 = [a_0, b_0] \supset I_1 = [a_1, b_1] \supset \ldots \supset I_n = [a_n, b_n] \supset \ldots \ .$$

Allora c'è almeno un punto comune a tutti gli intervalli. Se esistono intervalli di lunghezza piccola quanto si vuole, c'è un solo punto comune a tutti gli intervalli.

Dimostrazione: Da $[a_0, b_0] \supset [a_1, b_1] \supset \ldots \supset [a_n, b_n] \supset \ldots$, segue $a_0 \leq a_1 \leq \ldots \leq a_n \leq \ldots$ e $b_0 \geq b_1 \ldots \geq b_n \geq \ldots$, con $a_n < b_n$ per ogni $n \in \mathbb{N}$. Consideriamo le due classi

$$A = \{a_n : n \in \mathbb{N}\} \quad \text{e} \quad B = \{b_n : n \in \mathbb{N}\} \quad .$$

Le due classi A e B sono separate. Siano $m, n \in \mathbb{N}$. Se $m < n$ è $I_n \subset I_m$ e quindi $a_m \leq a_n < b_n \leq b_m$; perciò vale $a_m < b_n$. Se $m = n$ la conclusione è ovviamente la stessa. Se $n < m$, avremo $I_m \subset I_n$ e quindi $a_n \leq a_m < b_m \leq b_n$ e quindi, ancora, $a_m < b_n$. Dunque, comunque si prendano $m, n \in \mathbb{N}$ si verifica che $a_m < b_n$, cioè le classi sono separate. Per Dedekind, esiste dunque un elemento di separazione, cioè un elemento $c \in \mathbb{R}$, tale che $\forall\, m, n \in \mathbb{N}$ si ha $a_m \leq c \leq b_n$ e, in particolare, $\forall n \in \mathbb{N}$, si ha $a_n \leq c \leq b_n$. Per la proprietà caratteristica degli intervalli ciò significa che $c \in I_n$ per ogni $n \in \mathbb{N}$, ossia $c \in \bigcap_{n=0}^{\infty} I_n$.

Anzi, se $\alpha = \sup A$, $\forall\, m, n \in \mathbb{N}$ vale $a_m \leq \alpha \leq b_n$, essendo α la minima limitazione superiore di A mentre i b_n sono limitazioni superiori di A. Per analoga ragione, se $\beta = \inf B$, vale

$$a_m \leq \alpha \leq \beta \leq b_n, \ \forall\, m, n \in \mathbb{N} \quad .$$

Dunque tutti i numeri $\alpha \leq \gamma \leq \beta$ sono compresi tra le due classi e, per la proprietà caratteristica degli intervalli, stanno in $\cap_{n=0}^{\infty} I_n$. Solamente questi numeri stanno in tutti gli intervalli. Infatti se $c < \alpha$ esiste qualche $a_n \in A$ tale che $a_n > c$ e quindi c non è elemento di separazione tra le classi A e B. Se poi $c > \beta$ esisterebbe qualche $b_n < c$, e, anche in questo caso, c non potrebbe essere elemento di separazione tra le due classi. Supponiamo poi che per ogni $\varepsilon > 0$ esista qualche $n \in \mathbb{N}$ tale che $b_n - a_n < \varepsilon$. Allora le due classi A e B sono contigue e solo un numero può essere compreso tra le due classi. $\square$

Osservazione 2.4.6 *In $\mathbb{R}$ due classi separate A e B sono contigue se e solo se* $\sup A = \inf B$. *È chiaro che questa definizione di contiguità delle classi si può adottare solo in un corpo completo,*

nel quale esiste $\sup A$ *per ogni insieme non vuoto e superiormente limitato. In* $\mathbb{Q}$ *invece, è valida in ogni caso la definizione data in precedenza(per ogni* $\varepsilon > 0$*, esistono* $\overline{a} \in A$ *e* $\overline{b} \in B$ *tali che* $\overline{b} - \overline{a} < \varepsilon$*), mentre in generale non ha senso quella basata su* sup *e* inf*.*

2.5 Topologia della retta reale

Diremo *intervallo sferico di centro* x_0 *e raggio* $\delta > 0$ l'insieme

$$I^{\delta}_{x_0} = \{x \in \mathbb{R} \colon x_0 - \delta < x < x_0 + \delta\} = \{x \in \mathbb{R} \colon |x - x_0| < \delta\} \quad .$$

Diremo *intorno* di $x_0 \in \mathbb{R}$ ogni insieme U che sia soprainsieme di un intervallo sferico di centro x_0. Cioè U è intorno di x_0 se $\exists\, \delta > 0$ tale che $U \supset I^{\delta}_{x_0}$. Indicheremo con $\mathcal{I}_x$ la famiglia degli intorni di x. Gli intorni di un punto soddisfano le seguenti proprietà:

(I1) $\forall U \in \mathcal{I}_x \; U \neq \emptyset$.

(I2) Se $U_1, U_2 \in \mathcal{I}_x$, allora $U_1 \cap U_2 \in \mathcal{I}_x$.

(I3) Se $U \in \mathcal{I}_x$ e $V \supset U$, allora $V \in \mathcal{I}_x$.

Ciò si vede agevolmente: infatti, se $U \in \mathcal{I}_x$, esiste $\delta > 0$ tale che $I^{\delta}_x \subset U$. Almeno $x \in U$, che è quindi non vuoto. Se $U_1, U_2 \in \mathcal{I}_x$, allora esistono $\delta_1 > 0$, $\delta_2 > 0$ tale che $U_i \supset I^{\delta_i}_x$, $(i = 1, 2)$. Se $\delta = \min(\delta_1, \delta_2)$, allora $U_i \supset I^{\delta}_x$, $(i = 1, 2)$, e quindi $U_1 \cap U_2 \supset I^{\delta}_x$. Cioè $U_1 \cap U_2 \in \mathcal{I}_x$. Infine se $V \supset U \in \mathcal{I}_x$, evidentementemente, $V \in \mathcal{I}_x$.

Conviene inoltre osservare che in $\mathbb{R}$ gli intorni dei punti soddisfano un'ulteriore prorietà, detta *assioma di separazione di Hausdorff* [2]:

(H) Se $x \neq y$ esistono intorni $U \in \mathcal{I}_x$ e $V \in \mathcal{I}_y$ tali che $U \cap V = \emptyset$, cioè U e V sono intorni *disgiunti* di x e y rispettivamente.

Ciò si può vedere agevolmente come segue. Se $x \neq y$, sia $0 < \varepsilon < \dfrac{|x - y|}{2}$. Allora $U = \{z \in \mathbb{R} \colon |z - x| < \varepsilon\}$ e $V = \{z \in \mathbb{R} \colon |z - y| < \varepsilon\}$ sono gli intorni cercati. Infatti non ci può essere $z \in U \cap V$. Se, per assurdo, ci fosse avremmo $|x - y| \leq |x - z| + |z - y| < 2 \cdot \varepsilon < |x - y|$, che è chiaramente una contraddizione.

Un punto $x \in \mathbb{R}$ si dice *d'accumulazione* per un insieme $E \subset \mathbb{R}$ se ogni intorno di x, $U \in \mathcal{I}_x$, contiene infiniti punti di E. [3]

[2] Felix Hausdorff (1868–1942). Lavorò a Bonn fino al 1935, quando, essendo ebreo, fu costretto a dimettersi dal regime nazista. Fu insigne studioso della topologia e della teoria degli insiemi. Molte sue ricerche di teoria degli insiemi sono tuttora di grande attualità e hanno trovato di recente notevoli applicazioni.

[3] Precisiamo meglio il significato di insieme *finito* e *infinito*. L'insieme vuoto è finito e si dice che ha 0 elementi o che non ha elementi. Se c'è $n \in \mathbb{N}^+$ tale che esiste un'applicazione biiettiva da $\{1, 2, \ldots, n\}$ a E, diremo che l'insieme

Equivalentemente, si dice che x è d'accumulazione per E se ogni $U \in \mathcal{I}_x$ contiene almeno un punto di E diverso da x.

Che le due definizioni siano equivalenti si vede facilmente; evidentemente, se ogni intorno di x contiene infiniti punti di E, ce ne sono di diversi da x. Se poi ci fosse qualche intorno che contiene solo un numero finito di punti di E: $x_1, x_2, \ldots, x_n$, allora, posto $\delta = \min(|x - x_1|, \ldots, |x - x_n|)$, I_x^δ sarebbe un intorno di x non contenente alcun punto di E diverso da x (si noti che x non è necessariamente un punto di E).

Un punto $x \in E$ che *non* sia d'accumulazione per E si dice un punto *isolato* di E.

Un punto x si dice *aderente* ad E se ogni $U \in \mathcal{I}_x$ contiene almeno un punto di E. Evidentemente i punti di E sono aderenti ad E e i punti d'accumulazione sono, a maggior ragione, punti aderenti.

Diremo *chiusura* di un insieme $E \subset \mathbb{R}$, l'insieme dei suoi punti aderenti

$$\overline{E} = cl(E) = \{x \in \mathbb{R} : x \text{ è aderente a } E\} \quad . \tag{2.22}$$

Si dice che x è *interno* a E se E è intorno di x.

L'insieme dei punti interni ad un insieme E si dice la *parte interna* di E: $\text{int}\,(E)$.

Un insieme $A \subset \mathbb{R}$ si dice *aperto* se è intorno di ogni suo punto, ossia se $\forall x \in A,\ \exists\, \delta > 0 : I_x^\delta \subset A$. Ossia se $\text{int}\,(A) = A$.

È facile riconoscere che ogni intervallo aperto (limitato o no, in particolare $\mathbb{R}$) è un insieme aperto.

Un insieme $C \subset \mathbb{R}$ si dice *chiuso* se coincide con la sua chiusura: $\overline{C} = C$.

Gli intervalli chiusi $[a, b]$, $[a, +\infty[$, $]-\infty, b]$, $\mathbb{R}$, sono insiemi chiusi.

L'operatore di chiusura soddisfa le seguenti proprietà (dette di Kuratowski[4])

(Cl1) $\overline{\emptyset} = \emptyset$.

E ha n elementi; ogni insieme che ha n elementi per qualche n, si dice finito. Diremo infinito un insieme che non è finito.

