ELEMENTI DI TEORIA DEGLI INSIEMI
Dispensa 4

Mauro Di Nasso

Ultimo aggiornamento: April 5, 2024

L'aritmetica di Peano e gli insiemi numerici

1. Gli insiemi finiti

Grazie ai numeri naturali, si può usare la nozione di equipotenza per definire in modo rigoroso il concetto di insieme finito.

DEFINIZIONE 1.1. Un insieme A si dice *finito* se esiste un numero naturale n tale che $|A| = |n|$, cioè se esiste una bigezione $f : n \to A$ per qualche $n \in \omega$. Un insieme si dice *infinito* se non è finito.

ESERCIZIO 1.2. Sia $(X, <)$ un insieme ordinato. Allora ogni $A \subseteq X$ finito ammette massimo e minimo; inoltre ogni elemento tranne il massimo ha un successore immediato, e ogni elemento tranne il minimo è un successoore immediato. Di conseguenza, ogni insieme ordinato $(X, <)$ dove X è finito è bene ordinato (cioè ogni suo sottoinsieme non vuoto ammette minimo).

ESERCIZIO 1.3. Due insiemi ordinati $(A, <)$ e $(B, <)$ dove A e B sono insiemi finiti equipotenti, sono isomorfi: $(A, <) \cong (B, <)$.

Ci sono molte proprietà degli insiemi finiti che vengono usualmente assunte come evidenti. Qui di seguito, invece, le enunceremo esplicitamente e ne daremo una dimostrazione. Cominciamo col dimostrare che l'antico principio secondo il quale *il tutto è maggiore della parte* vale tra insiemi finiti. In particolare, seguirà che un sottoinsieme di un insieme finito è finito.

PROPOSIZIONE 1.4. *Se $|B| = |n|$ è un insieme finito, e $A \subset B$ è un suo sottoinsieme proprio, allora $|A| = |m|$ per un opportuno $m < n$.*

DIM. Prendiamo una bigezione $f : B \to n$. Chiaramente $f(A)$ è un sottoinsieme proprio di n e $|A| = |f(A)|$. Per raggiungere la tesi, basta allora verificare che per ogni sottoinsieme proprio $X \subset n$ di un numero naturale, esiste $m < n$ con $|X| = |m|$. Procediamo per induzione su n.

Quando $n = 0$, la proprietà è vera a vuoto perché $\emptyset$ non ha alcun sottoinsieme proprio. Supponiamo ora che $X \subset n + 1 = \{0, 1, \dots, n\}$, e distinguiamo due casi.

1) $n \notin X$. In questo caso $X \subseteq n = \{0, 1, \dots, n - 1\}$. Se $X = n$, allora banalmente $|X| = |n|$ dove $n < n + 1$; se invece $X \subset n$ è un sottoinsieme proprio, dall'ipotesi induttiva segue che $|X| = |m|$ per qualche $m < n$, e dunque $m < n + 1$.

2) $n \in X$. In questo caso, $X' = X \setminus \{n\}$ è un sottoinsieme proprio di n e dunque, per ipotesi induttiva, $|X'| = |m|$ dove $m < n$. A questo punto, basta notare che da $|X'| = |m|$ segue che $|X| = |X' \cup \{n\}| = |m \cup \{m\}| = |m + 1|$, e inoltre $m < n \Rightarrow m + 1 < n + 1$, come voluto. □

Un'importante strumento della combinatoria finita è il cosiddetto *principio dei cassetti*: "Se sono stati distribuiti n oggetti in m cassetti dove $m < n$, allora c'è un cassetto dove trovo almeno due oggetti". In termini più formali:

PROPOSIZIONE 1.5 (Principio dei cassetti). *Siano n, m numeri naturali. Se $n > m$ allora non esistono funzioni iniettive $f : n \to m$. Equivalentemente, se $|n| \leq |m|$ allora $n \leq m$.*

DIM. Mostriamo che vale l'implicazione $|n| \leq |m| \Rightarrow n \leq m$ procedendo per induzione su n. La base $n = 0$ è vera a vuoto, perché la tesi $0 \leq m$ è sempre vera.[1] Consideriamo ora il passo induttivo, e supponiamo che esista una funzione iniettiva $f : n+1 \to m$. La restrizione $f|_n : n \to X$ dove $X = m \setminus \{f(n)\}$ è ancora iniettiva. Inoltre, visto che $X \subset m$ è un sottoinsieme proprio, per la Proposizione precedente esiste $k < m$ ed una bigezione $g : X \to k$. Ma allora la composizione $g \circ f|_n : n \to k$ è iniettiva e dunque, per l'ipotesi induttiva, $n \leq k < m$, e quindi $n + 1 \leq m$. □

Come diretta conseguenza otteniamo la naturale proprietà che due numeri naturali sono equipotenti se e solo se sono uguali.

PROPOSIZIONE 1.6. *Due numeri naturali diversi non sono equipotenti.*

DIM. Se $n \neq m$, allora uno è maggiore dell'altro, ad esempio $n > m$. L'esistenza di una bigezione $g : n \to m$ contraddirebbe il principio dei cassetti. □

COROLLARIO 1.7. Se A è un insieme finito e $B \subset A$ è un suo sottoinsieme proprio, allora $|A| \neq |B|$.

DIM. Sia $|A| = |n|$. Per la Proposizione 1.4, esiste $m < n$ con $|B| = |m|$ e quindi, per la proposizione precedente, $|A| = |n| \neq |m| = |B|$. □

ESERCIZIO 1.8. Sia $f : A \to A$ una funzione dove A è un insieme finito. Senza usare l'assioma di scelta, dimostrare che le seguenti proprietà sono equivalenti:

(1) f è iniettiva.
(2) f è suriettiva.
(3) f è biunivoca.

Per quanto visto sopra, la seguente definizione è ben posta.

DEFINIZIONE 1.9. Si dice *cardinalità* di un insieme finito A quell'unico numero naturale n tale che $|A| = |n|$. In tal caso scriviamo direttamente $|A| = n$.

Dunque prenderemo i numeri naturali come i *cardinali finiti*, cioè come i rappresentanti canonici delle classi di equipotenza di insiemi finiti. Definire i cardinali infiniti, cioè rappresentanti canonici delle classi di equipotenza di insiemi infiniti, sarà più complicato e richiederà lo sviluppo della teoria degli ordinali, che tratteremo più avanti.

La seguente nozione ha un'importanza storica, perché Dedekind la adottò come definizione di insieme infinito.

DEFINIZIONE 1.10. Un insieme A si dice *Dedekind-infinito* se è equipotente ad una sua parte propria, e si dice *Dedekind-finito* se non è Dedekind-infinito.

---

[1] Ricordiamo che un'implicazione $P \Rightarrow Q$ è vera quando l'ipotesi P è falsa (con Q qualunque); ed è vera quando la tesi Q è vera (con P qualunque).

PROPOSIZIONE 1.11. Se A è Dedekind-infinito allora A è infinito. Inoltre, assumendo (AC), vale anche il viceversa.[2]

DIM. Abbiamo già visto nel Corollario 1.7 che si ottiene direttamente che un insieme finito *non* può essere equipotente ad una sua parte propria. Viceversa, usando (AC), abbiamo dimostrato nel Teorema **??** che se A è infinito, allora esiste una funzione iniettiva $f : \mathbb{N} \to A$. La seguente funzione $g : A \to A \setminus \{f(1)\}$ è una bigezione tra A e una sua parte propria:

$$g(a) = \begin{cases} f(n+1) & \text{se } a = f(n) \text{ per qualche } n \in \mathbb{N} \\ a & \text{se } a \notin \operatorname{imm}(f). \end{cases}$$

□

Come diretta conseguenza, dimostriamo finalmente l'esistenza di insiemi infiniti.