[4]Kazimierz Kuratowski (1896 – 1980). Insigne matematico polacco, studioso di topologia. Desideroso di divenire ingegnere si iscrisse nel 1913 alla scuola d'ingegneria di Glasgow. Nel primo anno di studio ottenne il primo premio in Matematica. Tornato per trascorrere le vacanze estive a Varsavia, nel 1914 fu sorpreso dallo scoppio della prima guerra mondiale e gli fu impossibile tornare in Scozia. La carriera ingegneristica di Kuratowski fu distrutta, ma la Matematica ne trasse un enorme beneficio. Egli studiò sotto la guida dei professori Janiszewski e Mazurkiewicz, che, a partire dal 1917, tennero all'università di Varsavia un seminario di Topologia, disciplina matematica che iniziava a svilupparsi rigogliosamente in quel periodo.

(Cl2) $E \subset \overline{E}$.

(Cl3) $\overline{C_1 \cup C_2} = \overline{C_1} \cup \overline{C_2}$

(Cl4) $\overline{\overline{E}} = \overline{E}$.

Esercizio 2.5.1 *Si dimostrino le proprietà* (Cl1) – (Cl4).

Si vede dunque, per (Cl1), che $\emptyset$ è chiuso; peraltro, non avendo punti, è vera la proposizione $(\forall x \in \mathbb{R})\,((x \in \emptyset) \Rightarrow (x \text{ è interno a } \emptyset))$; $(x \in \emptyset)$ è proposizione falsa e un'implicazione con antecedente falso è vera, quale che sia la conseguenza. Ricordiamo che anche $\mathbb{R}$ è insieme contemporaneamente aperto e chiuso.

La famiglia degli insiemi aperti e quella dei chiusi godono delle seguenti proprietà.

(A1) La riunione di un insieme arbitrario di aperti è un aperto.

(A2) L'intersezione di un numero finito di aperti è un aperto.

(A3) Il complementare di un aperto è un chiuso.

(C1) L'intersezione di un insieme arbitrario di chiusi è un chiuso.

(C2) L'unione di un numero finito di chiusi è un chiuso.

(C3) Il complementare di un chiuso è un aperto.

Verifichiamo brevemente la cosa per gli insiemi aperti:

(A1) Sia $\{A_\alpha : \alpha \in I\}$ una famiglia finita o infinita di aperti, indiciati dall'insieme d'indici I. Se $x \in \cup_{\alpha\in I} A_\alpha$, allora $x \in A_{\alpha_0}$, con $\alpha_0 \in I$. Poiché A_{α_0}, è aperto, è intorno di x. A maggior ragione $\cup_{\alpha\in I} A_\alpha \supset A_{\alpha_0}$ è intorno di x.

(A2) Se A_1 e A_2 sono aperti e $A_1 \cap A_2 = \emptyset$, allora l'intersezione è aperta. Se $x \in A_1 \cap A_2$, allora, per la proprietà (I2) degli intorni, $A_1 \cap A_2$ è intorno di x e quindi di ogni suo punto. Dunque $A_1 \cap A_2$ è insieme aperto.

(A3) Sia A aperto e consideriamo $\mathcal{C}A = \mathbb{R} \setminus A$. Se $y \in \overline{\mathcal{C}A}$, $y \notin A$. Infatti se fosse $y \in A$, A stesso sarebbe un intorno di y privo di punti di $\mathcal{C}A$. Perciò i punti aderenti a $\mathcal{C}A$ stanno necessariamente in $\mathcal{C}A$, che è dunque chiuso.

Esercizio 2.5.2 *Si dimostrino le proprietà* (C1) – (C3) *degli insiemi chiusi.*

Osservazione 2.5.1 *Le proprietà (o assiomi) di Kuratowski della chiusura sono caratteristiche, nel senso che permettono di ricostruire la topologia considerata. Cioè, dichiarati chiusi gli insiemi che coincidono con la loro chiusura, si dicono aperti i complementari dei chiusi. Gli intorni di un punto x sono gli insiemi che contengono un insieme aperto al quale x appartiene. Si vede perciò che la topologia su un insieme può essere data equivalentemente assegnando la famiglia degli intorni dei punti, oppure la famiglia degli aperti, oppure la famiglia dei chiusi, oppure l'operatore di chiusura, oppure l'operatore di parte interna.*

Dato $E \subset \mathbb{R}$, e preso un punto $x \in \mathbb{R}$, abbiamo già dato il significato di "x è interno a E. Diremo che x è *esterno* ad E se è interno a $\mathcal{C}E$. Infine se x non è né interno né esterno ad E, diremo che è punto di *frontiera* per E. Ricordiamo che x è interno ad E se esiste $\delta > 0$ tale che $I_x^\delta \subset E$. Analogamente, x è esterno ad E se, per qualche $\delta > 0$, è $I_x^\delta \subset \mathcal{C}E$. Se x non è né interno, né esterno, allora ogni suo intorno contiene sia punti di E che del complementare. Cioè x è di frontiera per E se $x \in \overline{E} \cap \overline{\mathcal{C}E}$. L'insieme dei punti di frontiera di E è la *frontiera* di E: $\operatorname{fr} E = \mathcal{F}E$. Dunque $\operatorname{fr} E = \overline{E} \cap \overline{\mathcal{C}E}$, e quindi la frontiera è un insieme chiuso.

Esempio 2.5.1 *Si consideri l'insieme $E = \mathbb{Q} \cap [0,1]$ e si decida se esso è aperto o chiuso. Se ne calcoli la parte interna, la frontiera, la chiusura. Gli stessi quesiti si pongano per $\mathcal{C}E$.*

Svolgimento: Per quanto si è osservato relativamente alla densità in $\mathbb{R}$ dei numeri razionali e degli irrazionali, possiamo concludere che non esiste alcun intervallo di $\mathbb{R}$ composto solo da numeri razionali o solo da numeri irrazionali. Dunque se $x \in \mathbb{R}$ e $U \in \mathcal{I}_x$, vale $U \cap \mathbb{Q} \neq \emptyset$ e anche $U \cap (\mathbb{R} \setminus \mathbb{Q}) \neq \emptyset$. Allora possiamo concludere che E non ha punti interni (non esiste alcun intorno di un suo punto fatto solo da numeri razionali). Ogni punto dell'intervallo $[0,1]$ è aderente ad E (in ogni intorno di un punto $0 \leq y \leq 1$ ci sono punti di E), mentre i punti $z < 0$ e i punti $u > 1$ hanno intorni privi di punti di E (si prendano gli intervalli centrati in z, o rispettivamente in u, di semiampiezza la distanza di z da 0, cioè $|z|$, e, rispettivamente, di u da 1, cioè $|1-u|$). Allora si verifica che E non è né aperto né chiuso; $\operatorname{int} E = \emptyset$, $\overline{E} = [0,1]$, $\operatorname{fr} E = [0,1]$. Il complementare è dato da $\mathcal{C}E =]-\infty, 0[\cup ([0,1] \cap (\mathbb{R} \setminus \mathbb{Q})) \cup]1, +\infty[$. Esso non è né aperto né chiuso. $\operatorname{int} \mathcal{C}E =]-\infty, 0[\cup]1, +\infty[$, $\overline{\mathcal{C}E} = \mathbb{R}$, $\operatorname{fr} \mathcal{C}E = \operatorname{fr} E = [0,1]$. □

Si verifica facilmente che l'uguaglianza $\operatorname{fr} \mathcal{C}E = \operatorname{fr} E$ ha validità generale.

Saranno utili nel seguito anche le seguenti nozioni. Si dice *intorno destro* di un punto x ogni soprainsieme di un intervallo $[x, x+\delta[$, per qualche $\delta > 0$. Analogamente si dice *intorno sinistro* di x ogni soprainsieme di un intervallo $]x-\delta, x]$, per qualche $\delta > 0$. Si dice *intorno di* $+\infty$ ogni soprainsieme di una semiretta destra: $]a, +\infty[$. *Intorno di* $-\infty$ è ogni soprainsieme di una semiretta sinistra: $]-\infty, b[$. Infine diremo *intorno di* ∞ (senza segno) ogni soprainsieme della riunione di una semiretta sinistra e di una destra, ossia ogni soprainsieme di $\{x \in \mathbb{R} : |x| > a, a > 0\}$. Si noti che gli intorni destri e sinistri di un punto **non** sono necessariamente intorni del punto. Si ricordi anche che $+\infty, -\infty, \infty$ **non** sono elementi di $\mathbb{R}$, ma solo utili simboli da usare in ambiti ben precisi e codificati.

2.5.1 Teorema di Bolzano-Weierstrass e sottoinsiemi compatti di $\mathbb{R}$

Ricordiamo che dati un insieme $E \subseteq \mathbb{R}$ e un punto x_0 il punto si dice d'accumulazione per E se ogni intorno di x_0 contiene infiniti punti di E. È dunque chiaro che se F è un sottoinsieme finito di $\mathbb{R}$, esso non può avere punti d'accumulazione. Però $\mathbb{N} \subseteq \mathbb{R}$ è infinito, ma è privo di punti d'accumulazione. Infatti, preso un qualsiasi punto $x_0 \in \mathbb{R}$, esso non può essere d'accumulazione per $\mathbb{N}$. Se $x_0 < 0$, allora detto $\delta = |x_0|$, l'intervallo $]x_0 - \delta, x_0 + \delta[$ è un intorno di x_0 che non contiene alcun punto di $\mathbb{N}$. Se poi $x_0 \geq 0$, prendiamo un intero n tale che $n \leq x_0 < n+1$. Allora l'intervallo $]x_0 - 1, x_0 + 1[$ contiene un solo punto di $\mathbb{N}$. Dunque l'insieme dei punti d'accumulazione di $\mathbb{N}$ in $\mathbb{R}$ è vuoto. Possiamo chiederci sotto quali condizioni un insieme infinito in $\mathbb{R}$ abbia almeno un punto d'accumulazione. La condizione è data dal seguente

Teorema 2.5.1 [Bolzano - Weierstrass]. *Ogni insieme $E \subseteq \mathbb{R}$ infinito e limitato ha almeno un punto d'accumulazione in $\mathbb{R}$.*