PROPOSIZIONE 1.12. *L'insieme ω dei numeri naturali è infinito.*

DIM. Basta notare che ω è Dedekind-infinito. Infatti, la funzione "successore" $S : n \mapsto n + 1$ è una bigezione tra ω e il suo sottoinsieme proprio $\omega \setminus \{0\}$. □

ESERCIZIO 1.13.

(1) Se A e B sono finiti, allora anche $A \cap B$, $A \cup B$, $A \times B$, B^A e $\mathcal{P}(A)$ sono finiti;
(2) Se R è una relazione (binaria) finita, allora anche il dominio $\operatorname{dom}(R)$ e l'immagine $\operatorname{imm}(R)$ sono finiti. In particolare, se $f : X \to Y$ è una funzione e X è finito, allora anche l'immagine $\operatorname{imm}(f) = \{f(x) \mid x \in X\}$ è finita;
(3) Se $\mathcal{F}$ è una famiglia finita di insiemi finiti, allora anche l'unione $\bigcup_{F \in \mathcal{F}} \mathcal{F}$ è un insieme finito.

ESERCIZIO 1.14. Sia $\mathcal{F}$ una famiglia di insiemi. Allora:

(1) Se $\mathcal{F}$ è infinita e contiene insiemi a due a due disgiunti, allora l'unione $\bigcup_{A \in \mathcal{F}} A$ è infinita.
(2) Se per ogni $n \in \omega$ esiste $A \in \mathcal{F}$ con $n \leq |A|$, allora l'unione $\bigcup_{A \in \mathcal{F}} A$ è infinita.

Grazie al teorema di ricorsione, e all'assioma di scelta, possiamo finalmente dimostrare a partire dai nostri assiomi un'importante proprietà che già avevamo visto nella prima parte di teoria "ingenua" degli insiemi.

ESERCIZIO 1.15. Formalizzare nel dettaglio la dimostrazione del Teorema **??**: "*Se A è un insieme infinito, allora* $|\mathbb{N}| \leq |A|$".

[2] Se non si assume l'assioma di scelta, è consistente assumere l'esistenza di insiemi che non sono in bigezione con alcuna parte propria, e che allo stesso tempo non sono neanche in bigezione con alcun numero naturale.

2. Gli assiomi di Peano

Come abbiamo visto, l'insieme ω soddisfa il principio di induzione, e inoltre permette di formalizzare in modo rigoroso e soddisfacente la fondamentale nozione di finitezza. Vedremo di seguito che ω soddisfa anche le consuete proprietà algebriche che caratterizzano i numeri naturali. Per cominciare, definiremo le operazioni di *somma* e *prodotto*, facendo uso delle operazioni insiemistiche di unione disgiunta e di prodotto cartesiano.

Intuitivamente, il concetto di somma tra numeri naturali è strettamente collegato a quello di unione. Infatti, informalmente possiamo pensare alla somma $n+m$ come al numero di elementi dell'unione di un insieme avente n elementi con un insieme avente m elementi, purché siano disgiunti. Il prodotto $n \cdot m$ può essere pensato come la somma iterata $n+\cdots+n$ di n con se stesso per m volte. Notiamo che un prodotto cartesiano $A \times B$ è in realtà una unione $A \times B = \bigcup_{b\in B} A \times \{b\}$ di tante copie disgiunte di A quanti sono gli elementi di B. Questo suggerisce di pensare al prodotto $n \cdot m$ di numeri naturali, come al numero di elementi di un prodotto cartesiano tra un insieme con n elementi ed uno con m elementi. Tutte queste intuizioni, sono formalizzate nella seguente

Definizione 2.1. Se $n, m \in \omega$, poniamo:

- $n + m = |A \cup B|$ dove $|A| = n$, $|B| = m$, e $A \cap B = \emptyset$;
- $n \cdot m = |A \times B|$ dove $|A| = n$ e $|B| = m$.

Il fatto che la definizione data sopra è ben posta, segue da alcune proprietà. Anzitutto, unioni e prodotti cartesiani di insiemi finiti sono ancora insiemi finiti. Notiamo poi che per ogni $n, m \in \omega$, esistono sempre almeno due insiemi *disgiunti* A, B con $|A| = n$ e $|B| = m$. Non possiamo prendere direttamente m ed n, perché non sono disgiunti, ma il problema è facilmente risolubile, ad esempio considerando $A = n$ e $B = m \times \{0\}$. Infine, occorre che le cardinalità $|A \cup B|$ e $|A \times B|$ non dipendano dalla particolare scelta degli insiemi A e B, ma solo dalle loro cardinalità, ma anche questa proprietà era già stata verificata nel primo capitolo.

Un'ultima osservazione. Per ogni $n \in \omega$, la somma tra n ed 1 coincide con la cardinalità di $\widehat{n} = n \cup \{n\}$ (si tratta infatti di un'unione disgiunta), e quindi la notazione $n + 1 = \widehat{n}$ è coerente.

Adesso che abbiamo definito l'insieme ω con le operazioni di somma e prodotto, vogliamo verificare che la struttura che ne risulta realizza in effetti tutte le proprietà che la comune intuizione attribuisce ai numeri naturali. Per formalizzare tali proprietà, considereremo la cosiddetta "aritmetica di Peano", dal nome del matematico italiano che la introdusse nel 1889. Si tratta di una lista di assiomi che descrivono proprietà fondamentali della funzione successore $S(n) = n + 1$, delle operazioni di somma e prodotto, e che includono anche il principio di induzione. Gli assiomi di Peano hanno un contenuto intuitivo evidente, e tutte le fondamentali proprietà dei numeri naturali possono essere formalmente dimostrate a partire da essi. Per questo, il quadro assiomatico di Peano è universalmente adottato come il giusto riferimento per "definire" i numeri naturali.

Definizione 2.2. Una struttura $(\, N \,,\, 0 \,,\, S \,,\, + \,,\, \cdot \,)$ dove:

- N è un insieme;
- $0 \in N$ è un elemento fissato di N;

- $S : N \to N$ è una funzione, detta *funzione successore* ;
- $+ : N \times N \to N$ è una funzione binaria, detta *somma* ;
- $\cdot : N \times N \to N$ una funzione binaria, detta *prodotto* ;

è un *sistema di numeri naturali* se soddisfa i seguenti *assiomi di Peano*:

(PA1) Tutti e soli i numeri diversi da zero sono successori.
$\forall x\ (x \neq 0) \leftrightarrow (\exists y\ S(y) = x)$;

(PA2) La funzione successore è iniettiva.
$\forall x, y\ (x \neq y) \to (S(x) \neq S(y))$;

(PA3) La somma + soddisfa le seguenti proprietà:
(s1) $\forall x\ x + 0 = x$;
(s2) $\forall x, y\ (x + S(y) = S(x + y))$.

(PA4) Il prodotto $\cdot$ soddisfa le seguenti proprietà:
(p1) $\forall x\ x \cdot 0 = 0$;
(p2) $\forall x, y\ (x \cdot S(y) = (x \cdot y) + x)$.

$(\mathsf{PA5})_2$ *Principio di induzione del secondo ordine.*
Sia A un sottoinsieme di N. Se $0 \in A$ ed A è chiuso per successore, cioè $\forall x\ (x \in A) \to (S(x) \in A)$, allora $A = N$.

Quella data sopra è l'assiomatizzazione di Peano al *secondo ordine* PA_2, che differisce da quella al *primo ordine* PA solo nella formulazione del principio di induzione. Precisamente, in PA si rimpiazza $(\mathsf{PA5})_2$ con

(PA5) *Principio di induzione del primo ordine.*
Sia $P(x)$ una proprietà espressa come formula nel linguaggio dell'aritmetica di Peano. Allora

$$(\, P(0)\ \wedge\ (\forall x\ P(x) \to P(S(x)))\,)\ \to\ \forall x\ P(x).$$

Osserviamo che l'induzione al primo ordine segue direttamente dall'induzione al secondo ordine: infatti, per ogni formula assegnata $P(x)$, basta considerare il corrispondente insieme $A = \{x \in N \mid P(x)\}$. Viceversa, non tutti i sottoinsiemi $A \subseteq N$ sono della forma $\{x \in N \mid P(x)\}$, come si può capire con un semplice ragionamento sulle cardinalità. Infatti, l'insieme N deve essere infinito visto che – in base agli assiomi (PA1) e (PA2) – la funzione successore S è una bigezione tra N e il suo sottoinsieme proprio $N \setminus \{0\}$. Dunque i sottoinsiemi di N sono una quantità più che numerabile, mentre le possibili formule $P(x)$ nel linguaggio dell'aritmetica di Peano sono una quantità numerabile, perché le formule sono particolari stringhe finite formate con una quantità finita di simboli.[3] La conclusione è che l'induzione al secondo ordine è una proprietà strettamente più forte di quella al primo ordine. Abbiamo adottato qui l'assiomatizzazione più forte perché ci permetterà di dimostrare l'unicità dei modelli a meno di isomorfismi (vedi Teorema 2.6).

Come ulteriore distinzione, notiamo che l'induzione al secondo ordine $(\mathsf{PA5})_2$ *non* è formalizzabile usando formule del linguaggio dell'aritmetica; infatti non abbiamo simboli che denotino sottoinsiemi $A \subseteq N$; e *non* è ammissibile come formula la scrittura $\forall A \subseteq N \ldots$. Viceversa, l'induzione al primo ordine (PA5) è formalizzabile usando infinite formule nel linguaggio dell'aritmetica, una per ogni

[3] Le formule di PA vengono definite in modo analogo a come abbiamo definito le formule della teoria degli insiemi, considerando i simboli extra-logici 0, S, $+$, $\cdot$ al posto del simbolo di appartenenza $\in$.

fissata formula $\varphi(x)$; si tratta cioè di uno schema di assiomi, analogo all'assioma di separazione che abbiamo visto per la teoria degli insiemi ZFC.

A partire dagli assiomi di Peano si possono dimostrare ad una ad una tutte le proprietà che la pratica matematica attribuisce ai numeri naturali. Per cominciare con le più semplici, usando l'induzione si può verificare che valgono le proprietà associative, commutative e la distributività.

Esercizio 2.3. Verificare che le seguenti proprietà sono teoremi di PA:[4]

- $\forall x, y, z \;\; x + (y + z) = (x + y) + z$;
- $\forall x, y, z \;\; x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
- $\forall x, y \;\; x + y = y + x$;
- $\forall x \;\; x \cdot 1 = x$ dove $1 = S(0)$;
- $\forall x, y \;\; x \cdot y = y \cdot x$;
- $\forall x, y, z \;\; x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

L'ordinamento non è stato considerato nell'assiomatizzazione, perché può essere definito a partire dalla somma, ponendo

$$x < y \iff \exists z \neq 0 \; x + z = y.$$

Per induzione, si può poi verificare che

Esercizio 2.4. Le seguenti proprietà sono teoremi di PA:

- La relazione $<$ definita sopra è un ordine totale ;
- $\forall x, y, z \; (x < y \Rightarrow x + z < y + z)$;
- $\forall x, y \; \forall z \neq 0 \; (x < y \Rightarrow x \cdot z < y \cdot z)$.

Non ci dilunghiamo qui sullo sviluppo dell'aritmetica di Peano, che pure è argomento di grande importanza in logica, perché ci condurrebbe fuori dagli scopi di questo corso. Mostriamo ora che l'insieme ω ci fornisce effettivamente un sistema di numeri naturali.

Teorema 2.5.
La struttura $(\omega, 0, S, +, \cdot)$ dove la funzione successore è definita da $S(n) = \widehat{n} = n+1$, e le operazioni di somma e prodotto sono quelle della Definizione 2.1, soddisfa tutti gli assiomi dell'aritmetica di Peano al secondo ordine PA_2.

Dim. (PA1) e (PA2) esprimono la proprietà che S è una bigezione tra ω e $\omega \backslash \{0\}$, e questo è stato già dimostrato.

(PA3). Per la (s1) basta notare che $|\emptyset| = 0$, e che se $|A| = n$, banalmente anche $|A \cup \emptyset| = |A| = n$. Prendiamo A, B tali che $|A| = |n|$, $|B| = |m|$, e $A \cap B = \emptyset$, e prendiamo $\star$ tale che $\star \notin A \cup B$ (ad esempio, otteniamo le proprietà richieste con $A = n$, $B = m \times \{0\}$, e $\star = \{\{\{\emptyset\}\}\}$).[5] Abbiamo allora che:

$$n + S(m) = n + (m+1) = |A \cup (B \cup \{\star\})| = |(A \cup B) \cup \{\star\}| = (n+m)+1 = S(n+m),$$

e anche la (s2) è dimostrata.

[4] Cioè, si dimostrano a partire dagli assiomi dell'aritmetica di Peano al primo ordine.
[5] Notiamo che invece $\{\{\emptyset\}\} = (0, 0) \in B$.

(PA4). La (p1) segue dal fatto che per ogni A, il prodotto cartesiano $A \times \emptyset = \emptyset$. Per la (p2), notiamo che se $|A| = n$, $|B| = m$, e $\star \notin B$, allora $A \times B$ e $A \times \{\star\}$ sono disgiunti, e inoltre $|A \times \{\star\}| = |A| = n$. Dunque:

$$n \cdot S(m) = n \cdot (m+1) = |A \times (B \cup \{\star\})| = |(A \times B) \cup (A \times \{\star\})| = (n \cdot m) + n.$$

$(\mathsf{PA5})_2$ è la proprietà di induzione di ω, che abbiamo già dimostrato. □

Per completare la discussione, resta da vedere il fondamentale teorema di unicità, secondo il quale tutti i sistemi di numeri che soddisfano gli assiomi di Peano al secondo ordine sono tra loro isomorfi. In altre parole, l'assiomatizzazione PA_2 "definisce" il sistema dei numeri naturali.

Teorema 2.6 (Unicità del sistema dei numeri naturali).
Ogni sistema $(N, 0', S', \oplus, \odot)$ che soddisfa gli assiomi di Peano PA_2 al secondo ordine è isomorfo a $(\omega, 0, S, +, \cdot)$, cioè esiste una funzione biunivoca $\Theta : \omega \to N$ tale che:

(1) $\Theta(0) = 0'$;
(2) $\forall n \in \omega \quad \Theta(S(n)) = S'(\Theta(n))$;
(3) $\forall n, m \in \omega \quad \Theta(n+m) = \Theta(n) \oplus \Theta(m)$;
(4) $\forall n, m \in \omega \quad \Theta(n \cdot m) = \Theta(n) \odot \Theta(m)$.

Dim. Grazie al teorema di ricorsione numerabile, esiste ed unica funzione $\Theta : \omega \to N$ tale che

$$\begin{cases} \Theta(0) = 0' \\ \Theta(n+1) = S'(\Theta(n)) \end{cases}$$

Le proprietà (1) e (2) valgono banalmente per la definizione di Θ. Dobbiamo vedere che Θ è biunivoca, e che soddisfa anche le proprietà (3) e (4).

Θ è suriettiva. Per dimostrare che l'immagine di Θ coincide con N, procediamo per induzione all'interno del sistema $(N, 0', S', \oplus, \odot)$. Intanto $0' = \Theta(0) \in \mathrm{imm}(\Theta)$. Supponiamo ora che $x \in \mathrm{imm}(\Theta)$, cioè che $x = \Theta(n)$ per un opportuno $n \in \omega$. Ma allora anche $S'(x) = S'(\Theta(n)) = \Theta(n+1) \in \mathrm{imm}(\Theta)$.