Dimostrazione: Poiché E è un insieme limitato di $\mathbb{R}$ esso ha limitazioni superiori e inferiori; esistono cioè numeri reali a_0 e b_0 tali che per ogni $x \in E$ valga $a_0 \leq x \leq b_0$. Sia dunque $I_0 = [a_0, b_0]$ un intervallo che contiene E. Se $m_0 = \dfrac{a_0 + b_0}{2}$ è il punto di mezzo di I_0, dei due intervalli $[a_0, m_0]$ e $[m_0, b_0]$ almeno uno dei due contiene infiniti punti di E. Infatti la loro unione contiene tutto E, che è infinito. Sia $I_1 = [a_1, b_1]$ uno dei due intervalli che contiene infiniti punti di E; se ce n'è solo uno che contiene infiniti punti di E, prendiamo quello; se tutti e due contengono infiniti punti di E, scegliamone uno, per esempio quello di sinistra. Dunque $I_1 \cap E$ è un insieme infinito. Prendiamo il punto di mezzo m_1 di I_1 e consideriamo i due sottointervalli $[a_1, m_1]$ e $[m_1, b_1]$; almeno uno dei due ha intersezione finita con E. Diaciamo I_2 uno dei due sottointervalli di I_1 che contiene infiniti punti di E. Dividiamo I_2 a metà e proseguiamo scegliendo ogni volta un intervallo I_n tale che $I_n \cap E$ sia infinito. Otteniamo cosí una successione di intervalli chiusi e limitati, decrescente per inclusione

$$I_0 \supseteq I_1 \supseteq I_2 \supseteq \ldots \supseteq I_n \supseteq \ldots \tag{2.23}$$

ognuno dei quali contiene infiniti punti di E. Inoltre se $\ell_0 = b_0 - a_0$ è la lunghezza di I_0, poiché ad ogni passaggio al successivo sottointervallo la lunghezza viene dimezzata, la lunghezza di I_n è $\ell_n = \dfrac{\ell_0}{2^n}$ e quindi, dato $\varepsilon > 0$ esiste n tale che la lunghezza di I_n è $\ell_n < \varepsilon$. Per il Teorema (2.4.6) di Cantor sugli intervalli inscatolati esiste un solo punto comune a tutti gli intervalli: $c \in \bigcap_{n=0}^{\infty} I_n$. Questo punto è il punto d'accumulazione per E che stavamo cercando. Infatti sia $]c - \delta, c + \delta[$ un intorno sferico di c, avente semiampiezza $\delta > 0$. Esiste certamente qualche n tale che la lunghezza di I_n sia minore di δ. Poiché $c \in I_n$, si ha $I_n \subseteq]c - \delta, c + \delta[$. Ma I_n contiene infiniti punti di E. Poiché ogni intorno di c contiene un un intervallo centrato in c del tipo $]c - \delta, c + \delta[$, ogni intorno di c contiene infiniti punti di E. Dunque c è punto d'accumulazione di E. □

Un sottoinsieme $K \subseteq \mathbb{R}$ si dice *compatto* se è un insieme chiuso e limitato di $\mathbb{R}$. Questa definizione è semplice ma vale per $\mathbb{R}$, per $\mathbb{R}^n$ e in pochi altri casi speciali. Una definizione generale di compattezza è la seguente. Dato un insieme $K \subseteq \mathbb{R}$ diremo *ricoprimento aperto* di K, ogni famiglia $\mathcal{U}$ di

insiemi aperti in $\mathbb{R}$, tale che $\bigcup \mathcal{U} \supseteq K$. Diremo che K è compatto se, comunque si prenda un suo ricoprimento aperto $\mathcal{U}$, esiste una sottofamiglia **finita** $\mathcal{F} \subseteq \mathcal{U}$ che copre K, cioè tale che $\bigcup \mathcal{F} \supseteq K$. In realtà quella che abbiamo assunto come definizione è il contenuto di un importante Teorema (di Heine, Borel, Pincherle) che dimostra l'equivalenza in $\mathbb{R}$ tra l'essere K chiuso e limitato e l'essere compatto nel senso dei ricoprimenti aperti. Ci sono altre definizioni equivalenti di compattezza, di una delle quali (valida negli spazi metrici) ci occuperemo nel seguito.

2.5.2 Insiemi connessi di $\mathbb{R}$

Un insieme $A \subset \mathbb{R}$ si dice *sconnesso* se esiste una partizione di A in due classi $\{B, C\}$ (ossia se esistono insiemi $B \neq \emptyset$, $C \neq \emptyset$, tali che $B \cap C = \emptyset$ e $A = B \cup C$) tali che $\overline{B} \cap C = \emptyset$ e $B \cap \overline{C} = \emptyset$. Un insieme **non** sconnesso, si dice *connesso*.

Vale il seguente teorema del quale omettiamo la dimostrazione

Teorema 2.5.2 *In $\mathbb{R}$ sono connessi, oltre agli insiemi formati da un solo punto, tutti e soli gli intervalli.* □

Dunque un insieme A che contiene più di un punto sarà connesso se, comunque se ne prenda una partizione $\{B, C\}$, o $\overline{B} \cap C \neq \emptyset$ o $B \cap \overline{C} \neq \emptyset$. Si noti che affinché un insieme sia connesso non basta che $\overline{B} \cap \overline{C} \neq \emptyset$!

La definizione data sopra conserva la sua validità in ambiti più ampi di $\mathbb{R}$ (per esempio $\mathbb{R}^n$, spazi metrici o, più in generale, topologici). Anzi è un "lusso se riferita a $\mathbb{R}$, bastando ivi gli intervalli. Ma l'intento è di "seminare per tempo qualche nozione più generale, da sfruttare in seguito...

2.6 Cardinalità degli insiemi

Già abbiamo presentato la differenza tra gli insiemi finiti e infiniti. Qui ci soffermeremo su un'ulteriore distinzione fra gli insiemi infiniti, distinguendo fra quelli che si possono porre in corrispondenza biuivoca con $\mathbb{N}$ (gli insiemi *infiniti numerabili*) e quegli insiemi E che ammettono un'applicazione iniettiva da $\mathbb{N}$ in E, ma per i quali non esiste alcuna applicazione biiettiva fra $\mathbb{N}$ ed E (insiemi *non numerabili*).

Dati due insiemi A e B diremo che essi sono *equipotenti* se esiste un'applicazione biiettiva $\phi : A \to B$. Se immaginiamo di potere considerare la *classe* di tutti gli insiemi, l'equipotenza soddisfa le proprietà riflessiva, simmetrica e transitiva (come facilmente si verifica) e quindi è atta a suddividere la totalità degli insiemi in classi d'equivalenza. Ogni classe di questa particolare equivalenza d'insiemi si dirà la *cardinalità* di quell'insieme. Cioè se $B, C, \ldots$ sono insiemi equipotenti con A diremo che hanno la stessa cardinalità di A. Ciò si scrive $\operatorname{card} B = \operatorname{card} A$. Converrà pensare che per ogni classe d'equipotenza si inventi un nuovo simbolo che si chiamerà la cardinalità di quella classe; è, in termini intuitivi, la proprietà comune alla classe d'equipotenza.

Per indicare la cardinalità di $\mathbb{N}$, ossia dell'infinito numerabile, è usuale impiegare il simbolo $\aleph_0$ (da leggere "aleph con zero): $\operatorname{card} \mathbb{N} = \aleph_0$.

Si dirà che $\operatorname{card} B \leq \operatorname{card} A$ se esiste un'applicazione iniettiva da B in A. Si dirà infine che $\operatorname{card} B < \operatorname{card} A$ se esiste un'applicazione iniettiva da B in A, ma non c'è alcuna applicazione biiettiva tra i due insiemi.

Relativamente alla cardinalità di $\aleph_0$ si possono dimostrare alcune semplici proposizioni

Teorema 2.6.1 *Siano A e B due insiemi equipotenti con $\mathbb{N}$. Allora anche $A \cup B$ ha cardinalità $\aleph_0$.*

DIMOSTRAZIONE: Per ipotesi A e B si possono mettere in corrispondenza biunivoca con $\mathbb{N}$ o, come si dice brevemente, si possono numerare. Perciò

$$A = \{a_0, a_1, a_2, \ldots, a_n \ldots\} \quad \text{e} \quad B = \{b_0, b_1, b_2, \ldots, b_n \ldots\} \quad .$$

Ma allora è facile dare una numerazione di $A \cup B$:

$$A \cup B = \{a_0, b_0, a_1, b_1, \ldots, a_n, b_n, \ldots\} \quad .$$

In questa numerazione si avrà l'avvertenza di non scrivere gli elementi già incontrati (cioè se b_1, per esempio, è già stato scritto, si ometterà di scriverlo un'ulteriore volta). □

Più in generale vale

Teorema 2.6.2 *Sia $\{A_n\}$ un insieme numerabile di insiemi numerabili. Allora anche*

$$\bigcup_{n=0}^{\infty} A_n$$

è numerabile.

DIMOSTRAZIONE: Per ipotesi abbiamo

$$A_n = \{a_0^n, a_1^n, a_2^n, \ldots, a_k^n, \ldots\}$$

per $n \in \mathbb{N}$. Se diciamo "peso di un elemento a_k^n il numero $p = k + n$, per ogni $p \in \mathbb{N}$ abbiamo un numero finito di elementi che possiamo elencare in ordine crescente dell'indice in posizione bassa, per esempio. Cioè nell'ordine $a_0^p, a_1^{p-1}, \ldots, a_p^0$, omettendo ogni volta gli elementi già elencati. Allora è chiaro che si può elencare la riunione numerabile degli insiemi A_n come segue:

$$\cup_{n=0}^{\infty} A_n = \{a_0^0, a_0^1, a_1^0, \ldots, a_0^p, a_1^{p-1}, \ldots, a_p^0, \ldots\} \quad .$$

Con la solita omissione dei termini già incontrati, in questo modo si stabilisce una corrispondenza biunivoca tra $\mathbb{N}$ e $\cup_{n=0}^{\infty} A_n$. $\square$

Più in particolare, possiamo determinare le cardinalità degli insiemi numerici $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ finora introdotti.