Θ è iniettiva. Stavolta procediamo per induzione nel sistema $(\omega, 0, S, +, \cdot)$, e dimostriamo che la seguente "proprietà" vale per ogni $n \in \omega$:[6]

$$P(n): \quad \forall m \quad \Theta(m) = \Theta(n) \Rightarrow m = n$$

Se $m \neq 0$ allora, in virtù dell'assioma (PA1) che vale in ω, sarà $m = m' + 1$ per un opportuno m'. In questo caso $\Theta(m) = \Theta(m'+1) = S'(\Theta(m')) \neq 0' = \Theta(0)$, visto che (PA1) vale anche in N. Con questo abbiamo dimostrato che vale $P(0)$. Supponiamo ora vera $P(n)$, e supponiamo che $\Theta(m) = \Theta(n+1) = S'(\Theta(n))$. Chiaramente $m \neq 0$, altrimenti $\Theta(m) = \Theta(0) = 0' \neq S'(\Theta(n))$. Allora $m = m' + 1$ per un opportuno m', e quindi $S'(\Theta(m')) = \Theta(m) = \Theta(n+1) = S'(\Theta(n))$. Dall'assioma (PA2) segue allora che $\Theta(m') = \Theta(n)$ e, applicando l'ipotesi induttiva, concludiamo che $m' = n$, da cui $m = n + 1$, come volevamo.

[6] Notiamo che $P(n)$ *non* è una proprietà formalizzabile nel linguaggio dell'aritmetica di Peano, perché vi compare il parametro Θ. Più correttamentre, avremmo dovuto considerare il corrispondente insieme $X = \{n \in \omega \mid \forall m \quad \Theta(m) = \Theta(n) \Rightarrow m = n\}$, che esiste per separazione, e dimostrare per induzione al secondo ordine che $X = \omega$.

Occupiamoci ora della proprietà (3). Procediamo per induzione, e dimostriamo che la seguente "proprietà" vale per ogni $m \in \omega$:[7]

$$P(m): \quad \forall n \;\; \Theta(n+m) = \Theta(n) \oplus \Theta(m)$$

Il caso base $P(0)$ è una immediata applicazione della (s1) di (PA3); infatti $\Theta(n+0) = \Theta(n) = \Theta(n) \oplus 0' = \Theta(n) \oplus \Theta(0)$. Per il caso successore, si usano l'ipotesi induttiva, la definizione di Θ, e la (s2) di (PA3), che vale sia in ω che in N. Precisamente, si hanno le uguaglianze:

$$\begin{aligned} \Theta(n+(m+1)) &= \Theta((n+m)+1) = S'(\Theta(n+m)) = S'(\Theta(n) \oplus \Theta(m)) = \\ &= \Theta(n) \oplus S'(\Theta(m)) = \Theta(n) \oplus \Theta(m+1). \end{aligned}$$

La proprietà (4) relativa al prodotto si dimostra in modo del tutto analogo alla proprietà (3), stavolta applicando l'assioma (PA4). □

Da qui in avanti, per seguire l'uso comune, talvolta scriveremo $\mathbb{N}$ per denotare l'insieme $\omega \setminus \{0\}$ dei naturali positivi; e scriveremo $\mathbb{N}_0$ per denotare $\mathbb{N} \cup \{0\} = \omega$.

3. Gli interi e i razionali

Storicamente si è cercato di ricondurre i fondamentali insiemi numerici (interi, razionali, reali e complessi) al sistema dei numeri naturali, visto come una solida base alla quale riferirsi per evitare possibili contraddizioni ed errori. Cominciamo a sviluppare questo progetto *riduzionista*, considerando la seguente relazione $\sim$ sul prodotto cartesiano $\omega \times \omega$:

$$(a,b) \sim (c,d) \quad \Longleftrightarrow \quad a+d = b+c.$$

L'idea intuitiva è quella di pensare alla coppia ordinata di numeri naturali (a,b) come al numero "$a-b$". Si può verificare facilmente che $\sim$ è una relazione di equivalenza. Diamo allora la:

DEFINIZIONE 3.1. Il sistema $(\mathbb{Z}, \leq, 0, +, \cdot)$ dei numeri interi è il sistema dove:

- $\mathbb{Z}$ è l'insieme quoziente $(\omega \times \omega)/\sim$;
- 0 è la classe di equivalenza $[(0,0)]$;
- $[(a,b)] \leq [(c,d)] \Leftrightarrow a+d \leq b+c$;
- La *somma* tra elementi di $\mathbb{Z}$ è definita ponendo:
$$[(a,b)] + [(c,d)] = [(a+c, b+d)];$$
- Il *prodotto* tra elementi di $\mathbb{Z}$ è definito ponendo:
$$[(a,b)] \cdot [(c,d)] = [(a \cdot c + b \cdot d\,,\; a \cdot d + b \cdot c)].$$

Dobbiamo verificare che le definizioni date sopra sono ben poste, cioè non dipendono dai rappresentanti scelti nelle classi di equivalenza. Precisamente, occorre dimostrare che se $(a,b) \sim (a',b')$ e se $(c,d) \sim (c',d')$, allora:

- $a+d \leq b+c \;\; \Leftrightarrow \;\; a'+d' \leq b'+c'$;
- $(a+c, b+d) \sim (a'+c', b'+d')$;
- $(ac+bd, ad+bc) \sim (a'c'+b'd', a'd'+b'c')$.

Si tratta di verifiche dirette, che possono essere svolte come esercizio.

[7] Anche in questo caso valgono le considerazioni della nota precedente.

Esercizio 3.2. Per ogni coppia ordinata $(a, b) \in \omega \times \omega$, si verifica una ed una sola delle seguenti due possibilità:

- $(a, b) \sim (0, 0)$;
- $(a, b) \sim (n, 0)$ per un unico naturale positivo $n \in \mathbb{N}$;
- $(a, b) \sim (0, m)$ per un unico naturale positivo $m \in \mathbb{N}$.

Nel primo caso, identifichiamo $[(a, b)] = [(0, 0)]$ con $0 \in \mathbb{N}_0$. Nel secondo caso, identifichiamo $[(a, b)] = [(n, 0)]$ con $n \in \mathbb{N}$, così da avere $\mathbb{N}_0 \subseteq \mathbb{Z}$. Infine, nel terzo caso, denotiamo l'elemento $[(a, b)] = [(0, m)] \in \mathbb{Z}$ con $-m$. In questo modo, ritroviamo la consueta scrittura adoperata per i numeri interi.

Teorema 3.3. *Il sistema dei numeri interi* $(\mathbb{Z}, \leq, 0, 1, +, \cdot)$ *è un anello ordinato discreto, la cui parte non-negativa è il sistema dei numeri naturali.*

Valgono la seguenti caratterizzazioni degli interi.

Esercizio 3.4. A meno di isomorfismi, $(\mathbb{Z}, \leq, 0, 1, +, \cdot)$ è l'unico anello ordinato discreto dove tutti i sottoinsiemi non vuoti e limitati inferiormente hanno minimo.

Esercizio 3.5. A meno di isomorfismi, $(\mathbb{Z}, 0, 1, +, \cdot)$ è l'unico anello con la *proprietà universale*: "Per ogni anello R con unità esiste un unico omomorfismo $\varphi : \mathbb{Z} \to R$".

La dimostrazione di questo teorema segue direttamente dalle definizioni, ed è lasciata per esercizio.

I numeri razionali sono introdotti in modo analogo agli interi. Precisamente si prende l'insieme $\mathbb{Z} \times \mathbb{N}$ delle coppie ordinate di interi la cui seconda componente è un intero positivo, e si considera la seguente relazione:

$$(a, b) \approx (c, d) \quad \iff \quad a \cdot d = b \cdot c.$$

Qui l'intuizione è quella di pensare ad una coppia ordinata (a, b) come al quoziente "a/b". Si può facilmente verificare che $\approx$ è una relazione di equivalenza.