Teorema 2.6.3 *Gli insiemi $\mathbb{Z}$ e $\mathbb{Q}$ sono numerabili.*

DIMOSTRAZIONE: Dobbiamo trovare un modo per numerare tutti gli elementi di $\mathbb{Z}$ e, rispettivamente, di $\mathbb{Q}$. Per quanto riguarda $\mathbb{Z}$ la cosa è piuttosto facile. Basta pensare di elencare i suoi elementi a partire dallo zero, elencando prima un numero positivo n e poi $-n$, se $n \neq 0$. Cioè:

$$\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots, n, -n, \ldots\} \quad .$$

Per dimostrare la numerabilità di $\mathbb{Q}$ procediamo come segue. Cominciamo a considerare i numeri razionali positivi rappresentati come frazioni $\frac{m}{n}$ con m ed n primi fra loro. Diciamo poi "peso di $\frac{m}{n}$, $p = m + n$. Per ogni assegnato valore di $p \geq 1$ ci sono solo un numero finito di razionali aventi peso p, che possiamo elencare in ordine crescente di valore del denominatore. C'è un solo razionale di peso 1: $\frac{0}{1} = 0$; un solo razionale di peso 2: $\frac{1}{1} = 1$; due razionali di peso 3: $\frac{1}{2}$ e $\frac{2}{1} = 2$; etc. Detti $\mathbb{Q}^\star$ i razionali positivi, li possiamo dunque elencare come segue

$$\mathbb{Q}^\star = \{\frac{0}{1}, \frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{1}, \ldots, \frac{1}{p-1}, \frac{2}{p-2}, \ldots, \frac{p-1}{1}, \ldots\} \; .$$

Si noti che il numero di peso 4 dato da $\frac{2}{2} = 1$, non è stato elencato, comparendo già nella lista come numero di peso 2: $\frac{1}{1} = 1$. Naturalmente queste omissioni saranno da fare in generale, come

più volte ricordato. È poi ovvio come numerare tutto $\mathbb{Q}$; basterà, per esempio, elencare un numero positivo e successivamente il negativo corrispondente, come segue

$$\mathbb{Q} = \{\frac{0}{1}, \frac{1}{1}, -\frac{1}{1}, \frac{1}{2}, -\frac{1}{2}, \frac{2}{1}, -\frac{2}{1}, \frac{1}{3}, -\frac{1}{3}, \frac{3}{1}, -\frac{3}{1}, \ldots, \frac{1}{p-1}, -\frac{1}{p-1}, \ldots, \} \ .$$

Dunque abbiamo $\operatorname{card}\mathbb{Z} = \operatorname{card}\mathbb{Q} = \aleph_0$. □

Teorema 2.6.4 $\mathbb{R}$ *non è numerabile.*

DIMOSTRAZIONE: Dimostreremo questo fatto verificando che nessuna successione di numeri reali strettamente compresi tra 0 e 1 può esaurire tutti i numeri reali compresi tra 0 e 1. Dunque, a maggiore ragione, la totalità dei numeri reali non può essere esaurita da alcuna successione degli stessi. Sia data una successione di numeri reali strettamente compresi tra 0 e 1 che penseremo rappresentati dai loro allineamenti decimali.

$$\begin{array}{lcl} \alpha_1 & = & 0, c_{11}c_{12}c_{13}\ldots c_{1n}\ldots \\ \alpha_2 & = & 0, c_{21}c_{22}c_{23}\ldots c_{2n}\ldots \\ \ldots & \ldots & \ldots\ldots\ldots\ldots\ldots \\ \alpha_n & = & 0, c_{n1}c_{n2}c_{n3}\ldots c_{nn}\ldots \\ \ldots & \ldots & \ldots\ldots\ldots\ldots\ldots \end{array}$$

Si consideri allora l'allineamento decimale, ottenuto con la seguente regola:

$$d_n = \begin{cases} 1, & \text{se } \ c_{n\,n} \neq 1, \\ 2, & \text{se } \ c_{n\,n} = 1. \end{cases}$$

Allora l'allineamento decimale $\delta = 0, d_1d_2d_3\ldots d_n\ldots$ rappresenta un numero reale strettamente compreso tra 0 e 1, diverso da ciascuno degli α_n. Infatti, $\delta \neq \alpha_n \, \forall n \in \mathbb{N}^+$ dal momento che δ è diverso da α_n almeno nella cifra di posto n. Si può concludere che $\operatorname{card}\mathbb{R} > \aleph_0$ poichè, essendo $\mathbb{R}$ soprainsieme di $\mathbb{Q}$ è certamente $\operatorname{card}\mathbb{Q} \leq \operatorname{card}\mathbb{R}$. □

Più in generale possiamo affermare che

Teorema 2.6.5 *Se A è un insieme infinito, allora* $\operatorname{card} A \geq \aleph_0$.

DIMOSTRAZIONE: A è infinito e quindi certamente non vuoto. Sia a_0 un elemento di A. $A \setminus \{a_0\} \neq \emptyset$, poiché, essendo A infinito ha più di un elemento. Sia dunque $a_1 \in A \setminus \{a_0\}$. Se sono stati scelti gli elementi distinti $\{a_1, a_2, \ldots a_n\} \subset A$, poiché A non può avere n elementi, esiste $a_{n+1} \in A \setminus \{a_1, a_2, \ldots a_n\}$. Dunque, per induzione, costruiamo un insieme $A' = \{a_0, a_1, \ldots, a_n, \ldots\} \subset A$, che è in corrispondenza biunivoca con $\mathbb{N}$. Esiste perciò un'applicazione iniettiva da $\mathbb{N}$ in A. Cioè $\operatorname{card} A \geq \aleph_0$. [5] □

[5] Per i puristi: in questo ragionamento "ingenuo si è totalmente sorvolato sul ruolo – fondamentale – dell'assioma di scelta!

Utilizzando il risultato del teorema precedente, si può dimostrare il seguente risultato, del quale omettiamo la dimostrazione.

Teorema 2.6.6 *Se A è un insieme infinito e N è un insieme infinito numerabile oppure è finito, allora* $\operatorname{card}(A \cup N) = \operatorname{card} A$. $\square$

Teorema 2.6.7 [di Cantor]. *Sia E un insieme e sia $\mathcal{P}(E)$ l'insieme dei sottoinsiemi (o delle parti) di E. Allora* $\operatorname{card} E < \operatorname{card} \mathcal{P}(E)$.

DIMOSTRAZIONE: È facile trovare un'applicazione iniettiva da E a $\mathcal{P}(E)$. Basta associare ad ogni elemento $a \in E$ il sottoinsieme singoletto $\{a\} \in \mathcal{P}(E)$. Dunque esistono applicazioni iniettive $\phi : E \to \mathcal{P}(E)$. Mostriamo che non può esserci un'applicazione biiettiva tra i due insiemi.

Per assurdo, si supponga data un'applicazione siffatta $\psi\colon E \to \mathcal{P}(E)$. Consideriamo allora il seguente sottoinsieme di E:

$$S = \{x \in E\colon x \notin \psi(x)\} \quad .$$

Poiché ψ è suriettiva esiste $s \in E$ tale che $S = \psi(s)$. Chiediamoci come sta s rispetto a S. Può essere $s \in S$? Se $s \in S$ allora deve godere della proprietà che definisce S e quindi $s \notin \psi(s) = S$. Dunque $s \in S \Rightarrow s \notin S$. Può essere $s \notin S = \psi(s)$? Se così fosse allora s godrebbe della proprietà per essere incluso in S; cioè $s \notin S \Rightarrow s \in S$. In conclusione otteniamo

$$s \in S \Leftrightarrow s \notin S \quad ,$$

che è una contraddizione. Alla contraddizione siamo giunti avendo supposto l'esistenza di un'applicazione biiettiva $\psi\colon E \to \mathcal{P}(E)$. Dunque una tale applicazione non può esistere, e quindi $\operatorname{card} E < \operatorname{card} \mathcal{P}(E)$. $\square$

Se $\operatorname{card} E = n$, cioè se $E = \{a_1, a_2, \ldots, a_n\}$, si riconosce facilmente che il numero degli elementi di $\mathcal{P}(E)$ è lo stesso delle n-ple ordinate di 0 e 1: infatti, all'n-pla $(1, 0, \ldots, 0)$ si faccia corrispondere il sottoinsieme $\{a_1\}$, all'n-pla $(0, 0, \ldots, 0)$, l'insieme vuoto, etc. In generale a un'n-pla nella quale al posto k compare 1 corrisponde un sottoinsieme che contiene l'elemento a_k, mentre se vi compare 0, l'elemento a_k non c'è nel sottoinsieme corrispondente. In questo modo si stabilisce una corrispondenza biunivoca tra n-ple di 0 e 1 e sottoinsiemi di E. Ma le n-ple distinte sono $2^n = 2^{\operatorname{card} E}$. Si estende la notazione

$$\operatorname{card} \mathcal{P}(E) = 2^{\operatorname{card} E} \quad ,$$

anche quando si tratta di insiemi infiniti.

Teorema 2.6.8 $\mathbb{R}$ *è equipotente con l'intervallo aperto* $(0, 1)$.

DIMOSTRAZIONE: Basta considerare l'applicazione $f\colon (0,1) \to \mathbb{R}$, definita da

$$f(x) = \tan\left(\frac{\pi}{2}(2 \cdot x - 1)\right) \quad . \quad \square$$

Si vede infine che l'intervallo aperto $(0,1)$ ha la stessa cardinalità delle successioni di 0 e 1.

Teorema 2.6.9

$$\operatorname{card}(0,1) = \operatorname{card} 2^{\mathbb{N}} = 2^{\aleph_0} \quad .$$

DIMOSTRAZIONE: Possiamo pensare di rappresentare i numeri dell'intervallo aperto $(0,1)$ come allineamenti binari: $0, b_1 b_2 \dots b_n \dots$, dove b_n assume solo i valori 0 o 1. Infatti già ci siamo soffermati sulla rappresentazione dei numeri reali come allineamenti decimali. Quello che si è fatto con la base dieci, si può ripetere usando una base diversa, in particolare la base due. L'allineamento $0, b_1 b_2 \dots b_n \dots$ rappresenta il numero reale di $(0,1)$ dato da

$$\beta = \sup\{\sum_{k=1}^{n} \frac{b_k}{2^k} : n \in \mathbb{N}^+\} \quad .$$

Naturalmente, dagli allineamenti binari sopra ricordati, vanno esclusi quelli che hanno periodo 1. Ma questi sono in numero di $\aleph_0$. Poiché $2^{\mathbb{N}} = (0,1) \cup \{\text{allineamenti binari di periodo } 1\}$, allora, per il Teorema 2.6.6

$$\operatorname{card} 2^{\mathbb{N}} = 2^{\aleph_0} = \operatorname{card}(0,1) \quad .$$

E infine, poiché $\operatorname{card}(0,1) = \operatorname{card} \mathbb{R}$, concludiamo che

$$\operatorname{card} \mathbb{R} = 2^{\aleph_0} > \aleph_0 \quad .$$

La cardinalità $2^{\aleph_0}$ si dice anche la cardinalità del *continuo* e si indica anche con la lettera gotica (fraktur) c:

$$\mathfrak{c} = 2^{\aleph_0} \quad .$$

Vogliamo infine ricordare un ultimo aspetto un po' paradossale della cardinalità degli insiemi (in particolare, di $\mathbb{R}$).

Teorema 2.6.10

$$\operatorname{card} \mathbb{R}^2 = \operatorname{card} \mathbb{R} \quad ;$$

Più in generale

$$\operatorname{card} \mathbb{R}^n = \operatorname{card} \mathbb{R} \quad ,$$

con $n \in \mathbb{N}^+$.

DIMOSTRAZIONE: Osserviamo che vi è una corrispondenza biunivoca tra $(0,1) \times (0,1)$ e $(0,1)$.

Se $(x,y) \in (0,1)^2$, essendo le rappresentazioni decimali di x e y rispettivamente $x = 0, a_1 a_2 \dots a_n \dots$ e $y = 0, b_1 b_2 \dots b_n \dots$, al punto (x,y) del quadrato possiamo associare il punto z dell'intervallo $(0,1)$ così individuato $z = 0, a_1 b_1 a_2 b_2 \dots a_n b_n \dots$. La corrispondenza è chiaramente iniettiva e suriettiva. Dunque

$$\operatorname{card}(0,1)^2 = \operatorname{card}(0,1) \quad .$$

Si può dimostrare che se A è equipotente con C e B è equipotente con D, allora $A \times B$ è equipotente con $C \times D$. Allora $(0,1)^2$ è equipotente con $\mathbb{R}^2$, essendo $(0,1)$ equipotente con $\mathbb{R}$. Perciò si ottiene finalmente

$$\operatorname{card} \mathbb{R}^2 = \operatorname{card} \mathbb{R} \quad .$$

Per induzione si può facilmente dimostrare che

$$\operatorname{card} \mathbb{R}^n = \operatorname{card} \mathbb{R} \quad ,$$

per ogni numero naturale $n \geq 1$, cioè

$$\mathfrak{c}^n = \mathfrak{c} \quad . \quad \square$$

2.7 I numeri complessi

Ci accingiamo a considerare un'ulteriore estensione di campi numerici, precisamente quella dal campo dei numeri reali al campo dei numeri complessi $\mathbb{C}$. Questa estensione permette di sanare un'ulteriore incompletezza presente in $\mathbb{R}$. Abbiamo visto che le estensioni da $\mathbb{N}$ a $\mathbb{Z}$ sono state giustificate dalla necessità di trovare soluzione in ogni caso all'equazione $a+x=b$, mentre l'estensione da $\mathbb{Z}$ a $\mathbb{Q}$ permetteva di dare soluzione ad ogni equazione del tipo $a\cdot x=b$, con $a\neq 0$. Il passaggio da $\mathbb{Q}$ a $\mathbb{R}$ permette di sanare eventuali lacune presenti in $\mathbb{Q}$, ma in $\mathbb{R}$ troviamo ancora equazioni algebriche prive di soluzione. Infatti $x^2+1=0$ non ha soluzioni in $\mathbb{R}$, dal momento che, per ogni $x\in\mathbb{R}$ si ha $x^2+1\geq 1$. Dopo lunga maturazione dei concetti a partire dal 1500, i matematici sono pervenuti ad una soluzione del problema nei termini che seguono.

Consideriamo l'insieme delle coppie di numeri reali $\mathbb{R}\times\mathbb{R}$ e definiamo in esso due operazioni

$$(a,b)+(c,d) = (a+c,b+d) \quad , \tag{2.24}$$
$$(a,b)\cdot(c,d) = (ac-bd,ad+bc) \quad . \tag{2.25}$$

Non è difficile (ma è certamente noioso) verificare che le operazioni sopra definite sono associative, commutative e che vale la distributività della moltiplicazione rispetto all'addizione. Le coppie del tipo $(0,0)$ e $(1,0)$ fungono da elementi neutri rispetto all'addizione e alla moltiplicazione rispettivamente. Infatti qualunque sia (a,b), $(a,b)+(0,0)=(a+0,b+0)=(a,b)$ e $(a,b)\cdot(1,0)=(a\cdot 1-b\cdot 0,a\cdot 0+b\cdot 1)=(a,b)$; si tenga conto inoltre della commutatività. Perciò, dal punto di vista algebrico, l'insieme $\mathbb{R}\times\mathbb{R}$ con le due operazioni dette è un anello commutativo con unità. L'uguglianza tra due elementi si intende definita come segue: $(a_1,b_1)=(a_2,b_2)$ se e solo se $a_1=a_2$ e $b_1=b_2$. Perciò l'elemento $(a,b)\neq(0,0)$ se **non** è $a=0$ e $b=0$; cioè se $a^2+b^2\neq 0$.

Dimostriamo ora che per ogni coppia $(a,b)\neq(0,0)$ esiste una coppia (α,β) tale che $(\alpha,\beta)\cdot(a,b)=(1,0)$. Cioè che per ogni coppia $(a,b)\in\mathbb{R}\times\mathbb{R}$ diversa dalla coppia nulla esiste una coppia che moltiplicata per essa produce la coppia unità. Eseguendo la moltiplicazione, si trova

$$(\alpha,\beta)\cdot(a,b)=(\alpha\cdot a-\beta\cdot b,\alpha\cdot b+\beta\cdot a) \quad .$$

Se si impone che tale prodotto sia uguale a $(1,0)$, si trova il seguente sistema nelle incognite α e β

$$\begin{cases} \alpha\cdot a-\beta\cdot b = 1 \\ \alpha\cdot b+\beta\cdot a = 0. \end{cases} \tag{2.26}$$

Moltiplicando la prima equazione per a, la seconda per b e sommando si trova

$$\alpha\cdot(a^2+b^2)=a \quad .$$

Moltiplicando la prima equazione per $-b$, la seconda per a e sommando si trova

$$\beta\cdot(a^2+b^2)=-b \quad .$$

Dunque necessariamente si trovano per α e β i seguenti valori

$$\begin{cases} \alpha &= \dfrac{a}{a^2+b^2} \\ \beta &= \dfrac{-b}{a^2+b^2}. \end{cases} \tag{2.27}$$

È stata cosí stabilita l'unicità dell'inverso di (a,b), ammesso che esso esista. Ma un calcolo immediato mostra che

$$(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}) \cdot (a,b) = (1,0) \quad . \tag{2.28}$$

Il che stabilisce l'esistenza dell'inverso di (a,b).

Dunque il sistema numerico $(\mathbb{R}\times\mathbb{R}, +, \cdot)$ che abbiamo costruito è un sistema numerico che dal punto di vista algebrico è un corpo communtativo o campo. Vedremo che in esso non può essere coerentemente definita una relazione d'ordine compatibile con le operazioni. Chiameremo *corpo o campo dei numeri complessi* questo sistema numerico; lo indicheremo con $\mathbb{C}$.

Osserviamo che questo campo dei numeri complessi estende quello dei numeri reali. Infatti se consideriamo i numeri complessi del tipo

$$\mathbb{R}' = \{(x,0) : x \in \mathbb{R}\} \quad ,$$

non solo $\mathbb{R}'$ è in corrispondenza biunivoca con $\mathbb{R}$, ma la corrispondenza naturale che si può stabilire conserva le operazioni. Precisamente se indichiamo con $\varphi : \mathbb{R}' \to \mathbb{R}$ l'applicazione definita da $\varphi(x,0) := x$, abbiamo anche che

$$\varphi((x,0)+(u,0)) = \varphi((x+u,0)) = x+u = \varphi((x,0)) + \varphi((u,0)) \quad \text{e}$$

$$\begin{aligned} \varphi((x,0)\cdot(u,0)) &= \varphi((x\cdot u - 0\cdot 0, x\cdot 0 + 0\cdot u)) = \\ &= \varphi((x\cdot u,0)) = x\cdot u = \varphi((x,0))\cdot\varphi((u,0)) \,. \end{aligned}$$

Cioè, se indichiamo con $x' = (x,0)$ e $u' = (u,0)$ gli elementi di $\mathbb{R}'$, si ha $\varphi(x'+u') = \varphi(x') + \varphi(u')$ e $\varphi(x'\cdot u') = \varphi(x')\cdot\varphi(u')$. Dunque $\mathbb{R}'$ si comporta dal punto di vista algebrico come una copia di $\mathbb{R}$. Si dice che $\mathbb{R}'$ è *isomorfo* a $\mathbb{R}$. Poiché $\mathbb{C}$ contiene un sottocorpo isomorfo ad $\mathbb{R}$ esso si può considerare un'*estensione* di $\mathbb{R}$. Cerchiamo ora di semplificare la scrittura dei numeri complessi. Evidentemente si ha $(a,b) = (a,0)+(0,b) = (a,0)+(b,0)\cdot(0,1)$. Poiché $(a,0)$ è in corrispondenza biunivoca con a e $(b,0)$ con b, potremo scrivere piú semplicemente $(a,b) = a + b\cdot(0,1)$. L'unico simbolo non riconducibile ai numeri reali che conosciamo è la coppia $(0,1)$. Da tempo si è deciso di indicare questa coppia con il simbolo i, chiamato l'*unità immaginaria*. Allora il numero complesso dato dalla coppia (a,b) sarà indicata piú semplicemente con $a+i\,b$. È facile valutare che $(0,1)\cdot(0,1) = (-1,0)$, cioè, nella nuova notazione

$$i\cdot i = i^2 = -1 \quad . \tag{2.29}$$

Questa è l'unica regola nuova che permette di eseguire i calcoli algebrici con i numeri complessi. Infatti, usando questa regola, se $z_1 = x_1 + i\,y_1$ e $z_2 = x_2 + i\,y_2$, si trova $z_1+z_2 = (x_1+x_2)+i\,(y_1+y_2)$ e $z_1\cdot z_2 = x_1\cdot x_2 - y_1\cdot y_2 + i\,(x_1\cdot y_2 + y_1\cdot x_2)$.