Definizione 3.6. Il sistema $(\mathbb{Q}, \leq, 0, 1, +, \cdot)$ dei numeri razionali è il sistema dove:

- $\mathbb{Q}$ è l'insieme quoziente $(\mathbb{Z} \times \mathbb{N}) / \approx$;
- 0 è la classe di equivalenza $[(0, 1)]$;
- 1 è la classe di equivalenza $[(1, 1)]$;
- $[(a, b)] \leq [(c, d)] \Leftrightarrow a \cdot d \leq b \cdot c$;
- La *somma* tra elementi di $\mathbb{Q}$ è definita ponendo:
$$[(a, b)] + [(c, d)] = [(a \cdot d + b \cdot c, b \cdot d)];$$
- Il *prodotto* tra elementi di $\mathbb{Z}$ è definito ponendo:
$$[(a, b)] \cdot [(c, d)] = [(a \cdot c, b \cdot d)].$$

Anche in questo caso, è necessario dimostrare che le definizioni di sopra sono ben poste, cioè che se $(a, b) \approx (a', b')$ e se $(c, d) \approx (c', d')$, allora:

- $ad \leq bc \quad \Leftrightarrow \quad a'd' \leq b'c'$;
- $(ad + bc, bd) \approx (a'd' + b'c', b'd')$;
- $(ac + bd, ad + bc) \approx (a'c' + b'd', a'd' + b'c')$.

La verifica delle proprietà di sopra e la dimostrazione del seguente teorema, sono lasciate per esercizio.

TEOREMA 3.7. *Il sistema dei numeri razionali* $(\mathbb{Q}, \leq, 0, 1, +, \cdot)$ *è un campo ordinato.*[8] *Inoltre:*

(1) $\mathbb{Q}$ *è denso, cioè per ogni* $q_1 < q_2$ *esiste* q *con* $q_1 < q < q_2$ *;*
(2) $\mathbb{Q}$ *gode della "proprietà archimedea", cioè per ogni* $0 < q_1 < q_2$ *esiste* $n \in \mathbb{N}$ *con* $q_1 \cdot n > q_2$*.*

4. I numeri reali

Dedichiamo questo paragrafo all'introduzione dei numeri reali $\mathbb{R}$, definiti a partire dall'insieme dei numeri razionali $\mathbb{Q}$. Successivamente, definiremo i numeri complessi $\mathbb{C}$ a partire da $\mathbb{R}$. Con questo ultimo passo, avremo così raggiunto l'obbiettivo "riduzionista" che ci eravamo prefissati, cioè quello di definire tutti i fondamentali insiemi numerici a partire dal sistema dei numeri naturali.

È importante far presente subito che, dal punto di vista fondazionale, la riduzione dei numeri reali ai numeri razionali è un processo essenzialmente più complicato rispetto alle altre riduzioni viste fin qui. Infatti, le costruzioni coinvolte per le definizioni dei numeri interi e dei numeri razionali richiedevano soltanto l'uso di prodotti cartesiani e di loro quozienti rispetto ad opportune relazioni di equivalenza. Invece la costruzione dei reali richiederà un uso essenziale dell'*assioma delle parti*, che tra l'altro determinerà il salto di cardinalità dal numerabile al continuo.

La prima parte della costruzione si basa esclusivamente sulle proprietà di $\mathbb{Q}$ come insieme ordinato, senza alcun riferimento alla sua struttura algebrica di campo.

DEFINIZIONE 4.1. Un sottoinsieme $X \subseteq \mathbb{Q}$ si dice *taglio di Dedekind* se:

(1) X è non banale, cioè $X \neq \emptyset$ e $X \neq \mathbb{Q}$;
(2) X è un *segmento iniziale*, cioè se $x' < x \in X$ allora anche $x' \in X$;
(3) X non ha massimo.

Notiamo che, in base alla condizione (2), $x \notin X$ se e solo se x è un maggiorante di X. Il segmento iniziale $\mathbb{Q}_q$ generato da un razionale $q \in \mathbb{Q}$, è un taglio di Dedekind:

$$\mathbb{Q}_q = \{q' \in \mathbb{Q} \mid q' < q\}.$$

Ma ci sono anche tagli di Dedekind che non sono di quella forma. Un tipico esempio è dato dal seguente taglio, che sarà identificato con il numero reale $\sqrt{2}$.

ESERCIZIO 4.2. L'insieme $X = \{q \in \mathbb{Q} \mid (q \leq 0) \vee (q^2 < 2)\}$ è un taglio di Dedekind, ed inoltre $X \neq \mathbb{Q}_q$ per ogni $q \in \mathbb{Q}$.

ESERCIZIO 4.3. Sia X un taglio di Dedekind. Allora per ogni razionale $\varepsilon > 0$, esistono $x \in X$ e $y \notin X$ aventi distanza $y - x < \varepsilon$.

[8] In linguaggio algebrico, $\mathbb{Q}$ è il campo delle frazioni dell'anello degli interi $\mathbb{Z}$.

DEFINIZIONE 4.4. L'insieme dei *numeri reali* è l'insieme

$$\mathbb{R} = \{X \in \mathcal{P}(\mathbb{Q}) \mid X \text{ taglio di Dedekind}\}.$$

Identifichiamo ogni numero razionale $q \in \mathbb{Q}$ con il corrispondente taglio di Dedekind $\mathbb{Q}_q \in \mathbb{R}$, così da avere $\mathbb{Q} \subset \mathbb{R}$.

Osserviamo che l'esistenza dell'insieme $\mathbb{R}$ è garantita dall'assioma delle *parti* e dall'assioma di *separazione*.

La relazione d'inclusione tra gli elementi di $\mathbb{R}$ è una relazione d'ordine totale e *completa*. Precisamente:

TEOREMA 4.5.

(1) *Per $X, Y \in \mathbb{R}$, poniamo $X \leq Y$ quando $X \subseteq Y$. Allora $(\mathbb{R}, \leq)$ è un insieme totalmente ordinato;*
(2) *Per ogni $q, q' \in \mathbb{Q}$ si ha $q \leq q' \Leftrightarrow \mathbb{Q}_q \leq \mathbb{Q}_{q'}$. Dunque, vista l'identificazione di ogni $q \in \mathbb{Q}$ con il corrispondente taglio di Dedekind $\mathbb{Q}_q \in \mathbb{R}$, $(\mathbb{Q}, \leq)$ è un sottoinsieme ordinato di $(\mathbb{R}, \leq)$;*
(3) *$\mathbb{Q}$ è denso in $(\mathbb{R}, \leq)$, cioè per ogni $X, Y \in \mathbb{R}$ con $X < Y$, esiste $q \in \mathbb{Q}$ con $X < q < Y$;*
(4) *$(\mathbb{R}, \leq)$ è completo, cioè ogni sottoinsieme non vuoto $A \subset \mathbb{R}$ che sia superiormente limitato, ammette estremo superiore:*

$$\sup A = \min\{x \in \mathbb{R} \mid x > a \text{ per ogni } a \in A\}.$$

DIM. (1). La proprietà *riflessiva*, cioè "$X \subseteq X$", e la proprietà *simmetrica*, cioè "$(X \subseteq Y \wedge Y \subseteq X) \to X = Y$" sono banalmente soddisfatte. Per verificare la proprietà *tricotomica*, supponiamo che $X \neq Y$ siano due tagli di Dedekind diversi; allora esiste un elemento che appartiene ad uno ma non all'altro, ad esempio un elemento $x_0 \in X$ con $x_0 \notin Y$ (se esiste $y_0 \in Y$ con $y_0 \notin X$ la dimostrazione è del tutto simile). Da $x_0 \notin Y$ segue che $x_0 > y$ per ogni $y \in Y$, visto che Y è un segmento iniziale; ma allora $Y \subset X$, visto che X è un segmento iniziale, ed abbiamo $X < Y$.

(2). Siano $q < q'$ due numeri razionali. Banalmente $\mathbb{Q}_q \subseteq \mathbb{Q}_{q'}$. Dobbiamo vedere che $\mathbb{Q}_q \neq \mathbb{Q}_{q'}$, e questo segue subito dalla densità di $(\mathbb{Q}, \leq)$. Infatti se prendiamo $\widetilde{q}$ con $q < \widetilde{q} < q'$, chiaramente $\widetilde{q} \in \mathbb{Q}_{q'}$ mentre $\widetilde{q} \notin \mathbb{Q}_q$. Il viceversa "$\mathbb{Q}_q < \mathbb{Q}_{q'} \Rightarrow q < q'$" segue direttamente da quanto appena dimostrato (se per assurdo fosse $q \geq q'$, allora $\mathbb{Q}_{q'} \supseteq \mathbb{Q}_q$).

(3). Siano $X < Y$. Allora esiste $q \in Y \setminus X$. Osserviamo che non si può escludere che $X = \mathbb{Q}_q$. Per definizione di taglio di Dedekind, Y non ha massimo, dunque esiste $q' \in Y$ con $q < q'$. Così $q \in \mathbb{Q}_{q'} \setminus X$, e dunque $X < \mathbb{Q}_{q'}$. Inoltre da $q' \in Y$ segue subito che $\mathbb{Q}_{q'} < Y$.

(4). Sia $A \subset \mathbb{R}$ un insieme di tagli di Dedekind come nelle ipotesi. Consideriamo l'unione $Y = \bigcup A = \bigcup_{X \in A} X$ di tutti i suoi elementi. Vogliamo dimostrare che $Y \in \mathbb{R}$, cioè che Y stesso è un taglio di Dedekind. Da questo seguirà subito la tesi perché banalmente $X \subseteq Y$ per ogni $X \in A$, dunque Y è un maggiorante. Inoltre Y è il più piccolo dei maggioranti perché se $Y' \supseteq X$ per ogni $X \in A$, allora chiaramente $Y' \supseteq \bigcup_{X \in A} X = Y$.

Vediamo intanto Y è un sottoinsieme *non banale* di $\mathbb{Q}$. Per ipotesi $A \neq \emptyset$, dunque esiste un taglio di Dedekind $X \in A$ e quindi $\emptyset \neq X \subseteq Y$. Inoltre A è superiormente limitato, dunque esiste $Z \in \mathbb{R}$ con $X \subseteq Z$ per ogni $X \in A$, da cui

$Y = \bigcup_{X \in A} X \subseteq Z \neq \mathbb{Q}$. Per vedere che Y è un segmento iniziale, consideriamo $y' < y$ dove $y \in Y$. Prendiamo $X \in A$ con $y \in X$. Poiché X è un taglio di Dedekind, da $y' < y \in X$ segue che $y' \in X \subseteq Y$, come voluto. Resta infine da controllare che Y non ha massimo. Se $y \in Y$, prendiamo $X \in A$ con $y \in X$. Allora esiste $y' \in X \subseteq Y$ con $y < y'$. □

La nostra costruzione di $(\mathbb{R}, \leq)$ ha avuto come punto di partenza l'insieme ordinato $(\mathbb{Q}, \leq)$ dei numeri razionali. Più in generale, dato un qualunque insieme denso $(P, \leq)$ senza massimo né minimo, possiamo considere l'insieme $\widetilde{P}$ dei suoi tagli di Dedekind. Con gli stessi argomenti visti sopra, si dimostra che $(\widetilde{P}, \subseteq)$ è un insieme ordinato completo senza massimo nè minimo che ha (una copia di) P come sottoinsieme denso. Questo procedimento di *completamento* è unico a meno di isomorfismi. Precisamente, si può dimostrare che se $(P', \leq)$ è un un insieme ordinato completo privo di massimo e minimo e avente $P \subseteq P'$ come sottoinsieme denso, allora esiste una bigezione $\Theta : P' \to \widetilde{P}$ che preserva l'ordine: "$p_1 < p_2 \Leftrightarrow \Theta(p_1) < \Theta(p_2)$". In altre parole, a meno di cambiare i "nomi" agli elementi, $(\widetilde{P}, \subseteq)$ e $(P', \leq)$ sono lo stesso insieme ordinato. Non dimostriamo qui questo teorema generale di unicità del completamento; il caso che ci interessa, cioè quello di $\mathbb{Q}$ ed $\mathbb{R}$, seguirà come corollario del teorema di unicità dei reali come campo ordinato completo che vedremo più avanti.

Il nostro obbiettivo adesso è quello di dare una struttura algebrica di campo all'insieme dei numeri reali. Cominciamo definendo l'operazione di *somma* tra tagli di Dedekind (di razionali):

$$X + Y = \{x + y \mid (x \in X) \wedge (y \in Y)\}.$$

Esercizio 4.6.

(1) Siano $a, x, y \in \mathbb{Q}$ tre numeri razionali con $a < x + y$. Allora $a = x' + y'$ per opportuni $x', y' \in \mathbb{Q}$ dove $x' < x$ e $y' < y$;
(2) Se X, Y sono tagli di Dedekind, allora anche $X+Y$ è un taglio di Dedekind;
(3) L'operazione di somma tra tagli di Dedekind è coerente con la somma tra razionali, cioè per ogni $q, q' \in \mathbb{Q}$ si ha $\mathbb{Q}_q + \mathbb{Q}_{q'} = \mathbb{Q}_{q+q'}$.

Chiaramente, la somma tra tagli è una operazione *commutativa* e *associativa*.

Occupiamoci ora dell'*opposto*. Per i tagli di Dedekind originati da razionali, poniamo $-(\mathbb{Q}_q) = \mathbb{Q}_{-q}$. Se invece X non è della forma $\mathbb{Q}_q$, cioè quando $\mathbb{Q} \setminus X$ non ha minimo, allora poniamo:

$$-X = \{q \in \mathbb{Q} \mid -q \notin X\}.$$

Denotiamo direttamente con 0 il taglio $\mathbb{Q}_0 = \{q \in \mathbb{Q} \mid q < 0\}$.

Esercizio 4.7. Sia X un taglio di Dedekind. Allora:

(1) $-X$ è un taglio di Dedekind;
(2) $(X) + (-X) = 0$;
(3) $X < 0$ se e solo se $-X > 0$.

Per definire il *prodotto*, consideriamo prima il caso di tagli positivi $X, Y > X_0$. In questo caso $X^+ = \{x \in X \mid x > 0\}$ e $Y^+ = \{y \in Y \mid y > 0\}$ sono non vuoti, e si pone:

$$X \cdot Y = \{x \cdot y \mid (x \in X^+) \wedge (y \in Y^+)\} \cup \{q \in \mathbb{Q} \mid q \leq 0\}.$$

Esercizio 4.8. Siano $a, x, y \in \mathbb{Q}^+$ tre numeri razionali positivi con $a < x \cdot y$. Allora $a = x' \cdot y'$ per opportuni $x', y' \in \mathbb{Q}$ dove $0 < x' < x$ e $0 < y' < y$.

Utilizzando la proprietà di quest'ultimo esercizio, si verificano i seguenti risultati.

Esercizio 4.9.

(1) Se $X, Y > 0$ sono tagli di Dedekind positivi, allora anche $X \cdot Y$ è un taglio di Dedekind (positivo) ;
(2) L'operazione di prodotto tra tagli di Dedekind positivi è coerente con il prodotto tra razionali, cioè per ogni $q, q' \in \mathbb{Q}^+$ si ha $\mathbb{Q}_q \cdot \mathbb{Q}_{q'} = \mathbb{Q}_{q \cdot q'}$.

Chiaramente, il prodotto sopra definito tra tagli positivi è una operazione *commutativa* e *associativa*. Il prodotto tra tagli qualunque è definito facendo uso dell'opposto. Precisamente:

- Se $X = 0$ o $Y = 0$, si pone: $X \cdot Y = Y \cdot X = 0$;
- Se $X > 0$ e $Y < 0$, si pone: $X \cdot Y = Y \cdot X = -(X \cdot (-Y))$;
- Se $X < 0$ e $Y < 0$, si pone: $X \cdot Y = (-X) \cdot (-Y)$.

Osserviamo che, per la (3) dell'Esercizio 4.7, le definizioni di sopra sono ben poste perché si riconducono al prodotto tra tagli di Dedekind positivi. Segue poi direttamente dall'esercizio precedente che anche il prodotto tra tagli qualunque è una operazione *commutativa* e *associativa*.