La rappresentazione dei numeri complessi nella forma $z = x + i\,y$, con $x, y \in \mathbb{R}$, si dice *forma algebrica* o *di Eulero* dei numeri complessi. x si dice la *parte reale* del numero complesso z, e si denota con $x = \Re z$; y si dice la *parte immaginaria* del numero complesso z, e si denota con $y = \Im z$. Dunque, in modo tautologico, per ogni $z \in \mathbb{C}$, si ha

$$z = \Re z + i\ \Im z \quad . \tag{2.30}$$

Evidentemente $z_1 = z_2$ se e solo se $\Re z_1 = \Re z_2$ e $\Im z_1 = \Im z_2$.

Avevamo preannunciato che $\mathbb{C}$ non può ricevere un ordine che sia compatibile con le operazioni e coerente con l'ordine dei numeri reali. La ragione di ciò si può agevolmente riconoscere nell'equazione (2.29). Infatti se $\mathbb{C}$ ammettesse un ordine totale compatibile con le operazioni, sappiamo che, per la compatibilità con l'operazione di moltiplicazione, ogni numero elevato al quadrato, dovrebbe essere un numero positivo. Poiché $\mathbb{C}$ è estensione del campo reale il numero -1 dovrebbe essere negativo: $-1 < 0$. Ma ecco che $i^2 = -1$. Dunque ci sarebbe un numero complesso non nullo, e precisamente i, che ha un quadrato negativo, contro una proprietà di ogni ordine compatibile con le operazioni e coerente con l'ordine in $\mathbb{R}$.

2.7.1 Coniugio di numeri complessi

Possiamo ora considerare un'ulteriore operazione (non algebrica) sul campo dei numeri complessi: l'operazione di *coniugio*. Dato un numero complesso $z = x + i\ y$ diremo *coniugato di* z il numero complesso $\omega(z) = \bar{z} = x - i\ y$. È facile riconoscere che l'operazione di coniugio $\omega : \mathbb{C} \to \mathbb{C}$ è un'applicazione biiettiva che rispetta le operazioni; infatti

$$\begin{aligned} \omega(z_1 + z_2) = \omega(x_1 + x_2 + i\ (y_1 + y_2)) &= x_1 + x_2 - i\ (y_1 + y_2) = \\ &= \omega(z_1) + \omega(z_2) \end{aligned} \tag{2.31}$$

e

$$\begin{aligned} \omega(z_1 \cdot z_2) &= \omega(x_1x_2 - y_1y_2 + i\ (x_1y_2 + x_2y_1)) = \\ &= x_1x_2 - y_1y_2 - i\ (x_1y_2 + x_2y_1) = \omega(z_1) \cdot \omega(z_2)\,. \end{aligned} \tag{2.32}$$

Vale inoltre $\omega^2(z) = \omega(\omega(x + i\ y)) = \omega(x - i\ y) = x + i\ y = z$, cioè l'operazione di coniugio è *involutoria*.

Conviene osservare che sono autoconiugati tutti e soli i numeri complessi reali, cioè quelli che hanno parte immaginaria nulla. Infatti se $z = a + i\,0 = a$ allora $\omega(z) = a - i\,0 = a$. Viceversa se $\omega(z) = z$, ossia se $a - ib = a + i\,b$ allora $2i\,b = 0$ e quindi $b = 0$, ossia $\Im(z) = 0$.

Se $P(z)$ è un polinomio nella variabile complessa z, a coefficienti complessi, allora, indicando per brevità con una sopralineatura il passaggio al complesso coniugato, avremo che

$$\overline{P(z)} = \overline{P}(\overline{z}) \quad , \tag{2.33}$$

dove, se $P(u) = a_nu^n + a_{n-1}u^{n-1} + \ldots + a_1u + a_0$, $\overline{P}(u) = \overline{a_n}u^n + \overline{a_{n-1}}u^{n-1} + \ldots + \overline{a_1}u + \overline{a_0}$, che si dice il *polinomio coniugato* di $P(z)$. Infatti $\overline{a_nz^n + a_{n-1}z^{n-1} + \ldots + a_1z + a_0} = \overline{a_nz^n} +$

$\overline{a_{n-1}z^{n-1}} + \ldots + \overline{+a_1 z} + \overline{a_0}$ perché il coniugato di una somma è la somma dei coniugati e, infine, ricordando che il coniugato di un prodotto è il prodotto dei coniugati, si ottiene ulteriormente $\overline{P(z)} = \overline{a_n}(\overline{z})^n + \overline{a_{n-1}}(\overline{z})^{n-1} + \ldots + \overline{a_1}\,\overline{z} + \overline{a_0} = \overline{P}(\overline{z})$.

Se definiamo *radice* di un polinomio a coefficienti complessi $P(z)$ un numero α tale che $P(\alpha) = 0$, allora possiamo concludere che ogni polinomio a coefficienti complessi che abbia una radice α è tale che il polinomio coniugato ha come radice $\overline{\alpha}$. In particolare, se i coefficienti sono reali, il polinomio coniugato coincide con il polinomio di partenza e si può concludere che se un polinomio a coefficienti reali ha radice α, allora ha anche la radice $\overline{\alpha}$.

2.7.2 Forma polare o trigonometrica dei numeri complessi

Supponiamo che z sia un numero complesso non nullo. Perciò, se $z = x + i\,y \neq 0$, è certamente $x^2 + y^2 > 0$. La radice quadrata di questo numero si dice il *modulo* di z, denotato con $|z|$. Dunque $|z| = \sqrt{x^2 + y^2}$. Allora per $z \neq 0$ vale

$$z = x + i\,y = \sqrt{x^2 + y^2} \cdot \left(\frac{x}{\sqrt{x^2 + y^2}} + i\,\frac{y}{\sqrt{x^2 + y^2}}\right) \quad .$$

È noto dalla definizione delle funzioni trigonometriche che esiste un unico numero ϑ, con $0 \leq \vartheta < 2\pi$, tale che $\cos\vartheta = \dfrac{x}{\sqrt{x^2 + y^2}}$ e $\operatorname{sen}\vartheta = \dfrac{y}{\sqrt{x^2 + y^2}}$ e dunque si ottiene

$$z = x + i\,y = \sqrt{x^2 + y^2} \cdot (\cos\vartheta + i \operatorname{sen}\vartheta) = |z| \cdot (\cos\vartheta + i \operatorname{sen}\vartheta)\,. \tag{2.34}$$

Il numero ϑ si dice l'*argomento* del numero complesso z. Viceversa, se sono dati il modulo e l'argomento, è individuato il numero complesso z, che ha parte reale $\Re z = |z| \cdot \cos\vartheta$ e parte immaginaria data da $\Im z = |z| \cdot \operatorname{sen}\vartheta$, cioè $z = |z|\cos\vartheta + i\,|z|\operatorname{sen}\vartheta$.

Piú precisamente, se $0 \leq \vartheta < 2\pi$ oppure se $-\pi \leq \vartheta < \pi$, ϑ si dice il *valore principale dell'argomento*. L'argomento di un numero complesso non nullo è infatti determinato a meno di multipli di 2π; due argomenti che differiscono per multipli di 2π hanno uguali il seno e il coseno e quindi individuano lo stesso numero complesso, se il modulo è uguale. Infine se $z = 0$ evidentemente il modulo è nullo, mentre l'argomento può essere un numero qualunque. Se indichiamo con ρ il modulo di z, indicheremo z con la scrittura $z = \rho(\cos\vartheta + i \operatorname{sen}\vartheta)$ (detta talvolta rappresentazione trigonometrica del numero complesso) o con la scrittura formale $z = [\rho, \vartheta]$ (detta talvolta scrittura polare del numero complesso). Però spesso gli attributi trigonometrico e polare saranno usati come sinonimi. Infine, nelle applicazioni, sarà spesso usata l'utilissima notazione esponenziale $z = \rho e^{i\vartheta}$, che sarà pienamente giustificata dopo che avremo definito l'esponenziale d'argomento complesso e le relative formule d'Eulero.

Notiamo infine esplicitamente quanto è stato implicitamente detto nelle righe precedenti: dati due numeri complessi z_1 e z_2, scritti in forma trigonometrica $z_1 = [\rho_1, \vartheta_1]$ e $z_2 = [\rho_2, \vartheta_2]$ abbiamo che $z_1 = z_2$ se e solo se

$$\begin{cases} \rho_1 &= \rho_2 \\ \vartheta_1 &= \vartheta_2 + k \cdot 2\pi,\ k \in \mathbb{Z}\,. \end{cases} \tag{2.35}$$

Moltiplicazione e notazione trigonometrica

La forma trigonometrica o polare dei numeri complessi è particolarmente significativa quando l'operazione da eseguire sui numeri complessi è la moltiplicazione. Siano dunque $z_1 = \rho_1 \cdot (\cos\vartheta_1 + i\,\text{sen}\,\vartheta_1)$ e $z_2 = \rho_2 \cdot (\cos\vartheta_2 + i\,\text{sen}\,\vartheta_2)$.

$$\begin{aligned} z_1 \cdot z_2 &= \rho_1 \cdot (\cos\vartheta_1 + i\,\text{sen}\,\vartheta_1) \cdot \rho_2 \cdot (\cos\vartheta_2 + i\,\text{sen}\,\vartheta_2) = \\ &= \rho_1 \cdot \rho_2 \cdot [\cos\vartheta_1 \cdot \cos\vartheta_2 - \text{sen}\,\vartheta_1 \cdot \text{sen}\,\vartheta_2 + \\ &\quad + i(\cos\vartheta_1 \cdot \text{sen}\,\vartheta_2 + \text{sen}\,\vartheta_1 \cdot \cos\vartheta_2)] = \\ &= \rho_1 \cdot \rho_2 \cdot [\cos(\vartheta_1 + \vartheta_2) + i\,\text{sen}\,(\vartheta_1 + \vartheta_2)] = \\ &= [\rho_1 \cdot \rho_2, \vartheta_1 + \vartheta_2]\,. \end{aligned} \tag{2.36}$$

Dunque il prodotto di due numeri complessi è un numero complesso che ha come modulo il prodotto dei moduli e come argomento la somma degli argomenti. È subito chiaro da quest'ultima osservazione che se anche z_1 e z_2 usano l'argomento principale come argomento, non è detto che il loro prodotto abbia come argomento un argomento principale. Ovviamente, ci si potrà ridurre ad un argomento principale sottraendo (o aggiungendo) qualche multiplo di 2π. L'unità è rappresentata in forma polare da $[1, 0]$, i numeri reali $x > 0$ da $[x, 0]$, i numeri reali $x < 0$ da $[\,|x|, \pi]$. Il numero complesso 0 si può rappresentare con $[0, 0]$ o con $[0, \varphi]$, dove φ è arbitrario. Si riconosce facilmente che il reciproco di un numero $z = [\rho, \vartheta]$, con $z \neq 0$, è il numero $[\frac{1}{\rho}, -\vartheta]$ (infatti moltiplicato per $[\rho, \vartheta]$ dà $[1, 0]$). Perciò, se $z_2 \neq 0$, si ha $\dfrac{z_1}{z_2} = \left[\dfrac{\rho_1}{\rho_2}, \vartheta_1 - \vartheta_2\right]$. Le potenze di un numero complesso $z = [\rho, \vartheta]$ sono allora agevolmente espresse dalle Formule di De Moivre

$$z^n = [\rho, \theta]^n = [\rho^n, n\theta], \quad (n \in \mathbb{Z}) \quad . \tag{2.37}$$

Infine, è facile riconoscere che se $z = [\rho, \vartheta]$, allora $\overline{z} = \omega(z) = [\rho, -\vartheta]$.