Esercizio 4.10.

(1) Vale la proprietà *distributiva*: $X \cdot (Y + Z) = X \cdot Y + X \cdot Z$;
(2) Le operazioni di somma e prodotto tra tagli di Dedekind sono coerenti con l'ordinamento: $X \leq Y$ e $Z \geq 0 \Rightarrow X + Z \leq Y + Z$ e $X \cdot Z \leq Y \cdot Z$.

Proseguiamo definendo l'*inverso* di ogni taglio positivo $X > 0$.

Se $X = \mathbb{Q}_q$ è generato da un razionale $q > 0$, poniamo $1/\mathbb{Q}_q = \mathbb{Q}_{1/q}$. Se invece $X > 0$ non è della forma $\mathbb{Q}_q$, poniamo

$$1/X = \{1/q \mid q \notin X\}.$$

Si verifica facilmente che anche $1/X > 0$ è un taglio di Dedekind positivo. Per $X < 0$ negativi, poniamo $1/X = -(1/(-X))$.

Esercizio 4.11. Per ogni $X \neq 0$, $X \cdot (1/X) = 1$ è il taglio generato da 1.

Abbiamo cosí finalmente introdotto tutta la struttura dei reali, che ricapitoliamo nella seguente

Definizione 4.12. Il sistema dei *numeri reali* è il sistema $(\mathbb{R}, \leq, 0, 1, +, \cdot)$ dove:

- $\mathbb{R} = \{X \subset \mathbb{Q} \mid X \text{ è un taglio di Dedekind}\}$;
- $X \leq Y$ se e solo se $X \subseteq Y$;
- Ogni numero razionale $q \in \mathbb{Q}$ è identificato con il corrispondente taglio $X_q = \{q' \in \mathbb{Q} \mid q' < q\}$. In particolare $0 = X_0$ e $1 = X_1$;
- La somma e il prodotto tra tagli sono definiti come visto sopra.

Mettendo insieme i risultati presentati negli ultimi esercizi, si ottiene una dimostrazione del:

TEOREMA 4.13. *Il sistema dei numeri reali* $(\mathbb{R}, \leq, 0, 1, +, \cdot)$ *è un campo ordinato completo.*

Sia ora F un campo ordinato qualunque. Visto che il campo $\mathbb{Q}$ è generato da $\{0, 1\}$, esiste ed unico omomorfismo di campi $\psi : \mathbb{Q} \to F$ tale che $\psi(0) = 0_F$ e $\psi(1) = 1_F$, dove 0_F e 1_F sono gli elementi neutri della somma e del prodotto di F, rispettivamente. Precisamente, se $n, m \in \mathbb{N}$ con $m > 0$, $\psi(\pm\frac{n}{m}) = \pm\frac{n_F}{m_F}$, dove $n_F = 1_F + \ldots + 1_F$ è la somma iterata di 1_F con se stesso per n volte. Si può verificare facilmente che ψ è un omomorfismo iniettivo di campi ordinati.[9] Visto che ψ determina un isomorfismo con la sua immagine $\mathbb{Q} \cong \psi(\mathbb{Q})$, possiamo assumere direttamente che $\mathbb{Q} \subseteq F$ sia un sottocampo ordinato di F.

Il prossimo teorema ci mostrerà che la proprietà di essere un campo ordinato completo caratterizza (a meno di isomorfismi) il sistema dei numeri reali.

TEOREMA 4.14 (Unicità dei reali).
Ogni campo ordinato completo è isomorfo al sistema dei numeri reali $(\mathbb{R}, \leq, 0, 1, +, \cdot)$.

DIM. Sia F un qualunque campo ordinato completo. Abbiamo visto sopra che si può direttamente assumere $\mathbb{Q} \subset F$. Per evitare confusioni, denotiamo con $\leq_F$ la relazione d'ordine su F, e con $\leq_R$ la relazione d'ordine su $\mathbb{R}$ data dall'inclusione tra tagli di Dedekind. Sui numeri razionali $q, q' \in \mathbb{Q}$ le due relazioni coincidono, e in questo caso scriveremo semplicemente $q < q'$. Denotiamo infine con $\sup_F$ l'estremo superiore calcolato in F.

Notiamo che se $X \in \mathbb{R}$ è un taglio di Dedekind, allora X è superiormente limitato anche in F. Risulta così ben definita la funzione:

$$\psi : \mathbb{R} \to F \quad \text{dove} \quad \psi(X) = \sup_F X.$$

La funzione ψ preserva l'ordine, ed è quindi iniettiva. Infatti se $X \subset Y$, per densità esiste $q \in \mathbb{Q}$ con $X <_R q <_R Y$, e dunque

$$\psi(X) = \sup_F X \leq q < \sup_F Y = \psi(Y).$$

Occupiamoci ora della suriettività, e prendiamo un generico $x \in F$. È facile verificare che l'insieme di razionali $F_x = \{q \in \mathbb{Q} \mid q <_F x\}$ è un taglio di Dedekind. Per la densità di $\mathbb{Q}$ in F, si ha $x = \sup_F F_x = \psi(F_x)$.

Resta da vedere che ψ è un omomorfismo di campi, cioè che per ogni $X, Y \in \mathbb{R}$, valgono le uguaglianze $\psi(X + Y) = \psi(X) + \psi(Y)$ e $\psi(X \cdot Y) = \psi(X) \cdot \psi(Y)$. Denotiamo con:

$$\xi = \psi(X) = \sup_F X\,, \quad \eta = \psi(Y) = \sup_F Y.$$

Se $x \in X$ e $y \in Y$, chiaramente $x < \xi$ e $y < \eta$, dunque $x + y < \xi + \eta$, e quindi

$$\psi(X + Y) = \sup_F\{x + y \mid (x \in X) \wedge (y \in Y)\} \leq \xi + \eta.$$

Fissiamo ora $a <_F \xi + \eta$. Per definizione di estremo superiore, esistono $x \in X$ e $y \in Y$ con $x >_F \xi - \varepsilon$ e $y >_F \eta - \varepsilon$, dove abbiamo preso $\varepsilon = \frac{\xi+\eta-a}{2} > 0$. Ma allora $x + y >_F \xi + \eta - 2\varepsilon = a$. Questo dimostra che

$$\psi(X + Y) = \sup_F\{x + y \mid (x \in X) \wedge (y \in Y)\} \geq \sup_F\{a \mid a <_F \xi + \eta\} = \xi + \eta.$$

[9] Notiamo che il campo F ha necessariamente caratteristica zero perché è ordinato.

Con il prodotto la dimostrazione è analoga. Supponiamo prima che $X, Y > 0$. Una delle due disuguaglianze è banale:

$$\psi(X \cdot Y) = \sup_F\{x \cdot y \mid (x \in X^+) \wedge (y \in Y^+)\} \leq \xi \cdot \eta.$$

Fissiamo ora un elemento $a <_F \xi \cdot \eta$ positivo. Per densità, possiamo prendere un razionale q con $\frac{a}{\xi \cdot \eta} < q < 1$. Per la (1) dell'Esercizio 4.9, possiamo scrivere $q = q_1 q_2$ come prodotto di due razionali positivi $q_1, q_2 < 1$. Visto che $\xi \cdot q_1 < \xi$ e $\eta \cdot q_2 < \eta$, per definizione di estremo superiore, esistono $x \in X$ e $y \in Y$ tali che $x > \xi \cdot q_1$ e $y > \eta \cdot q_2$. Dunque abbiamo $x \cdot y > \xi \cdot \eta \cdot (q_1 q_2) > \xi \cdot \eta \cdot \frac{a}{\xi \cdot \eta} = a$. Possiamo così concludere che vale anche l'altra disuguaglianza:

$$\psi(X \cdot Y) = \sup_F\{x \cdot y \mid (x \in X) \wedge (y \in Y)\} \geq \sup_F\{a \mid a <_F \xi \cdot \eta\} = \xi \cdot \eta.$$

Infine, per il caso generale di tagli non necessariamente positivi, osserviamo che:

$$\psi(-X) = \sup_F\{q \in \mathbb{Q} \mid -q \notin X\} = -\inf_F\{q \in \mathbb{Q} \mid q \notin X\} = -\sup_F\{q \in \mathbb{Q} \mid q \in X\}.$$

Dunque $\psi(-X) = -\psi(X)$, e ci si può ricondurre al caso visto sopra di tagli positivi. □

Ricordiamo l'importante proprietà archimedea.

Proposizione 4.15. Sia F un campo ordinato qualunque. Allora le seguenti condizioni sono equivalenti:

(1) F soddisfa la *proprietà archimedea*:
"Sia $x > 0$. Allora per ogni $\varepsilon > 0$ esiste $n \in \mathbb{N}$ tale che $n \cdot \varepsilon > x$".
(2) $\mathbb{Q}$ è denso in F;
(3) Non esistono *infinitesimi* $\delta \neq 0$, cioè elementi $\delta \neq 0$ tali che $-1/n < \delta < 1/n$ per ogni $n \in \mathbb{N}^+$.
(4) $\mathbb{N}$ è illimitato in F, cioè per ogni $x \in F$ esiste $n \in \mathbb{N}$ con $x < n$.

Inoltre, quando F è completo, tutte le condizioni di sopra sono verificate.

Dim. Per vedere l'equivalenza delle quattro condizioni, dimostriamo in sequenza le implicazioni (1) ⇒ (2) ⇒ (3) ⇒ (4) ⇒ (1).

(1) ⇒ (2). Siano $0 < x < y$ due elementi positivi di F. Per la proprietà archimedea, esiste $m \in \mathbb{N}$ tale che $m \cdot 1 > \frac{1}{y-x}$, cioè $\frac{1}{m} < y - x$. Di nuovo per la proprietà archimedea, l'insieme $A = \{n \in \mathbb{N} \mid n \cdot \frac{1}{m} > x\} \neq \emptyset$, e per il principio del buon ordinamento dei numeri naturali, esisterà $n = \min A$. Chiaramente $(n-1) \cdot \frac{1}{m} \notin A$, e quindi:

$$x < \frac{n}{m} = (n-1) \cdot \frac{1}{m} + \frac{1}{m} \leq x + \frac{1}{m} < x + (y - x) = y.$$

Dunque $\frac{n}{m}$ è la frazione cercata. Il caso $x < 0 < y$ è banale perché $0 \in \mathbb{Q}$. Infine, se $x < y < 0$, per il caso già dimostrato esiste $\frac{n}{m}$ con $0 < -y < \frac{n}{m} < -x$, e quindi $x < -\frac{n}{m} < y$.

(2) ⇒ (3). Per assurdo sia $\delta \neq 0$ un infinitesimo. Possiamo supporre $\delta > 0$ (altrimenti prendiamo $-\delta$). Per ogni $n, m \in \mathbb{N}^+$ si ha $0 < \delta < \frac{n}{m}$, visto che $\delta < \frac{1}{m}$ per definizione di infinitesimo. Ne seguirebbe che $\mathbb{Q}$ non è denso in F.

(3) $\Rightarrow$ (4). Se $\mathbb{N}$ fosse limitato, esisterebbe $x \in F$ tale che $x > n$ per ogni $n \in \mathbb{N}$. Ma allora $\frac{1}{x}$ sarebbe un infinitesimo positivo.

(4) $\Rightarrow$ (1). Per ipotesi, esiste $n \in \mathbb{N}$ tale che $\frac{x}{\varepsilon} < n$, dunque $n \cdot \varepsilon > x$.

Per concludere la dimostrazione, basta vedere che se una delle quattro condizioni (equivalenti) di sopra *non* vale, allora F *non* è completo. Supponiamo dunque che (4) non valga, cioè che $\mathbb{N}$ sia limitato in F. È facile verificare che se x è un maggiorante di $\mathbb{N}$, allora anche $x - 1$ lo è. Dunque $\sup \mathbb{N}$ non esiste. □

Un primo esempio di campo archimedeo (non completo) è il campo $\mathbb{Q}$ dei numeri razionali. Vediamo ora un esempio di campo non-archimedeo.

Esercizio 4.16. Sia

$$\mathbb{Q}(x) = \left\{ \frac{A(x)}{B(x)} \,\middle|\, A(x), B(x) \in \mathbb{Q}[x], B(x) \neq 0 \right\}$$

il campo delle frazioni dell'anello dei polinomi $\mathbb{Q}[x]$ a coefficienti razionali. Poniamo:

$$\frac{a_0 + a_1 x + \ldots + a_n x^n}{b_0 + b_1 x + \ldots + b_m x^m} \prec 0 \Leftrightarrow \frac{a_n}{b_m} < 0 \quad \text{e} \quad \frac{A(x)}{B(x)} \prec \frac{C(x)}{D(x)} \Leftrightarrow \frac{A(x)}{B(x)} - \frac{C(x)}{D(x)} \prec 0$$

Dimostrare che:

(1) $(\mathbb{Q}(x), \preceq, 0, 1, +, \cdot)$ è un campo ordinato;
(2) Tutti gli elementi $\frac{a_0 + a_1 x + \ldots + a_n x^n}{b_0 + b_1 x + \ldots + b_m x^m}$ dove $n < m$ sono infinitesimi.

Esercizio 4.17. Il campo $\mathbb{Q}(x)$ (con l'ordine $\preceq$ definito sopra) è il più piccolo campo non-archimedeo, nel senso che ogni campo non-archimedeo ha un sottocampo isomorfo a $\mathbb{Q}(x)$.

Concludiamo questo capitolo definendo i numeri complessi. I numeri interi e i numeri razionali sono stati definiti come opportuni insiemi quoziente di coppie ordinate. L'idea di considerare coppie ordinate viene usata anche per definire i numeri complessi a partire dai numeri reali. Precisamente, si dà la seguente

Definizione 4.18. Il sistema $(\mathbb{C}, 0, 1, +, \cdot)$ dei *numeri complessi* è il sistema dove:

- $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ è l'insieme delle coppie ordinate di numeri reali;
- 0 è la coppia $(0, 0)$ e 1 è la coppia $(1, 0)$;
- La somma è definita ponendo: $(a, b) + (c, d) = (a + c, b + d)$;
- Il prodotto è definito ponendo: $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

Nella pratica si introduce il simbolo i, detto *unità immaginaria*, e si usa la notazione $z = a + ib$ per indicare $z = (a, b) \in \mathbb{C}$. Il numero reale a, cioè la prima componente della coppia ordinata, viene chiamato *parte reale* di z, mentre il numero reale b, cioè la seconda componente, viene chiamato *parte immaginaria* di z. Coerentemente con la definizione di sopra, dati due numeri complessi $z = a + ib$ e $w = c + id$, la somma si calcola sommando le rispettive parti reali e immaginarie:

$$(a + ib) + (c + id) = (a + b) + i(b + d).$$

Per il prodotto, si procede come nei prodotti tra polinomi con incognita i, adottando la convenzione che $i^2 = -1$. Dunque:

$$(a + ib) \cdot (c + id) = ac + iad + ibc + i^2 bd = (ac - bd) + i(ad + bc).$$

Identificando ogni numero reale $a \in \mathbb{R}$ con il numero complesso $(a, 0) = a + i \cdot 0$, il campo dei reali $\mathbb{R}$ risulta un sottocampo di $(\mathbb{C}, 0, 1, +, \cdot)$. Inoltre vale la seguente ben nota proprietà, per la quale rimandiamo ad un corso di algebra.

TEOREMA 4.19. *Il sistema dei numeri complessi* $(\mathbb{C}, 0, 1, +, \cdot)$ *è la chiusura algebrica del campo dei numeri reali.*