2.7.3 Rappresentazione geometrica dei numeri complessi

I numeri complessi sono individuati da una coppia di numeri reali, $z = x + i\,y$ con $x, y \in \mathbb{R}$, perciò ogni numero complesso z si può porre in corrispondenza biunivoca con i punti di un piano cartesiano $\mathbb{R}^2$. Il piano cartesiano, se si pensa rappresentativo dei numeri complessi, si dice piano di Argand - Gauss[6].

Pensando alla rappresentazione trigonometrica di un numero complesso, si vede che il modulo $|z| = \rho$ è la distanza tra l'origine delle coordinate e il punto z del piano di Gauss, che rappresenta il numero complesso. Invece l'argomento è l'angolo, preferibilmente espresso in radianti, formato dal semiasse positivo delle x (della parte reale di z), con la semiretta che congiunge l'origine O con z.

[6] Jean Robert Argand (1768–1822); Carl Friedrich Gauß (1777–1855). Gauß usò per la prima volta la rappresentazione dei numeri complessi come punti del piano, nella sua tesi nel 1799; aveva scoperto questa rappresentazione nel 1797. Caspar Wessel usò la rappresentazione in una memoria presentata all'Accademia danese delle Scienze nel 1797, pubblicata nel 1798-99. Argand la propose nel suo "Essai sur une manière de représenter les quantités imaginaires dans les constructions géométriques nel 1806. Infine a Gauß si deve il nome di "numeri complessi (1831), Werke, II, pag. 102.

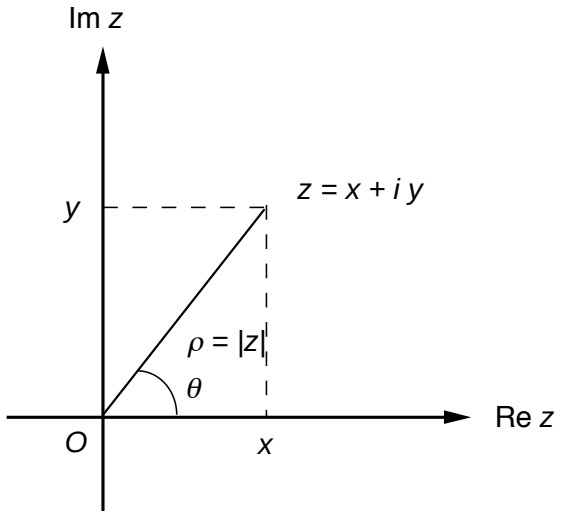

Figura 2.1: Piano di Argand-Gauss; rappresentazione algebrica e trigonometrica di un numero complesso.

La rappresentazione geometrica è particolarmente utile per guidare il passaggio tra la scrittura algebrica e quella trigonometrica dei numeri complessi. Se, per esempio è dato il numero $z = -1 + i\sqrt{3}$, posizionando il numero sul piano di Gauss, si riconosce facilmente che l'argomento

(principale) del numero è $\frac{2}{3}\pi$, mentre il modulo si calcola agevolmente: $\rho = \sqrt{1+3} = 2$. Se vogliamo calcolare la potenza 10.ma di z, la formula di De Moivre ci fornisce immediatamente $z^{10} = [2, \frac{2}{3}\pi]^{10} = [2^{10}, \frac{20}{3}\pi] = [2^{10}, \frac{2}{3}\pi] = 2^{10} \cdot (-\frac{1}{2} + i\,\frac{\sqrt{3}}{2}) = -2^9 + i\,\sqrt{3} \cdot 2^9$. Qui si è tenuto conto che $20 = 6 \cdot 3 + 2$ e quindi che $\frac{20}{3}\pi = 6 \cdot \pi + \frac{2}{3}\pi = 3 \cdot 2\pi + \frac{2}{3}\pi$. Si pensi a quanti calcoli si sarebbero dovuti fare per elevare alla decima potenza il binomio $(-1 + i\,\sqrt{3})$, raccogliendo successivamente i termini reali e quelli contenenti il fattore i.

La rappresentazione geometrica mette anche in evidenza che l'addizione tra numeri complessi, che avviene componente per componente, corrisponde all'addizione di vettori piani, mentre la moltiplicazione di $z = [\rho, \vartheta]$ per $w = [r, \varphi]$ corrisponde a un cambiamento di scala o omotetia di centro l'origine e di rapporto r e a una rotazione di misura φ intorno all'origine. La rotazione avviene in senso antiorario se $\varphi > 0$.

2.7.4 L'equazione $z^n = \gamma$

Abbiamo già trattato il problema della risoluzione dell'equazione $x^n = a$ nel campo reale. Abbiamo trovato che se $a > 0$ e n è pari vi sono sempre due soluzioni distinte in $\mathbb{R}$ dell'equazione, mentre se n è dispari c'è sempre una e una sola soluzione in $\mathbb{R}$, quale che sia il numero reale a. Infatti, nel caso $a > 0$ e n pari, oltre alla soluzione $x = \sqrt[n]{a}$ c'è anche la soluzione $x = -\sqrt[n]{a}$.

Vogliamo ora affrontare lo stesso problema nel campo complesso. In questo ambiente la soluzione è molto piú simmetrica e simpatica. Infatti si troveranno sempre n soluzioni distinte se γ è non nullo. Abbiamo il seguente

Teorema 2.7.1 *Sia $\gamma \neq 0$ un numero complesso arbitrario. Allora l'equazione*

$$z^n = \gamma \tag{2.38}$$

ha esattamente n soluzioni distinte, che si dicono le radici n-esime del numero complesso γ.

DIMOSTRAZIONE: Il numero complesso assegnato $\gamma \neq 0$ ha forma trigonometrica $\gamma = [r, \varphi]$, dove r è il modulo di γ e φ il suo argomento. Noi cerchiamo un numero complesso z tale che $z^n = \gamma$ che converrà venga anch'esso individuato con la forma trigonometrica; cioè lo cercheremo nella forma $z = [\rho, \vartheta]$, con modulo ρ e argomento ϑ da determinare.

Dunque deve valere l'equazione

$$z^n = [\rho, \vartheta]^n = [\rho^n, n \cdot \vartheta] = [r, \varphi] = \gamma\,.$$

Qui abbiamo tenuto conto delle formule di De Moivre precedentemente dimostrate sulle potenze dei numeri complessi. In base alla condizione d'uguaglianza dei numeri complessi in forma trigonometrica (2.35) dovranno perciò valere le condizioni

$$\begin{cases} \rho^n &= r \\ n \cdot \vartheta &= \varphi + k \cdot 2\pi,\ k \in \mathbb{Z}\,. \end{cases}$$

Questo sistema ha le seguenti soluzioni

$$\begin{cases} \rho &= \sqrt[n]{r} \\ \vartheta_k &= \dfrac{\varphi}{n} + k \cdot \dfrac{2\pi}{n},\ k \in \mathbb{Z}\,. \end{cases} \tag{2.39}$$

Può sembrare che ci siano infinite soluzioni, dal momento che gli argomenti dipendono da un intero relativo $k \in \mathbb{Z}$. In realtà il numero delle soluzioni distinte è esattamente n. Infatti, se a k attribuiamo i valori $0, 1, \ldots, n-1$ i numeri complessi ottenuti sono tutti distinti. Ma se $k = n$, si trova che $\vartheta_n = \dfrac{\varphi}{n} + n \cdot \dfrac{2\pi}{n} = \dfrac{\varphi}{n} + 2\pi = \vartheta_0 + 2\pi$. Ma i numeri $z_0 = [\sqrt[n]{r}, \vartheta_0]$ e $z_n = [\sqrt[n]{r}, \vartheta_n]$ sono uguali perché hanno lo stesso modulo mentre gli argomenti differiscono per 2π. Dunque le n soluzioni distinte di $z^n = \gamma$ ($\gamma \neq 0$) sono $z_k = [\rho, \vartheta_k]$, $k = 0, 1, \ldots, n-1$, con

$$\begin{cases} \rho &= \sqrt[n]{r} \\ \vartheta_k &= \dfrac{\varphi}{n} + k \cdot \dfrac{2\pi}{n},\ k \in \{0, 1, \ldots, n-1\}\,. \end{cases} \tag{2.40}$$

□

Le soluzioni dell'equazione $z^n = \gamma$ sono dunque tutte collocate sulla circonferenza di centro l'origine e raggio $\sqrt[n]{r}$; gli argomenti partono da $\dfrac{\varphi}{n}$ e sono distanziati l'uno dall'altro di un angolo uguale a $\dfrac{2\pi}{n}$. Sono dunque ai vertici di un poligono regolare di n lati inscritto in una circonferenza di raggio $\sqrt[n]{r}$. È chiaro che per descrivere tutte le soluzioni dell'equazione $z^n = \gamma$, si possono scegliere n valori distinti consecutivi di $k \in \mathbb{Z}$, invece dei valori $0, 1, \ldots, n-1$ che noi abbiamo scelto, per semplicità.

Esempio 2.7.1 *Se $\gamma = 3 + 4i$, si trovino tutte le soluzione in $\mathbb{C}$ dell'equazione*

$$z^7 = \gamma\,.$$

Svolgimento: L'equazione $z^7 = 3 + 4i = [r, \varphi]$, dove $r = \sqrt{25} = 5$ e $\varphi = \arccos\dfrac{3}{5} \approx 0,927295$ rad $\approx 53^o 7' 48''$, ha le seguenti soluzioni

$$\begin{aligned} \rho &= \sqrt[7]{5} \approx 1,2585 \\ \vartheta_k &= \frac{\arccos\frac{3}{5}}{7} + k\frac{2\pi}{7} \approx 0,132471 + k \cdot 0,897598,\ k = 0, 1, \ldots, 6\ .\square \end{aligned}$$

2.7.5 Le radici n-esime dell'unità

Le soluzioni dell'equazione

$$z^n = 1 \quad , \tag{2.41}$$

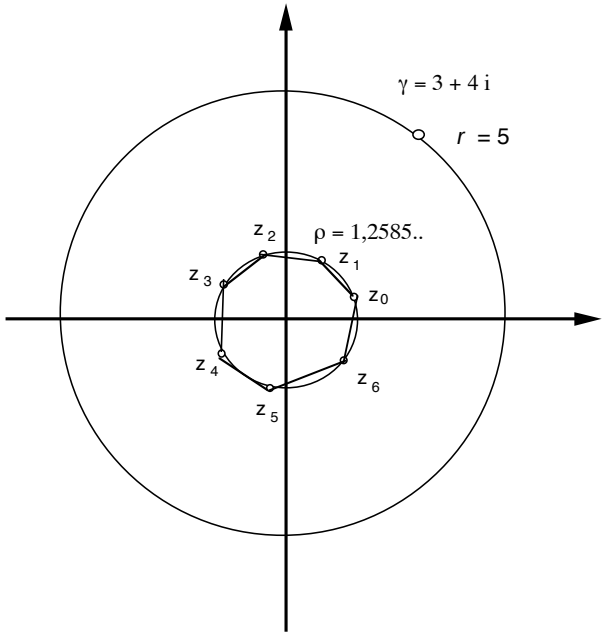

Figura 2.2: Rappresentazione delle soluzioni dell'equazione $z^7 = 3 + 4i$.

si dicono radici n-esime dell'unità. Sulla base della precedente discussione, le radici n-esime dell'unità sono numeri complessi aventi modulo 1 e argomento $\vartheta_k = k \cdot \dfrac{2\pi}{n},\ k = 0, 1, \ldots, n-1$. Cioè

sono i numeri (solitamente indicati con ω_k)

$$\omega_k = [1, k \cdot \frac{2\pi}{n}] = \cos(k \cdot \frac{2\pi}{n}) + i \text{ sen } (k \cdot \frac{2\pi}{n}) = e^{k \cdot \frac{2\pi}{n} i} . \tag{2.42}$$

Qui è stata utilizzata anche la notazione esponenziale che ancora non abbiamo giustificato, perché essa è estremamente espressiva e frequentemente utilizzata nelle applicazioni. Una proprietà interessante delle radici n-esime dell'unità da mettere in rilievo è che il loro insieme forma gruppo rispetto all'operazione di moltiplicazione in $\mathbb{C}$. Infatti si riconosce facilmente che

$$\omega_k \cdot \omega_h = \omega_{k+h} , \tag{2.43}$$

dove la somma $k+h$ deve intendersi fatta MODULO n, cioè al posto di $k+h$ in $\mathbb{N}$ si deve considerare il numero $r \in \{0, 1, \ldots, n-1\}$ che è il resto della divisione in $\mathbb{N}$ di $k+h$ per n. Dunque se, per esempio, $n = 7$, allora $\omega_2 \cdot \omega_4 = \omega_6$, ma $\omega_4 \cdot \omega_3 = \omega_7 = \omega_0 = 1$. L'elemento unità del gruppo è $\omega_0 = 1$, mentre le proprietà associativa e commutativa della moltiplicazione sono automaticamente soddisfatte, una volta riconosciuto che il prodotto di due elementi dell'insieme è ancora un elemento dell'insieme. Ogni elemento ω_h ha come elemento inverso ω_{n-h}, per $h = 1, 2, \ldots, n-1$. Ovviamente $\omega_0 = 1$ è l'inverso di sé stesso.

È interessante osservare che il gruppo è, ovviamente, stabile per l'elevazione a potenza dei suoi elementi e che si ha $\omega_h^k = \omega_k^h = \omega_{h \cdot k}$, dove l'indice $h \cdot k$ si deve intendere MOD n. Ossia $h \cdot k = r + m \cdot n$, con $r \in \{0, 1, \ldots, n-1\}$. Dunque $\omega_{h \cdot k} = \omega_r$. Ciò si riconosce facilmente usando la forma "polare $\omega_h = [1, h \cdot \frac{2\pi}{n}]$ e quindi $\omega_h^k = [1, h \cdot k \cdot \frac{2\pi}{n}] = \omega_k^h$. Un'altra osservazione importante, valida per le radici dell'unità $\omega \neq 1$ è la seguente.

Osservazione 2.7.1 *Se $\omega \neq 1$, vale*

$$1 + \omega + \omega^2 + \ldots + \omega^{n-1} = 0 . \tag{2.44}$$

DIMOSTRAZIONE: Infatti sappiamo che, se ω è radice dell'unità, $\omega^n = 1$ e quindi $1 - \omega^n = 0$. Ma $1 - \omega^n = (1 - \omega)(1 + \omega + \omega^2 + \ldots + \omega^{n-1})$. Ossia

$$(1 - \omega) \cdot (1 + \omega + \omega^2 + \ldots + \omega^{n-1}) = 0 .$$

Dunque se $\omega \neq 1$, ossia se $(1 - \omega) \neq 0$, vale la proprietà (2.44), che volevamo dimostrare, cioè

$$1 + \omega + \omega^2 + \ldots + \omega^{n-1} = 0 .$$

□

Quest'osservazione ci torna utile per dimostrare la seguente

Proposizione 2.7.1 *Siano ω_h e ω_k ($h, k = 0, 1, \ldots, n-1$) due radici dell'unità. Allora abbiamo*

$$1 + \omega_h \cdot \overline{\omega}_k + \omega_h^2 \cdot {\overline{\omega}_k}^2 + \ldots + \omega_h^{n-1} \cdot {\overline{\omega}_k}^{n-1} = \\ = \sum_{i=0}^{n-1} \omega_h^i \cdot {\overline{\omega}_k}^i = n \cdot \delta_{h,k} , \tag{2.45}$$

dove $\delta_{h,k}$ *è la "delta di Kronecker*[7] *che vale* 1 *se* $h = k$ *e* 0 *se* $h \neq k$.

DIMOSTRAZIONE: Osserviamo che $\overline{\omega}_k = \overline{[1, k \cdot \frac{2\pi}{n}]} = [1, -k \cdot \frac{2\pi}{n}] = \omega_{-k}$ e che perciò $\overline{\omega}_k{}^m = \omega_{-k}^m$. Allora abbiamo

$$\begin{aligned} 1 + \omega_h \cdot \overline{\omega}_k \quad &+ \quad \omega_h^2 \cdot \overline{\omega}_k{}^2 + \ldots + \omega_h^{n-1} \cdot \overline{\omega}_k{}^{n-1} = 1 + \omega_h \cdot \omega_{-k} + \omega_h^2 \cdot \omega_{-k}^2 + \\ \ldots \quad &+ \quad \omega_h^{n-1} \cdot \omega_{-k}^{n-1} = 1 + \omega_{h-k} + \omega_{h-k}^2 + \ldots + \omega_{h-k}^{n-1} \,. \end{aligned}$$

Se $h = k$, allora $\omega_{h-k} = \omega_0 = 1$ e la somma è una di n addendi ognuno uguale a 1 e perciò vale n. Se $h \neq k$, $\omega_{h-k} \neq 1$ è una radice dell'unità e, in forza dell'uguaglianza (2.44), otteniamo che

$$1 + \omega_{h-k} + \omega_{h-k}^2 + \ldots + \omega_{h-k}^{n-1} = 0 \,.$$

Dunque vale

$$\sum_{i=0}^{n-1} \omega_h^i \cdot \overline{\omega}_k{}^i = n \cdot \delta_{h,k} \,.$$

□

Questa relazione è utilissima nel calcolo delle trasformate di Fourier discrete (Discrete Fourier Transforms: DFT), che sono di fondamentale importanza per le moderne applicazioni delle trasmissioni digitali di dati. In essa vi è anche il fondamento per lo sviluppo dell'algoritmo delle trasformate di Fourier veloci (Fast Fourier Transforms: FFT).

[7] Leopold Kronecker (1823, Liegnitz (Prussia) ora Legnica (Polonia) – 1891, Berlino) studiò a Breslavia (ora Wrocław, Polonia) e a Berlino dove completò la tesi di dottorato con Dirichlet sulla teoria dei numeri algebrici: "Sulle unità complesse (1845). Era un uomo ricco che si limitò per vivere ad amministrare il patrimonio familiare. Tuttavia continuò a studiare matematica per diletto. Divenne membro dell'Accademia di Berlino nel 1861, e ciò gli diede il diritto d'insegnare all'università. I suoi corsi furono dedicati principalmente agli argomenti della sua ricerca: teoria delle equazioni, teoria dei numeri, dei determinanti e degli integrali. Tuttavia pochi studenti furono capaci di seguire fino alla fine il semestre delle sue lezioni. Un punto fondamentale del suo convincimento matematico era che "Dio creò gli interi; tutto il resto è opera dell'uomo. Fu perciò un fiero oppositore di Cantor e della sua teoria degli insiemi e, in particolare, della teoria degli irrazionali e, piú in generale, di tutti quei matematici che basavano le loro ricerche su metodi non costruttivi (Dedekind, Cantor, Heine, ...). Talvolta si complimentò con loro, per esempio con Lindemann, per la dimostrazione della trascendenza di π (1882), lamentando tuttavia che una dimostrazione cosí brillante fosse applicata ad un argomento inesistente come la teoria dei numeri trascendenti. Nel 1883, quando il suo maestro Kummer fu pensionato, gli successe nella cattedra all'università di Berlino. Ebbe modo di scontrarsi anche con Weierstrass che pensò di andarsene in Isvizzera nel 1888. Fu di bassa statura e molto suscettibile al proposito; troncò ogni relazione con Schwarz (discepolo di Weierstrass e genero di Kummer) per una scherzosa allusione fatta da costui sull'altezza di Kronecker. L'intuizionismo di Kronecker fu ripreso e sviluppato da Poincaré e da Brouwer.